Redes Virtuais Seguras: Uma Nova Abordagem de Mapeamento para Proteger contra Ataques de Disrupção na Rede Física

Rodrigo R Oliveira[1], Leonardo R Bays[1], Daniel S Marcon[1], Miguel C Neves[1], Luciana S Buriol[1], Luciano P Gaspary[1], Marinho P Barcellos[1]

[1]Universidade Federal do Rio Grande do Sul (UFRGS), Instituto de Informática

{ruas.oliveira, lrbays, daniel.stefani, mcneves, buriol, paschoal, marinho}@inf.ufrgs.br

Resumo. *Na virtualização de redes, roteadores e enlaces virtuais são alocados sobre uma infraestrutura de rede física. Tal característica representa uma vulnerabilidade a ataques de negação de serviço na rede física, visto que um único dispositivo físico comprometido afeta todos os virtuais sobrepostos. Trabalhos anteriores propõem a reserva de recursos sobressalentes. Apesar de funcional, esse tipo de solução agrega custo ao provedor da rede física. Neste artigo, propõe-se uma abordagem para alocação de redes virtuais que explora o compromisso entre a resiliência a ataques e a eficiência na utilização de recursos. A abordagem é separada em duas estratégias, uma preventiva e uma reativa. A primeira aloca enlaces virtuais em múltiplos caminhos do substrato, enquanto a segunda tenta recuperar a capacidade dos enlaces virtuais afetada por um ataque de negação de serviço subjacente. Ambas as estratégias são formuladas como problemas de otimização. Resultados numéricos demonstram o nível de resiliência a ataques propiciado pela abordagem e o baixo custo decorrente da mesma.*

Abstract. *In network virtualization, virtual routers and links are embedded into a physical network infrastructure. Such characteristic represents a vulnerability as a compromised physical device affects all the overlaid virtual ones. Previous work proposes setting aside backup resources. Although effective, this solution aggregates cost to infrastructure providers. In this paper, we propose a virtual network allocation approach which explores the trade-off between resilience to attacks, and efficiency in resource utilization. Our approach is composed of two strategies, one preventive and the other reactive. The former allocates virtual links into multiple substrate paths, while the latter attempts to recover the capacity of virtual links affected by an underlying DoS attack. Both strategies are formulated as optimization problems. Numerical results show the level of resilience to attacks and the low cost demanded by our approach.*

1. Introdução

A virtualização de redes consiste na instanciação de múltiplas redes virtuais sobre um mesmo substrato de rede física. Esse paradigma permite o isolamento entre redes virtuais, propiciando a independência funcional entre as mesmas. Uma de suas mais promissoras vantagens é a capacidade de limitar o escopo de ataques, através da organização de uma infraestrutura em múltiplas redes virtuais, isolando o tráfego das mesmas [Khan *et al* 2012]. De maneira geral, as redes virtuais são requisitadas por diferentes "Provedores de Serviço" (*Service Providers* – SP), e alocadas sob-demanda

 ©2012 SBC — Soc. Bras. de Computação

nos recursos físicos de "Provedores de Infraestrutura" (*Infrastructure Provider* – InP) [Belbekkouche *et al* 2012]. A alocação significa designar uma parcela dos nós e enlaces físicos do substrato aos nós e enlaces virtuais sobrepostos. Dessa forma, as redes virtuais compartilham os recursos dos dispositivos da rede física [Chowdhury and Boutaba 2010]. Tal particularidade tende a aumentar a dependência de certos recursos físicos. Consequentemente, um atacante pode lançar ataques de negação de serviço às redes virtuais, comprometendo para isso roteadores e/ou enlaces do substrato físico subjacente. Especificamente, caso determinado enlace do substrato seja comprometido, todos os enlaces virtuais sobrepostos (ou seja, alocados neste) serão afetados[1].

Para lidar com esse problema, a literatura propõe estratégias que reservam determinada quantidade de recursos do substrato como sobressalentes. Essa reserva pode ser uma fração de todos os recursos da rede [Rahman *et al* 2010] ou a alocação extra de nós disjuntos [Yeow *et al* 2010], caminhos disjuntos [Chen *et al* 2010, Guo *et al* 2011] ou ambos [Yu *et al* 2011]. Apesar de eficaz, essa abordagem pode ser muito custosa ao Provedor de Infraestrutura visto que os recursos sobressalentes (a) ficam ociosos caso não haja disrupções e (b) a ocupação extra pode limitar a alocação de novas redes. Dessa forma, a aplicabilidade dessas estratégias pode ficar limitada a nichos de mercado, deixando pragmaticamente as futuras redes virtuais vulneráveis a ataques de negação de serviço.

Neste artigo é proposta uma abordagem para aumentar a resiliência das redes virtuais dos Provedores de Serviço contra ataques de DoS, sem prejudicar a alocação dos recursos físicos do Provedor de Infraestrutura. A abordagem pode ser dividida em duas estratégias complementares, formuladas como problemas de otimização linear inteira. Primeiro utiliza-se uma estratégia **preventiva** para mitigar o impacto de um ataque. Nessa estratégia os enlaces virtuais são alocados em *múltiplos caminhos preferencialmente disjuntos* para impedir que toda a capacidade dos enlaces virtuais seja afetada quando um enlace físico subjacente é comprometido. Após a ocorrência de um ataque, utiliza-se uma estratégia **reativa** para recuperar, *parcial ou integralmente*, a capacidade perdida nos enlaces virtuais afetados.

A abordagem proposta acarreta dois problemas principais: (i) a alocação com *priorização por caminhos disjuntos* levar à sobrecarga de determinados enlaces físicos, deixando pouca ou nenhuma capacidade disponível, potencialmente impedindo a alocação de novas redes que dependem daquele enlace; e (ii) o uso de múltiplos caminhos, com atrasos de propagação potencialmente distintos, causa o problema da entrega de pacotes fora de ordem. Para mitigar o primeiro problema propõe-se o balanceamento de carga entre os enlaces do substrato, evitando saturar os caminhos escolhidos. Para tratar do segundo, alocações são feitas buscando minimizar a diferença dos atrasos entre caminhos, em linha com a literatura [Zhang *et al* 2010]. Tais escolhas serão discutidas na Seção 3.

As principais contribuições deste artigo são sumarizadas a seguir:

- **Modelagem dos três fatores do problema, combinando relativamente o impacto de caminhos disjuntos, balanceamento de carga e alocação eficiente de recursos (Seção 3).** Obtém-se assim um equilíbrio entre a resiliência das redes virtuais e a eficiência de alocação de recursos.

[1]Este artigo concentra-se em ataques, mas as soluções propostas também aplicam-se a falhas.

 ©2012 SBC — Soc. Bras. de Computação

- **Formulação das estratégias como problemas de otimização (Seção 4).** As duas estratégias propostas neste artigo, a *alocação em múltiplos caminhos* e a *redistribuição oportunística de carga*, são formuladas em programação linear inteira. As formulações geram o *resultado ótimo* de acordo com a priorização desejada.
- **Análise do compromisso gerado pela solução (Seção 5).** Experimentos demonstram que a abordagem proposta pode reduzir substancialmente o impacto de ataques de negação de serviço, porém ao custo de uma taxa de aceitação menor. Este artigo responde a seguinte questão: *como sobreviver à disrupção nas redes virtuais aumentando minimamente o custo?*

O restante do artigo está organizado da seguinte forma: a Seção 2 descreve trabalhos relacionados. A Seção 3 define o modelo de ataque e os principais conceitos relacionados à alocação de redes virtuais, ao atraso diferencial e ao objetivo. A Seção 4 apresenta as formulações em programação linear inteira das duas estratégias desenvolvidas. Por fim, os resultados da avaliação dos modelos são discutidos na Seção 5, e a Seção 6 conclui o trabalho.

2. Trabalhos relacionados

O presente trabalho se concentra em ataques de negação de serviço a redes virtualizadas através do comprometimento de enlaces físicos. O problema pode ser relacionado à pesquisa em sobrevivência em redes. Embora tal assunto não seja novo, apenas recentemente a comunidade científica começou a tratar dessa questão no contexto de redes virtuais. Esta seção discute os trabalhos relacionados, tanto em um contexto mais amplo como especificamente em redes virtualizadas.

A principal diferença entre o tratamento de disrupções nas redes virtuais para as redes convencionais (p.ex., redes ópticas, MPLS ou no planejamento de tráfego IP) é que na virtualização de redes o tráfego é gerado pelas redes virtuais, as quais podem ser instaladas e retiradas da rede sob-demanda. Em contraste, nas redes convencionais o tráfego entre os nós é conhecido e considerado como um parâmetro do modelo [Medhi 2006]. Ademais, as redes virtuais devem garantir a topologia, ou seja, os enlaces virtuais devem permanecer ativos. Por outro lado, nas redes convencionais basta manter a conectividade [Belbekkouche *et al* 2012].

De maneira geral, a resiliência das redes virtuais é provida através da alocação de recursos sobressalentes. [Rahman *et al* 2010], [Chen *et al* 2010] e [Guo *et al* 2011] estudam a *disrupção de enlaces do substrato físico*. [Rahman *et al* 2010] reservam determinado percentual de banda de cada enlace do substrato para proteger enlaces virtuais contra disrupções. Os autores calculam "k-caminhos mais curtos" entre os nós de cada enlace físico, resultando em micro-desvios. Caso um enlace físico seja interrompido, o fluxo é redirecionado pelos recursos sobressalentes desses desvios. Por sua vez, [Chen *et al* 2010] e [Guo *et al* 2011] utilizam a alocação de caminhos disjuntos, entre os mapeamentos primário e sobressalente, como estratégia para prover resiliência a disrupções.

Por outro lado, [Yeow *et al* 2010] estudam a *negação de serviço em nós da rede física*. Os autores consideram a existência de nós virtuais críticos. Para proteger esses nós, os autores oferecem redundância por meio da reserva de nós físicos sobressalentes. Apesar de não considerar disrupções em enlaces físicos, a estratégia também reserva caminhos sobressalentes para manter a topologia. Isso pode resultar em um número potencialmente grande de enlaces físicos alocados como

 ©2012 SBC — Soc. Bras. de Computação

sobressalentes, visto que cada nó redundante precisa manter a conectividade dos nós críticos mapeados.

[Yu *et al* 2011] consideram eventos de *disrupção regionalizada* no substrato. Tal evento ocorre quando uma única ação compromete múltiplos dispositivos de uma mesma localidade. Para sobreviver a esses eventos, cada nó virtual é replicado em regiões distintas. Além disso, os caminhos entre esses nós sobressalentes não podem passar pelas mesmas regiões dos primários. Essa solução, no entanto, pode restringir bastante o espaço de soluções.

As soluções anteriores fazem uso da reserva de recursos sobressalentes para oferecer resiliência. Tal abordagem pode ser muito custosa ao substrato pois os recursos sobressalentes limitam a alocação de novas redes e ficam ociosos caso não haja disrupções. Em contraste, [Houidi *et al* 2010] dispensam recursos sobressalentes e propõem o uso de multiagentes para lidar com *negação de serviço em nós e enlaces físicos*. Na proposta, os roteadores físicos devem implementar um agente que se comunica com os demais para realocar nós e enlaces virtuais de dispositivos sob ataque. Apesar de não alocar recursos sobressalentes, a estratégia precisa recalcular novos caminhos para os enlaces virtuais afetados. Essa estratégia demanda um período de convergência e pode deixar as redes virtuais inoperantes durante o mesmo.

A proposta apresentada neste artigo difere das anteriores pelas seguintes razões: i) ela não considera a alocação de recursos sobressalentes; ii) a recuperação de capacidade dos enlaces virtuais não necessita recalcular os caminhos fim-a-fim, evitando o custo de realizar esta computação na recuperação; iii) as restrições de resiliência são relaxadas de forma a oferecer uma estratégia menos custosa ao provedor de infraestrutura.

3. Definições Preliminares

3.1. Modelo de Ameaça

A principal ameaça considerada neste artigo é a disrupção de comunicação entre os nós das redes virtuais. Essa disrupção pode ocorrer por meio de ataques de negação de serviço nos roteadores ou enlaces da rede física.

Ataques a roteadores e enlaces físicos. Um ataque de negação de serviço pode ser feito por meio do acesso físico ao dispositivo, ou exploração de alguma vulnerabilidade. No primeiro caso, um atacante obtém a localização de uma fibra óptica ou roteador e interrompe seu funcionamento (p.ex., cortando a fibra ou desligando a energia). No segundo caso, o atacante explora alguma vulnerabilidade no protocolo ou *software* de controle para comprometer algum dispositivo.

Premissas. O escopo deste trabalho é delimitado pelas seguintes premissas:

- Considera-se que um atacante pode obter informação sobre a utilização de determinado dispositivo. Dessa forma, o ataque tem como alvo o nó ou enlace com maior utilização, de forma a causar o maior impacto.
- Há isolamento entre as redes virtuais. Portanto, uma rede virtual não pode interferir no funcionamento de outra ao tentar consumir mais recursos do que requisitou.
- A disrupção de um nó físico pode ser reduzida a disrupções em múltiplos enlaces físicos do substrato.

 ©2012 SBC — Soc. Bras. de Computação

3.2. Alocação de Redes Virtuais

A alocação de redes virtuais consiste em alocar nós e enlaces virtuais em nós e caminhos do substrato físico, respectivamente. Cada nó virtual é alocado em um nó físico distinto e cada enlace virtual é alocado em *um caminho* (ou *subconjunto dos caminhos*) do substrato. Ademais, as requisições de redes virtuais são enviadas ao substrato físico *sob-demanda*, ou seja, não é possível determinar com antecedência quais redes virtuais deverão ser alocadas. Essas e as demais definições estão em linha com trabalhos anteriores de alocação [Chowdhury *et al* 2009, Cheng *et al* 2012].

Substrato. Representado por um grafo dirigido $G^S(N^S, E^S, A^S)$, onde N^S é o conjunto de nós, E^S o conjunto de enlaces e A^S o conjunto de atributos dos nós e enlaces. Neste artigo, são considerados os seguintes atributos: *capacidade computacional* dos nós, *largura de banda* e *atraso de propagação* dos enlaces.

Requisição de rede virtual. Cada requisição é definida por um grafo dirigido $G^V(N^V, E^V, A^V)$, onde N^V, E^V e A^V são conjuntos similares aos supracitados.

3.3. Atraso Diferencial

A divisão do tráfego de dados nem sempre pode ser realizada por caminhos com mesmo atraso fim-a-fim. Particularmente, a utilização de caminhos com diferenças de atraso pode intensificar a entrega de pacotes fora de ordem. Esse problema (definido como *problema do atraso diferencial*) acaba impactando o funcionamento geral dos protocolos de entrega confiável (p.ex., TCP). De maneira geral, pode-se realizar a multiplexação de três formas [He and Rexford 2008]: por fluxo, por rajadas (*flowlets*) ou por pacotes. A primeira forma possui baixa granularidade, visto que cada fluxo está limitado à capacidade de um único caminho. A segunda permite que o mesmo fluxo modifique o caminho de tempos em tempos, o que pode ser ineficiente em fluxos que possuam comportamento contínuo. A terceira alternativa possui a melhor granularidade, permitindo que os fluxos agreguem toda a capacidade dos caminhos.

Neste trabalho optou-se por esta última alternativa, a qual permite aos enlaces das redes virtuais utilizar toda a capacidade requisitada. Apesar dessa grande vantagem, a multiplexação por pacotes pode impor um custo adicional ao destino, seja aos roteadores de borda ou aos hospedeiros. Tal custo, em memória e processamento, é diretamente proporcional às diferenças no atraso entre pacotes. Portanto, de forma similar a trabalhos anteriores [Zhang *et al* 2010], define-se como subobjetivo de otimização a minimização do atraso diferencial.

3.4. Objetivos de Otimização

A formulação apresentada neste trabalho possui por objetivo oferecer resiliência às redes virtuais, levando em consideração o custo gerado ao substrato físico. Para isso, o modelo proposto considera três fatores principais.

Priorização por multi-caminhos disjuntos. A alocação em múltiplos caminhos permite que um enlace virtual possa resistir a uma disrupção na rede física. No entanto, tal característica só é eficiente se os caminhos selecionados são suficientemente diferentes, caso contrário, uma disrupção em um enlace físico poderia afetar a maior parte dos caminhos utilizados por determinado enlace virtual. No pior caso, uma disrupção pode afetar completamente um ou mais enlaces virtuais. Para lidar com esse problema, define-se a função $\Xi = \sum_{\forall e^S \in E^S} \sum_{\forall e^V \in E^V} \xi_{e^S, e^V}$, a qual descreve a penalidade total dada pela similaridade entre os caminhos.

 ©2012 SBC — Soc. Bras. de Computação

Balanceamento de carga. Conforme mencionado anteriormente, a alocação de redes virtuais é feita sob-demanda. Com isso, a alocação a longo prazo pode causar a saturação de um subconjunto dos enlaces da rede física. Essa saturação, por sua vez, pode acabar gerando rejeição de novas requisições que possuam preferência por determinado (subconjunto de) enlace(s) físico(s). O balanceamento de carga é utilizado para evitar essa saturação de enlaces físicos. Para isso, define-se a função $\Phi = \sum_{\forall e^S \in E^S} \phi_{e^S}$, expressando a penalização pela saturação do substrato.

Minimização do atraso diferencial. Supondo P_{e^V} o conjunto de caminhos selecionados para alocar determinado enlace virtual, D_p como o atraso no caminho p e $\delta_{e^V} = \max_{\forall p,q \in P_{e^V}}(| D_p - D_q |)$ como a diferença entre o maior e menor atraso no conjunto de caminhos de um enlace virtual. A função $\Delta = \sum_{\forall e^V \in E^V} \delta_{e^V}$ penaliza o atraso diferencial acumulado de todos os enlaces virtuais.

4. Estratégias para Mitigar a Disrupção na Rede Física

Nesta seção são definidas as duas estratégias, preventiva e reativa, para oferecer resiliência contra ataques de negação de serviço às redes virtuais. A primeira estratégia consiste no mapeamento dos enlaces virtuais em múltiplos caminhos, de forma que o comprometimento de um ou mais enlaces físicos não afete completamente os enlaces virtuais. A segunda estratégia é utilizada quando um ataque obtém sucesso em derrubar um enlace. Essa estratégia tenta realocar a capacidade perdida nos caminhos que não foram afetados.

4.1. Mapeamento de Redes Virtuais considerando Resiliência

A estratégia utilizada para prover resiliência visa mapear cada enlace virtual das requisições em conjuntos de caminhos físicos, tal que: (i) toda a capacidade do enlace virtual seja distribuída por esses caminhos e (ii) tais caminhos tenham pouca similaridade entre si. A formulação da estratégia é dada conforme segue:

Variáveis:

- $\mathcal{X}_{n^S,n^V} \in \mathbb{B}$: indica que o nó $n^S \in N^S$ do substrato físico está sendo utilizado para mapear o nó virtual $n^V \in N^V$.
- $\mathcal{P}_{p,e^S,e^V} \in \mathbb{B}$: indica que o caminho p utiliza o enlace do substrato $e^S \in E^S$ para mapear o enlace virtual $e^V \in E^V$.
- $\mathcal{F}_{p,e^S,e^V} \in \mathbb{R}$ no intervalo $[0;1]$: indica a parcela do fluxo do enlace virtual $e^V \in E^V$ a ser alocada no enlace físico e^S para o caminho p.

Entrada:

- $c(.) \in A^*$: poder computacional de determinado nó (físico ou virtual).
- $b(.) \in A^*$: largura de banda de determinado enlace (físico ou virtual).
- $d(.) \in A^S$: atraso de determinado enlace físico.
- $P, |P|$: representam, respectivamente, o conjunto de índices dos caminhos e número máximo de caminhos por enlace virtual.

Objetivo: *minimizar o impacto causado pelos três fatores do problema*,

$$\min Z = w_\Xi \cdot \Xi + w_\Phi \cdot \Phi + w_\Delta \cdot \Delta \tag{1}$$

onde w_Φ, w_Ξ e w_Δ são pesos que representam a importância relativa de cada parte da função objetivo. A definição das funções de penalização que compõem Ξ, Φ e Δ serão apresentadas após as restrições do modelo.

 ©2012 SBC — Soc. Bras. de Computação

Restrições:

$$\sum_{\forall n^S \in N^S} x_{n^S,n^V} = 1 \qquad \forall n^V \in N^V \tag{2}$$

$$\sum_{\forall n^V \in N^V} x_{n^S,n^V} \leq 1 \qquad \forall n^S \in N^S \tag{3}$$

$$\sum_{\forall n^V \in N^V} x_{n^S,n^V} \cdot c(n^V) \leq c(n^S) \qquad \forall n^S \in N^S \tag{4}$$

$$\sum_{\forall p \in P} \sum_{\forall e^V \in E^V} f_{p,e^S,e^V} \cdot b(e^V) \leq b(e^S) \qquad \forall e^S \in E^S \tag{5}$$

$$\sum_{\forall b^S \in N^S : (a^S,b^S) \in E^S} p_{p,(a^S,b^S),e^V} - \sum_{\forall b^S \in N^S : (b^S,a^S) \in E^S} p_{p,(b^S,a^S),e^V} = x_{a^S,s^V} - x_{a^S,t^V} \tag{6}$$

$$\forall p \in P, \forall a^S \in N^S, \forall e^V = (s^V, t^V) \in E^V$$

$$\sum_{\forall p \in P} \sum_{\forall b^S \in N^S : (a^S,b^S) \in E^S} f_{p,(a^S,b^S),e^V} - \sum_{\forall p \in P} \sum_{\forall b^S \in N^S : (a^S,b^S) \in E^S} f_{p,(b^S,a^S),e^V} = x_{a^S,s^V} - x_{a^S,t^V} \tag{7}$$

$$\forall a^S \in N^S, \forall e^V = (s^V, t^V) \in E^V$$

$$f_{p,e^S,e^V} \leq p_{p,e^S,e^V} \qquad \forall p \in P, \forall e^S \in E^S, \forall e^V \in E^V \tag{8}$$

As restrições (2) e (3) garantem respectivamente que todo nó virtual será alocado a exatamente um nó físico e que nós virtuais serão alocados em nós físicos diferentes. As restrições (4) e (5) asseguram que as capacidades dos nós e enlaces físicos serão respeitadas. A formação de um caminho fim-a-fim válido é representada pela restrição (6). Por fim, as duas últimas restrições definem a quantidade de banda em cada caminho. Elas asseguram a conservação de fluxo ao longo dos caminhos (7) e que o fluxo só será definido em enlaces físicos selecionados (8).

O conjunto de restrições anterior não previne a formação de laços na rede. Dessa forma, adiciona-se a variável auxiliar h_{p,a^S,e^V} e a restrição não linear $h_{p,b^S,e^V} = p_{p,(a^S,b^S),e^V} \cdot h_{p,a^S,e^V} + p_{p,(a^S,b^S),e^V}$. Essa restrição "conta o número de saltos" do roteador origem ao destino de cada caminho. Com isso, mapeamentos com laços serão naturalmente descartados pois não seria possível encontrar solução factível. A linearização da restrição é feita pela substituição da multiplicação de variáveis por uma variável auxiliar τ. Após, com o uso de técnicas padrões é possível atribuir relação entre as mesmas. Esse processo culminou nas seguintes restrições:

$$h_{p,n^S,e^V} \leq \sum_{\substack{m^S \in N^S : \\ (m^S,n^S) \in E^S}} \sigma \cdot p_{p,(m^S,n^S),e^V} \qquad \forall p \in P, \forall n^S \in N^S, \forall e^V \in E^V : \sigma \to \infty \tag{9}$$

$$h_{p,n^S,e^V} = \sum_{\substack{m^S \in N^S : \\ (m^S,n^S) \in E^S}} \left(|\, E^S \,| \cdot \tau_{p,(m^S,n^S),e^V} + p_{p,(m^S,n^S),e^V} \right) \qquad \forall p \in P, \forall n^S \in N^S, \forall e^V \in E^V \tag{10}$$

$$\tau_{p,e^S,e^V} \leq \frac{h_{p,n^S,e^V}}{|\, E^S \,|} \qquad \forall p \in P, \forall e^S = (n^S, m^S) \in E^S, \forall e^V \in E^V \tag{11}$$

$$\tau_{p,e^S,e^V} \leq p_{p,e^S,e^V} \qquad \forall p \in P, \forall e^S \in E^S, \forall e^V \in E^V \tag{12}$$

$$\tau_{p,e^S,e^V} \geq \frac{h_{p,n^S,e^V}}{|\, E^S \,|} + p_{p,e^S,e^V} - 1 \qquad \forall p \in P, \forall e^S = (n^S, m^S) \in E^S, \forall e^V \in E^V \tag{13}$$

$$h_{p,n^S,e^V},\ \tau_{p,e^S,e^V} \geq 0 \qquad \forall p \in P, \forall n^S \in N^S, \forall e^S \in E^S, \forall e^V \in E^V \tag{14}$$

 ©2012 SBC — Soc. Bras. de Computação

Funções de penalização: a priorização por caminhos disjuntos é dada pela penalização da similaridade de caminhos. Tal restrição é definida por uma aproximação linear de uma função que cresce exponencialmente com o compartilhamento de enlaces físicos. A expressão generalizada é dada pela seguinte formula:

$$\xi_{e^S,e^V} \geq w_K \cdot \sum_{p \in P} \mathcal{P}_{p,e^S,e^V} - c_K \qquad \forall e^S \in E^S, \forall e^V \in e^V \tag{15}$$

onde a constante K ($\leq |P|$) indica quantos caminhos do enlace virtual e^V utilizam o mesmo enlace físico e^S, e $w_K = s^{K-1}$ ($s \geq 2$) indica o peso dessa sobreposição. Por sua vez, c_K é dado pela seguinte equação: $c_K = w_K \cdot (K-1) - [w_{K-1} \cdot (K-1) - c_{K-1}]$, $\forall e^S \in E^S, \forall e^V \in e^V, c_0 = 0, w_0 = 0$. A expressão da Eq. (15) é utilizada para criar uma restrição para cada caminho. Portanto, no caso de 2 caminhos serão criadas duas restrições da seguinte forma:

$$\xi_{e^S,e^V} \geq \sum_{p \in P} \mathcal{P}_{p,e^S,e^V} \qquad \forall e^S \in E^S, \forall e^V \in e^V$$

$$\xi_{e^S,e^V} \geq s^1 \cdot \sum_{p \in P} \mathcal{P}_{p,e^S,e^V} - c_1 \qquad \forall e^S \in E^S, \forall e^V \in e^V$$

Para prover a penalidade na saturação de enlaces (ϕ) utilizou-se a função clássica de engenharia de tráfego proposta por [Fortz and Thorup 2004]. Tal função define um custo exponencial (com aproximação linear) proporcional à utilização do enlace físico e a capacidade do mesmo.

Por fim, para calcular o atraso diferencial, é preciso encontrar os atrasos mínimo e máximo ao longo dos caminhos. Como a ordem dos caminhos não é importante para a formulação, é possível adicionar a seguinte restrição sem alterar o resultado da otimização:

$$\sum_{\forall e^S \in E^S} \mathcal{P}_{p,e^S,e^V} \cdot d(e^S) \leq \sum_{\forall e^S \in E^S} \mathcal{P}_{p+1,e^S,e^V} \cdot d(e^S) \qquad \forall p \in P = \{1,\ldots,k\} \setminus \{k\}, \forall e^V \in E^V$$

a qual ordena os caminhos selecionados de menor a maior atraso. Logo, o atraso diferencial em um enlace virtual δ_{e^V} pode ser calculado pela seguinte expressão:

$$\delta_{e^V} = \sum_{\forall e^S \in E^S} \mathcal{P}_{k,e^S,e^V} \cdot d(e^S) - \sum_{\forall e^S \in E^S} \mathcal{P}_{1,e^S,e^V} \cdot d(e^S) \qquad \forall e^V \in E^V : P = \{1,\ldots,k\}$$

4.2. Recuperação Oportunística de Carga

Uma contribuição chave do presente trabalho é o que cunhamos de **recuperação oportunística**. Ao invés de reservar recursos sobressalentes, a capacidade perdida após um ataque de DoS bem sucedido é redistribuída sobre a banda disponível nos caminhos remanescentes dos enlaces virtuais afetados (denominados de *caminhos ativos*).

Quando um enlace físico torna-se inacessível, a capacidade dos enlaces virtuais sobrepostos é totalmente ou parcialmente comprometida. Caso determinado enlace virtual seja parcialmente afetado, ele ainda possuirá um conjunto de caminhos ativos no substrato. Dessa forma, é possível utilizar qualquer banda disponível nesses caminhos para tentar recuperar a capacidade do enlace virtual. A formulação da estratégia de recuperação é dada conforme segue:

 ©2012 SBC — Soc. Bras. de Computação

Variável:

- $Q_{p,e^V} \in \mathbb{R}$ no intervalo $[0;1]$: indica a taxa de fluxo do enlace virtual $e^V \in \dot{E}^V$ utilizada no caminho p. Essa taxa é relativa apenas ao fluxo afetado, visto que o restante do fluxo do enlace virtual não é redistribuído.

Entrada:

- $\dot{E}^S \subset E^S$: conjunto de enlaces físicos disponíveis após a disrupção.
- P_{e^V}: conjunto de caminhos ativos para cada enlace virtual após a disrupção.
- $P_{p,e^S,e^V} \in \mathbb{B}$: indica que o enlace físico e^S está sendo utilizado pelo caminho ativo p do enlace virtual e^V.
- $\dot{E}^V \subset E^V$: indica o conjunto de enlaces virtuais afetados.

Objetivo: *maximizar a capacidade de recuperação após uma disrupção.* Dessa forma, a função

$$\max T = \sum_{\forall e^V \in E^V} \sum_{\forall p \in P_{e^V}} Q_{p,e^V} \tag{16}$$

visa realocar todo o tráfego afetado sobre o conjunto de caminhos ativos.

Restrições:

$$\sum_{\forall p \in P_{e^V}} Q_{p,e^V} \leq F_{e^V} \qquad \forall e^V \in \dot{E}^V \tag{17}$$

$$\sum_{\forall e^V \in E^V} \sum_{\forall p \in P_{e^V}} P_{p,e^S,e^V} \cdot Q_{p,e^V} \cdot b(e^V) \leq b(e^S) \qquad \forall e^S \in \dot{E}^S \tag{18}$$

A primeira restrição (17) impede que o modelo aloque mais banda do que o necessário (ou seja, somente aquela afetada pelo ataque). A segunda restrição (18) assegura que as capacidades de banda dos enlaces físicos serão respeitadas.

5. Avaliação

Os principais objetivos das estratégias descritas na seção anterior são (i) prevenir ataques de disrupção, alocando redes virtuais com múltiplos caminhos e de forma eficiente, e (ii) reagir perante ataques, realocando a capacidade comprometida em outros enlaces (quando possível). Esta seção avalia a abordagem proposta através da quantidade de enlaces virtuais afetados por ataques, com e sem proteção, e da quantidade de requisições aceitas na alocação determinada pela abordagem. Além disso, avalia-se o tempo necessário para realizar a alocação ótima de redes virtuais.

A formulação matemática descrita nas seções anteriores foi implementada no software CPLEX 12.3. Esse software utiliza variações do algoritmo Simplex e da técnica de *Branch-and-Bound* para encontrar a solução ótima dentro de determinada margem de erro (ou distância para a solução ótima). Todos os experimentos foram executados em um Intel Core i7 com 8 núcleos de 2,93 GHz e 8GB de memória ram. As condições dos experimentos e seus parâmetros são descritos a seguir.

5.1. Configuração dos Experimentos

Durante os experimentos o tempo foi discretizado, organizado em rodadas. Cada rodada pode receber uma ou mais requisições e executar o algoritmo de alocação para cada uma delas. Ademais, caso ocorra um evento de ataque, o algoritmo de recuperação também é executado. A rodada é encerrada somente após a conclusão de todas as etapas pertinentes à alocação e/ou recuperação.

 ©2012 SBC — Soc. Bras. de Computação

As topologias de rede dos experimentos foram geradas sinteticamente utilizando o *software* BRITE com o modelo de redes Barabási-Albert (BA-2). As configurações das redes e da carga de trabalho são similares às definidas em trabalhos anteriores [Chowdhury *et al* 2009, Cheng *et al* 2012].

Substrato. A rede física é composta por 30 nós e 114 enlaces em uma grade de 60x60. As capacidades de processamento dos nós e de largura de banda dos enlaces são uniformemente distribuídas no intervalo [50,100][2]. O atraso dos enlaces é diretamente proporcional à distância entre os nós, conforme gerado pelo BRITE, normalizados para o maior valor (ou seja, em intervalos entre 0 e 1).

Redes virtuais. O número de nós de uma requisição de criação de rede virtual é gerado uniformemente entre 2 e 4. Conforme será discutido ao final da Subseção 5.2, o uso de valores assim baixos foi necessário para viabilizar a realização do conjunto de experimentos, visto que a etapa de alocação demanda muito tempo de processamento e memória. A capacidade dos nós e enlaces é uniformemente distribuída nos intervalos [5,20] e [50,100], respectivamente. Essas configurações de capacidade foram escolhidas de modo que um único atributo não seja o principal fator de impacto nos experimentos.

Cargas de trabalho. A carga de trabalho é composta por requisições de redes virtuais e por ataques de negação de serviço às mesmas via disrupção da rede física. A chegada de requisições é dada por um processo de Poisson com média de 7 para cada 100 rodadas. A duração de cada rede virtual segue uma distribuição geométrica com média de 1000 rodadas. Por sua vez, os ataques são modelados por um processo de Poisson com média de 1 para cada 100 rodadas. Conforme mencionado anteriormente (Seção 3.1), cada ataque é lançado contra o nó que possui a maior alocação de largura de banda em seus enlaces.

Os experimentos executaram durante 5000 rodadas. Dessa forma, durante cada experimento foram geradas, em média, 350 requisições e 50 ataques. Por fim, a margem de erro do CPLEX foi definida para 1%, de modo que soluções fossem encontradas em tempo factível.

5.2. Avaliação dos Resultados

As estratégias propostas ajudam a evitar o impacto de ataques. A abordagem proposta divide-se em duas estratégias: mapeamento em múltiplos caminhos (preventiva) e recuperação da capacidade perdida (reativa). A Fig. 1 ilustra o efeito da disrupção da rede física com e sem o uso das estratégias, em ambos os casos tendo os parâmetros w_{Ξ}, w_{Φ} e w_{Δ} fixados em $1/3$ (de modo que seu somatório seja 1). Os eixos x e y representam respectivamente o número de caminhos a ser usado entre dois nós e a perda média de largura de banda (proporcional) para cada enlace virtual causada pelo ataque. Intuitivamente, um número maior de caminhos deve tornar a rede mais resiliente, e quanto menor a barra, melhor.

No caso padrão, sem a abordagem proposta, há apenas 1 caminho por enlace virtual. Neste caso, quando ocorre um ataque, toda a banda alocada para os enlaces virtuais afetados é perdida e o mesmo fica completamente inoperante. Com o incremento no número de caminhos é possível utilizar as duas estratégias propostas para

[2]Em linha com trabalhos similares, mantém-se unidade no nível abstrato; a mesma poderia representar Mbps no caso de enlaces ou número de fatias de tempo no caso de nós.

 ©2012 SBC — Soc. Bras. de Computação

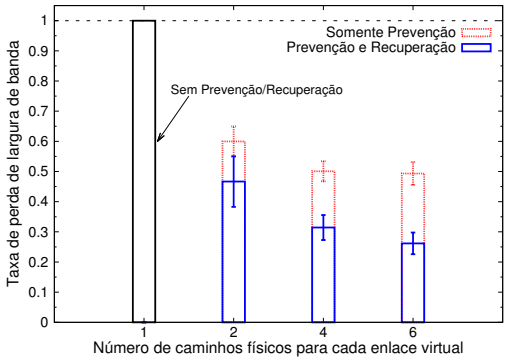


Figura 1. Perda e recuperação da largura de banda para cenários com 1, 2, 4 e 6 caminhos por enlace virtual. Neste experimento, $w_\Xi = w_\Phi = w_\Delta = 1/3$.

mitigar o efeito de ataques. O comportamento da estratégia preventiva é representado pelas barras vermelhas (contorno tracejado), enquanto o comportamento das duas estratégias em conjunto é representado pelas barras azuis (contorno contínuo). Considerando o cenário com 6 caminhos por enlace virtual, é possível perceber que a estratégia preventiva consegue proteger, em média, 50% da capacidade do enlace. Por sua vez, a utilização posterior da estratégia reativa para recuperar a capacidade comprometida reduz a perda para aproximadamente 25%. Como esperado, a abordagem proposta tem melhor resultado quando ambas as estratégias são utilizadas. Ademais, apesar da eficiência das estratégias aumentar com o número de caminhos utilizados, observa-se que seu comportamento não é linear. Tal é explicado pelas limitações na quantidade de caminhos disjuntos do substrato conforme evidenciado a seguir.

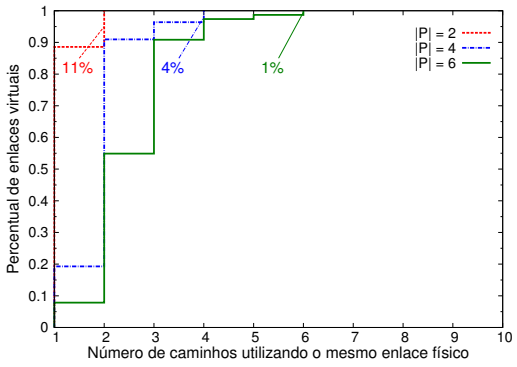
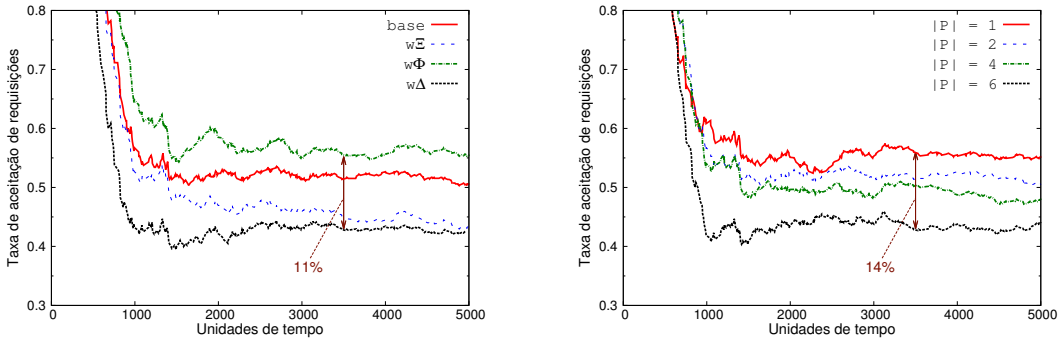


Figura 2. Nível de compartilhamento de enlaces físicos pelos caminhos alocados aos enlaces virtuais.

A alocação em múltiplos caminhos reduz a severidade de ataques a pontos críticos. Define-se um "ponto crítico" como um recurso, seja ele nó ou caminho, que por uma circunstância da rede física e/ou da alocação, acaba por concentrar toda a capacidade de um enlace virtual. Um ataque a um ponto crítico pode comprometer um ou mais enlaces virtuais por completo. A Função de Distribuição Acumulada (*Cumulative Distribution Function* – CDF) apresentada na Fig. 2 permite avaliar

 ©2012 SBC — Soc. Bras. de Computação

a quantidade de enlaces virtuais suscetíveis a esse tipo de ataque. O eixo x indica quantos caminhos de um mesmo enlace virtual utilizam determinado enlace físico (ou seja, quando for 1 não existe compartilhamento). Considerando dois caminhos por enlace virtual ($|P| = 2$), aproximadamente 11% desses enlaces possuem ambos os caminhos compartilhando o mesmo enlace físico. Ao incrementar o número de caminhos, a quantidade de enlaces virtuais suscetíveis ao ataque cai para 4% ($|P| = 4$) e então para 1% ($|P| = 6$). Por outro lado, é possível perceber que o número de caminhos disjuntos também decresce. A importância de tais caminhos está no fato de que se dois ou mais caminhos compartilham algum enlace físico, a eficiência da recuperação fica limitada à capacidade do mesmo. Quando os enlaces virtuais são mapeados em dois caminhos, 89% deles possuem caminhos disjuntos. Esse número decresce para 7% quando são usados 6 caminhos por enlace virtual. Tal evidência corrobora a afirmação anterior de que a quantidade de caminhos disjuntos no substrato pode afetar o desempenho da abordagem proposta.



(a) Número de caminhos por enlace virtual ($|P|$) fixado em 2

(b) Parâmetros $w_\Xi = w_\Phi = w_\Delta = 1/3$

Figura 3. Taxa de aceitação de acordo com a variação (a) dos parâmetros w_Ξ, w_Φ e w_Δ e (b) no número de caminhos por enlace virtual.

O custo da solução é diretamente proporcional ao nível de resiliência contra disrupção. A Fig. 3 ilustra as diferenças na taxa de aceitação de redes virtuais para diferentes parâmetros de entrada ao longo do tempo, com a taxa de aceitação sendo representada no eixo y. Em um primeiro momento ($0 \sim 900$), as requisições de rede virtual encontram um substrato ocioso com ampla disponibilidade de recursos. À medida que os recursos vão ficando escassos ($900 \sim 2000$), a taxa de aceitação diminui. Por fim, o substrato alcança estabilidade ($2000 \sim \infty$) quando a quantidade de recursos liberados pelas redes virtuais extintas é similar à quantidade demandada pelas novas requisições e 40 a 60% são aceitas. A Fig. 3(a) demonstra a diferença na taxa de aceitação causada pela escolha de prioridades distintas na alocação. O caso base (primeira curva da legenda e segunda de cima para baixo) foi utilizado para verificar a importância relativa de cada parâmetro. O aumento na *priorização por caminhos disjuntos* (parâmetro $w\Xi$, segunda curva na legenda e terceira de cima para baixo) provoca uma sobrecarga na alocação de recursos do substrato e diminui a taxa de aceitação. Tal se deve ao algoritmo de alocação, que opta por caminhos maiores para evitar a sobreposição de enlaces físicos. A escolha por *enlaces menos saturados* (parâmetro $w\Phi$) ou pela *minimização do atraso diferencial* (parâmetro $w\Delta$) acarretaram respectivamente na melhor e pior taxas de aceitação (com uma diferença de aproximadamente 11%). O aumento de $w\Phi$ ajuda a evitar a formação de gargalos, deixando o acesso mais livre aos nós da rede. Por outro lado, o aumento

 ©2012 SBC — Soc. Bras. de Computação

de $w\Delta$ prioriza a escolha de caminhos maiores com atrasos similares, ao invés de caminhos menores com maior diferença nos atrasos.

A Fig. 3(b) demonstra a eficiência do algoritmo de alocação ao longo do tempo com a variação no número de caminhos por enlace virtual. Apesar de possibilitar maior granularidade na alocação, o aumento no número de caminhos pode resultar em alocações piores. No pior caso, ao considerar 6 caminhos por enlace virtual, a taxa de aceitação decresce 14%. Isso ocorre porque ao considerar somente um único caminho, os efeitos colaterais causados pela priorização de caminhos disjuntos Ξ e pela minimização do atraso diferencial Δ são anulados. Dessa forma, o critério dominante na alocação passa a ser o balanceamento de carga Φ. No entanto, quanto maior for a quantidade de caminhos, maior será a importância relativa destes dois outros critérios.

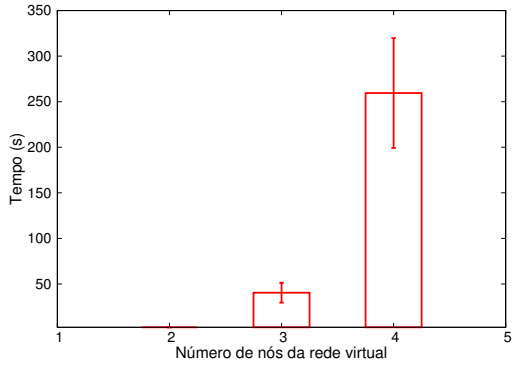


Figura 4. Tempo médio para alocar cada requisição de rede virtual.

A característica exponencial do problema de alocação justifica o estudo de heurísticas. Diversos trabalhos da literatura estudam heurísticas para lidar com o problema da alocação de redes virtuais [Chowdhury *et al* 2009, Alkmim *et al* 2011, Cheng *et al* 2012]. Sua similaridade com o *multiway separator problem* [Andersen 2002] é um forte indicio de que o problema é NP-Difícil. A Fig. 4 demonstra o tempo médio para a execução do algoritmo de alocação de redes sobre uma única requisição. Conforme pode ser observado, o problema de alocação limita a escalabilidade da solução, demandando em torno de 250s para resolver de forma ótima *uma única instância* de rede virtual com 4 nós na rede física descrita anteriormente. Dessa forma, a evolução natural deste trabalho é a definição de heurísticas para a abordagem proposta.

6. Conclusão

Apesar das potenciais vantagens de redes virtuais, como o isolamento, elas ainda estão sujeitas a ataques de negação de serviço lançados à rede física. Este trabalho apresentou uma abordagem inovadora para aumentar a proteção de redes virtuais contra ataques de DoS via rede física. Entre suas contribuições, destaca-se a que a abordagem de alocação proposta, diferentemente dos trabalhos anteriores, não precisa reservar recursos sobressalentes ou recalcular os caminhos utilizados pelos enlaces virtuais. A mesma é dividida em duas estratégias complementares. A primeira estratégia visa prevenir os ataques pelo uso de múltiplos caminhos *prioritariamente* disjuntos. A segunda visa recuperar a capacidade comprometida utilizando os caminhos ativos (ou seja, aqueles não afetados pelo ataque).

 ©2012 SBC — Soc. Bras. de Computação

Conforme discutido na seção de avaliação, a solução proposta oferece um ganho na proteção e recuperação de capacidade, ao custo de uma menor taxa de aceitação. Ademais, esse ganho é incrementalmente menor à medida que a resiliência é priorizada sobre a alocação. Portanto, é possível adequar a solução aos requisitos do ambiente, priorizando a resiliência em detrimento da alocação ou adotando uma estratégia mais conservadora, mas ainda assim mitigar os ataques de disrupção.

Quanto aos trabalhos futuros, vislumbramos a definição de heurísticas para tornar a abordagem mais rápida, possibilitando sua aplicação em cenários maiores. Ademais, estamos investigando novas estratégias para o processo de recuperação, como a migração de nós, a qual possibilitará tornar a rede ainda mais robusta a ataques de negação de serviço.

Referências

Alkmim *et al* (2011). Optimal mapping of virtual networks. In *GLOBECOM, IEEE*, pages 1–6.

Andersen, D. G. (2002). Theoretical approaches to node assignment. Unpublished manuscript. `http://www.cs.cmu.edu/~dga/papers/andersen-assign.ps`.

Belbekkouche *et al* (2012). Resource discovery and allocation in network virtualization. *Comm. Surv. Tut., IEEE*, PP(99):1–15.

Chen *et al* (2010). Resilient virtual network service provision in network virtualization environments. In *ICPADS, IEEE*, pages 51–58.

Cheng *et al* (2012). Virtual network embedding through topology awareness and optimization. *Comput. Netw.*, 56(6):1797–1813.

Chowdhury, N. M. K. and Boutaba, R. (2010). A survey of network virtualization. *Comp. Netw.*, 54(5):862–876.

Chowdhury *et al* (2009). Virtual network embedding with coordinated node and link mapping. In *INFOCOM, IEEE*, pages 783–791.

Fortz, B. and Thorup, M. (2004). Increasing internet capacity using local search. *Comput. Optim. and Applic.*, 29:13–48.

Guo *et al* (2011). Shared backup network provision for virtual network embedding. In *ICC, IEEE*, pages 1–5.

He, J. and Rexford, J. (2008). Toward internet-wide multipath routing. *Network, IEEE*, 22(2):16–21.

Houidi *et al* (2010). Adaptive virtual network provisioning. In *2nd SIGCOMM VISA workshop, ACM*, pages 41–48.

Khan *et al* (2012). Network virtualization: a hypervisor for the internet? *Comm. Mag., IEEE*, 50(1):136–143.

Medhi, D. (2006). Network restoration. In Resende, M. G. C. and Pardalos, P. M., editors, *Handbook of Optimization in Telecomm.*, pages 801–836. Springer US.

Rahman *et al* (2010). Survivable virtual network embedding. In Crovella, M. *et al.*, editor, *NETWORKING 2010*, volume 6091 of *LNCS*, pages 40–52. Springer Berlin / Heidelberg.

Yeow *et al* (2010). Designing and embedding reliable virtual infrastructures. In *2nd SIGCOMM VISA workshop, ACM*, pages 33–40.

Yu *et al* (2011). Cost efficient design of survivable virtual infrastructure to recover from facility node failures. In *ICC, IEEE*, pages 1–6.

Zhang *et al* (2010). Reliable adaptive multipath provisioning with bandwidth and differential delay constraints. In *Proc. INFOCOM, IEEE*, pages 2178–2186.

 ©2012 SBC — Soc. Bras. de Computação