Um Modelo para Mapeamento Ótimo de Redes Virtuais com Requisitos de Segurança

Leonardo Richter Bays[1], **Rodrigo Ruas Oliveira**[1], **Luciana Salete Buriol**[1], **Marinho Pilla Barcellos**[1], **Luciano Paschoal Gaspary**[1]

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brazil

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

Abstract. *Network virtualization enables the creation of multiple instances of virtual networks on top of a single physical infrastructure. Given its wide applicability, this technique has attracted a lot of interest both from academic researchers and major companies within the segment of computer networks. Although recent efforts (motivated mainly by the search for mechanisms to enable the evaluation of Future Internet proposals) have contributed substantially to materialize this concept, none of them has attempted to combine efficient resource allocation with fulfillment of security requirements (e.g., confidentiality). It is important to note that, in the context of virtual networks, the protection of shared network infrastructures constitutes a fundamental condition to enable its use in large scale. To address this problem, in this paper we propose a virtual network embedding model that aims to provide the desired level of security while optimizing physical resource usage. The results obtained demonstrate that the model is able to correctly and optimally map virtual networks to a physical substrate, minimizing bandwidth costs for infrastructure providers.*

Resumo. *A virtualização de redes permite a criação de múltiplas instâncias de redes virtuais sobre uma única infraestrutura física. Devido à sua ampla aplicabilidade, tal técnica tem atraído grande interesse tanto de pesquisadores quanto de empresas importantes do segmento de redes de computadores. Apesar de esforços recentes (motivados principalmente pela busca de mecanismos para viabilizar a avaliação de propostas na temática Internet do Futuro) terem contribuído substancialmente para a materialização do conceito, nenhum preocupou-se em conciliar alocação eficiente de recursos e satisfação de requisitos de segurança (ex: confidencialidade). Ressalta-se que, no contexto de redes virtuais, a proteção de infraestruturas de rede compartilhadas constitui condição fundamental para seu uso em larga escala. Para abordar o referido problema, neste artigo propõe-se um modelo de alocação de redes virtuais que busca satisfazer o nível especificado de segurança e, ao mesmo tempo, otimizar a utilização dos recursos físicos. Os resultados obtidos demonstram que o modelo é capaz de alocar redes virtuais a um substrato físico de forma correta e ótima, minimizando custos de largura de banda para provedores de infraestrutura.*

1. Introdução

Nos últimos anos, têm surgido demandas cada vez maiores por serviços de rede específicos, com requisitos peculiares e distintos. Motivados por tais demandas, e estimulados pelo sucesso no emprego de virtualização para hospedagem de servidores personalizados, pesquisadores passaram a explorar o uso dessa técnica em infraestruturas de

rede. A virtualização de redes permite a criação de múltiplas topologias virtuais sobre um mesmo substrato físico. Isso é possível por meio da instanciação de um ou mais roteadores virtuais em dispositivos físicos e do estabelecimento de enlaces virtuais entre esses roteadores, formando topologias arbitrárias.

Entre outras vantagens, o uso de virtualização de redes permite a um provedor de infraestrutura acomodar simultaneamente múltiplas pilhas de protocolo no mesmo substrato. Isso possibilita a criação de infraestruturas de rede adaptadas às necessidades de aplicações de rede específicas [Fernandes et al. 2010]. Ademais, essa técnica pode ser usada para a execução de experimentos sem interferir com tráfego de produção, em escala e com um alto grau de similaridade com infraestruturas reais. Dessa forma, é possível criar ambientes favoráveis ao desenvolvimento e avaliação de novas arquiteturas e protocolos, o que pode contribuir para o avanço de pesquisas relacionadas à Internet do Futuro [Anderson et al. 2005].

A virtualização de redes também tem recebido grande apoio no mercado. Empresas importantes passaram a oferecer dispositivos com suporte nativo à virtualização. Essa nova funcionalidade permite que provedores de infraestrutura passem também a oferecer novos serviços. O suporte de grandes nomes da indústria a esse tipo de iniciativa pode ser observado, por exemplo, na lista de membros da *Open Networking Foundation*[1], que promove o desenvolvimento e o uso de redes virtualizadas definidas por software.

Apesar de sua ampla aplicabilidade, manter um ambiente de virtualização de redes requer uma distribuição adequada dos recursos. Por um lado, há provedores de infraestrutura, que desejam obter o máximo de lucro hospedando a maior quantidade possível de redes virtuais, minimizando seus custos. Por outro, há uma série de clientes que solicitam redes virtuais com demandas de recursos específicas. O método de alocação deve garantir que os recursos requisitados estarão disponíveis para esses clientes e, ao mesmo tempo, minimizar os custos do provedor de infraestrutura. Além disso, o resultado do processo de mapeamento deve ser entregue em um tempo aceitável.

Outra grande preocupação que surge com o uso compartilhado de dispositivos de roteamento e canais de comunicação é a segurança. Sem a proteção adequada, é possível que usuários de uma rede virtual capturem ou até mesmo adulterem dados de outras redes virtuais no mesmo substrato. Tais ações violariam propriedades de segurança tais como confidencialidade e integridade. Portanto, é de grande importância que arquiteturas de virtualização ofereçam proteção contra essas e outras ameaças que possam comprometer sua segurança.

Para viabilizar o uso de virtualização em ambientes reais, tanto alocação eficiente de recursos quanto segurança devem ser levados em consideração. O problema da alocação de recursos é considerado *NP-hard* devido a sua similaridade com o *multi-way separator problem* [Andersen 2002], e tem sido geralmente abordado na literatura com algoritmos de alocação modelados por meio de programação linear. Há uma série de trabalhos focando no problema da alocação de recursos de redes virtuais [Yu et al. 2008, Chowdhury et al. 2009, Alkmim et al. 2011, Cheng et al. 2011, Davy et al. 2011]. No entanto, os autores deste artigo desconhecem propostas que levam em consideração requisitos de segurança. Para preencher essa lacuna, no presente artigo é proposto um modelo de alocação de redes virtuais que otimiza a utilização de recursos físicos ao mesmo tempo em que atende requisitos de segurança. Além de requisitos de capacidade e

[1] http://www.opennetworking.org/membership

localização, solicitantes de redes virtuais podem especificar requisitos de segurança para suas redes, que devem ser atendidos pelo provedor de infraestrutura. O modelo proposto recebe requisições de forma *on-line* e determina a melhor alocação possível em termos de utilização de recursos, considerando todos os requisitos de segurança dos solicitantes.

O restante deste artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados às áreas de mapeamento de recursos e segurança em redes virtuais. Na seção 3 é descrito o modelo proposto e sua formulação. A Seção 4 relata a avaliação realizada e apresenta os resultados obtidos. Por fim, na Seção 5 são apresentadas as considerações finais e perspectivas para trabalhos futuros.

2. Trabalhos Relacionados

Nessa seção, serão apresentados os trabalhos relacionados focando no mapeamento de redes virtuais, bem como algumas das principais propostas visando prover segurança a redes virtuais. Cada trabalho será descrito brevemente, ressaltando suas principais características.

Yu et al. [Yu et al. 2008] propõem um modelo de alocação de redes virtuais com suporte à separação de caminhos (fragmentação de enlaces virtuais por múltiplos caminhos do substrato físico) e migração. O modelo proposto aproveita-se do ganho em flexibilitade obtido pela separação de enlaces virtuais em múltiplos caminhos (caso tal separação seja permitida pelo solicitante), reduzindo o tempo necessário para completar o processo de mapeamento. Além disso, o substrato é capaz de reotimizar sua utilização de recursos periodicamente por meio da migração de roteadores e enlaces virtuais previamente alocados. O modelo considera que requisições de redes virtuais não são conhecidas *a priori*, e leva em consideração requisitos de CPU e largura de banda, bem como o tempo máximo que uma requisição pode aguardar antes de ser atendida.

Outro modelo, formulado por Chowdhury et al. [Chowdhury et al. 2009], visa aprimorar a coordenação entre a alocação de roteadores e enlaces, que é realizada em duas fases separadas. Isso é feito por meio da pré-seleção de alocações de roteadores de forma a auxiliar o estágio de mapeamento de enlaces. Assim como o modelo previamente mencionado, esse também permite a separação de caminhos, e considera requisitos de CPU e largura de banda. Requisições de redes virtuais são alocadas de forma *on-line*, e podem especificar as localizações físicas em que certos roteadores virtuais devem ser mapeados.

O modelo desenvolvido por Alkmim et al. [Alkmim et al. 2011] estende os trabalhos anteriores combinando requisitos de capacidade com restrições relacionadas à transferência de imagens utilizadas nos roteadores virtuais. O modelo visa minimizar o tempo necessário para transferir tais imagens, ao mesmo tempo que considera requisitos de CPU, memória, banda e localização. Como nos trabalhos anteriores, requisições são recebidas e alocadas de forma *on-line*.

Cheng et al. [Cheng et al. 2011] apresentam uma abordagem baseada na classificação de nós (*node ranking*), que considera tanto a capacidade de roteadores e enlaces quanto as capacidades de seus vizinhos. Por exemplo, a classificação de roteadores físicos é afetada não só por sua própria capacidade, mas também pela capacidade disponível em outros roteadores conectados ao mesmo. De forma análoga, a classificação de roteadores e enlaces virtuais também leva em consideração as características de seus vizinhos. O processo de mapeamento aloca roteadores e enlaces virtuais a elementos da

rede física com classificações similares. Tal estratégia, segundo os autores, tende a reduzir possíveis gargalos criados pela alocação de redes virtuais.

Ao contrário das propostas apresentadas anteriormente, o modelo proposto por Davy et al. [Davy et al. 2011] não recebe como entrada uma topologia de rede completa. Em vez disso, requisições contêm apenas os *end points* que devem ser interconectados (uma origem e um ou mais destinos). A solução constrói redes virtuais em forma de árvore, partindo da localização de origem até os destinos requisitados. Além de restrições de localização, o modelo também considera a preferência dos solicitantes por redes de baixo custo, ou redes com menor atraso e custo maior. As redes virtuais são então instanciadas, obedecendo os requisitos previamente mencionados e visando minimizar os custos do provedor de infraestrutura.

Apresentados e discutidos os principais trabalhos relacionados à alocação de recursos, passa-se, agora, a uma síntese das investigações que buscam oferecer segurança em redes virtualizadas. Cabuk et al. [Cabuk et al. 2007] apresentam um arcabouço para criação de redes virtuais seguras. Os autores utilizam "Domínios Virtuais Confiáveis" (*Trusted Virtual Domains* – TVDs) para prover controle de acesso, confidencialidade e integridade a comunicações de rede. Cada TVD representa um domínio isolado, composto de entidades virtuais e de enlaces entre as mesmas. Certificados digitais são usados para assegurar que somente entidades que satisfaçam um determinado conjunto de condições sejam capazes de participar de um TVD. Os autores usam VLANs para isolar o tráfego dentro de cada rede confiável, e VPNs para interconectar tais redes.

Huang et al. [Huang et al. 2010] propõem um método que lança mão de criptografia para proteger informações de roteamento, bem como caminhos variáveis para mitigar ataques de análise de tráfego. Tal método classifica roteadores em diferentes grupos, e distribui chaves de grupo para cada roteador. Dessa forma, somente roteadores pertencentes a um determinado grupo são capazes de acessar as informações protegidas de tal grupo. Além disso, cada enlace virtual é mapeado a múltiplos caminhos físicos. Fluxos transmitidos por tais enlaces são divididos aleatoriamente entre os caminhos físicos disponíveis, visando evitar análise de tráfego.

Ao mesmo tempo em que há trabalhos focando no problema de alocação de redes virtuais, há outros visando oferecer serviços de segurança a ambientes de redes virtuais. No entanto, os autores deste artigo desconhecem trabalhos que abordem ambas as áreas simultaneamente. Ao não considerarem segurança, um aspecto essencial em ambientes de virtualização de redes devido ao compartilhamento de recursos físicos, os trabalhos anteriores na área de alocação de redes virtuais acabam por subestimar a quantidade de recursos necessária para acomodar tais redes. Nesse contexto, busca-se, neste artigo, suprir tal lacuna, ao propor uma solução que concilia alocação eficiente de recursos com satisfação de requisitos de segurança, fatores fundamentais para ampla adoção de redes virtuais em ambientes de produção.

3. Modelo Proposto

Para abordar o problema da otimização do uso de recursos considerando requisitos de segurança, foi desenvolvido um modelo por meio de Programação Linear Inteira. Para criar um modelo que represente o cenário de alocação de redes virtuais com um nível desejável de fidelidade, diversos detalhes foram levados em consideração. Vislumbra-se um cenário em que um provedor de infraestrutura fornece redes virtuais a diversos clientes. Para solicitar a criação de uma rede virtual, clientes devem firmar um Acordo de

Nível de Serviço (*Service Level Agreement* – SLA) com o provedor de infraestrutura. Tal SLA descreve as características da rede virtual solicitada e seus requisitos de segurança, que devem ser atendidos pelo provedor.

Assume-se que um provedor de infraestrutura receberá uma série de requisições de redes virtuais ao longo do tempo. Portanto, tais requisições devem ser tratadas de forma *on-line*, isto é, uma a uma conforme são recebidas. Caso haja recursos suficientes no substrato para que a alocação seja possível, a saída do modelo deve indicar a melhor alocação em termos de utilização de recursos, maximizando os recursos disponíveis para futuras requisições. Caso não haja recursos suficientes para alocar uma rede virtual, a requisição é negada.

Antes de apresentar o modelo proposto, será descrita a sintaxe usada na sua formulação. Letras maiúsculas são usadas para representar conjuntos ou variáveis. Letras sobrescritas indicam se um conjunto refere-se a recursos virtuais (V) ou físicos (P), ou se o mesmo se refere a roteadores (R) ou enlaces (L). Ademais, letras subscritas representam índices associados a variáveis.

Topologias. Requisições de redes virtuais devem especificar a topologia desejada, isto é, o número de roteadores virtuais na rede e as interconexões entre os mesmos. Cada topologia de rede virtual, bem como a topologia da rede física, é representada como um grafo direcionado $N = (R, L)$, no qual os vértices R e as arestas L representam, respectivamente, roteadores e enlaces. Além disso, um enlace entre dois roteadores a e b é representado por um par de arestas simétricas com direções opostas, (a, b) e (b, a). Roteadores virtuais são mapeados a exatamente um roteador físico, enquanto que enlaces virtuais podem ser mapeados a um único enlace físico ou a um caminho composto por dois ou mais enlaces físicos.

Capacidades físicas e virtuais. Roteadores físicos possuem capacidades limitadas de CPU e memória, expressas por C_i^P e M_i^P, respectivamente (em que i é o índice do roteador). Por sua vez, enlaces possuem capacidade de banda limitada $B_{i,j}^P$, em que o par (i, j) representa um enlace físico entre i e j. De forma similar, $C_{r,i}^V$ e $M_{r,i}^V$ representam os requisitos de CPU e memória de um roteador virtual de uma rede r. Além disso, $B_{r,i,j}^V$ representa o requisito de largura de banda de um enlace virtual entre os roteadores virtuais i e j de uma rede r. Os requisitos desses elementos virtuais definem a parcela dos recursos físicos que deve ser alocada para seu consumo. Presume-se que a arquitetura de virtualização é capaz de isolar adequadamente os recursos físicos, garantindo o cumprimento desses limites.

Localidades. Assume-se que a maioria dos clientes requisitará redes virtuais fixando um ou mais pontos onde roteadores virtuais deverão ser hospedados. Portanto, cada roteador físico está associado a um identificador de localização S^P, e requisições de redes virtuais podem ou não requerer que alguns de seus roteadores sejam mapeados a roteadores físicos em localidades específicas. Roteadores virtuais com requisitos de localidade são armazenados no conjunto S^V.

Segurança. O modelo também permite que cada requisição de rede virtual possua requisitos de segurança associados. O oferecimento de serviços de confidencialidade visa tratar preocupações relacionadas ao uso compartilhado de roteadores físicos e canais de comunicação, o que pode fazer com que dados sensíveis sejam expostos a terceiros. Tais requisitos, se presentes, indicam um de três níveis distintos de confidencialidade que devem ser fornecidos às comunicações dessas redes:

- Criptografia fim-a-fim: caso esse nível de confidencialidade seja solicitado, os roteadores de borda da rede virtual devem ser hospedados em roteadores físicos que suportam tal característica. Na prática isso significa que esses roteadores físicos devem dar suporte a suítes de protocolos tais como IPSec [Kent and Seo 2005], que fornece criptografia fim-a-fim quando usado em *modo de transporte*.
- Criptografia ponto-a-ponto: nesse nível de confidencialidade, pacotes inteiros são criptografados, protegendo não só os dados contidos nos mesmos mas também seu cabeçalho. Isso significa que pacotes precisam ser decriptografados e recriptografados em cada salto para serem roteados adequadamente. Portanto, cada roteador em uma rede virtual que requer esse nível de confidencialidade deve ser mapeado a um roteador físico capaz de dar suporte a tais operações. Esse nível corresponde ao *modo de túnel* do IPSec, o que significa que roteadores físicos com suporte a esse protocolo são capazes de prover tal característica.
- Não-sobreposição de redes: uma requisição de rede virtual pode também exigir que seus roteadores e enlaces virtuais não compartilhem roteadores nem caminhos físicos com uma ou mais redes virtuais. Tal caso extremo pode ser usado, por exemplo, para proteger informações altamente sigilosas de empresas concorrentes.

Para prover os dois primeiros níveis de segurança, requisições de redes virtuais devem ser capazes de indicar quais de seus roteadores devem ser capazes de criptografar e decriptografar pacotes de rede, caso desejado. Portanto, o modelo também incorpora os conjuntos K_i^P e $K_{r,i}^V$, que indicam se um roteador físico é capaz de oferecer tal característica, e se um roteador virtual a requer.

Já quanto ao terceiro nível, requisições devem ser capazes de especificar o conjunto de redes virtuais com o qual roteadores e enlaces físicos não serão compartilhados. Para oferecer tal nível, é usado o conjunto X. Esse conjunto é composto por pares de redes virtuais que não devem compartilhar recursos do substrato (por exemplo, se $(i, j) \in X$, não é permitido que as redes virtuais i e j compartilhem recursos).

Alocação prévia. Por fim, os conjuntos $E_{i,r,j}^R$ e $E_{i,j,r,k,l}^L$ indicam onde encontram-se alocados, respectivamente, os roteadores e enlaces das redes virtuais já alocadas no substrato. Caso não haja nenhuma rede virtual alocada no momento em que uma requisição é recebida, tais conjuntos estarão vazios. A seguir, para maior clareza, apresenta-se um sumário das entradas do modelo proposto.

- $N^P = \{R^P, L^P\}$ – Representa a rede física, composta por um conjunto de roteadores físicos R^P e um conjunto de enlaces físicos L^P.
- $N^V = \{R^V, L^V\}$ – Representa uma requisição de rede virtual, composta por um conjunto de roteadores virtuais R^V e um conjunto de enlaces virtuais L^V.
- $X \in N^V \times N^V$ – Conjunto de redes virtuais conflitantes. Representa redes virtuais que não devem ser mapeadas aos mesmos elementos do substrato físico.
- $S \in \mathbb{N}$ – Conjunto de todas as possíveis localidades físicas onde roteadores físicos podem residir, representadas por números naturais.
- $S^P \in R^P \times S$ – Indica a localização de roteadores da rede física.
- $S^V \in R^V \times S$ – Indica requisitos de localização de roteadores em requisições de redes virtuais.
- $C_i^P \in \mathbb{N}$ – Indica a capacidade total de CPU de um roteador físico i.
- $M_i^P \in \mathbb{N}$ – Indica a capacidade total de memória de um roteador físico i.
- $B_{i,j}^P \in \mathbb{N}$ – Indica a largura de banda de um enlace físico (i, j).

- $K_i^P \in \{0,1\}$ – Indica se um roteador físico i suporta protocolos que o permitam criptografar e decriptografar pacotes de rede. Se um roteador físico é capaz de dar suporte a tais protocolos, o valor é definido como 1; caso contrário, é definido como 0.
- $C_{r,i}^V \in \mathbb{N}$ – Indica a capacidade de CPU exigida por um roteador virtual i de uma rede virtual r.
- $M_{r,i}^V \in \mathbb{N}$ – Indica a capacidade de memória necessária a um roteador virtual i de uma rede virtual r.
- $B_{r,i,j}^V \in \mathbb{N}$ – Indica a largura de banda exigida por um enlace virtual (i,j) de uma rede virtual r.
- $K_{r,i}^V \in \{0,1\}$ – Indica se um roteador virtual i de uma rede virtual r deve ser capaz de criptografar e decriptografar pacotes de rede. Se um roteador virtual requer tal característica, o valor é definido como 1; caso contrário, é definido como 0.
- $E_{i,r,j}^R \in \{0,1\}$ – Indica se um roteador virtual j de uma rede virtual r previamente recebida encontra-se alocado no roteador físico i. Em caso positivo, assume o valor 1; caso contrário, assume o valor 0.
- $E_{i,j,r,k,l}^L \in \{0,1\}$ – Indica se um enlace virtual (k,l) de uma rede virtual r previamente recebida encontra-se alocado no enlace físico (i,j). Em caso positivo, assume o valor 1; caso contrário, assume o valor 0.

De forma similar, as variáveis de saída do modelo proposto são apresentadas a seguir. Os valores retornados por tais variáveis indicam a alocação de elementos virtuais no substrato físico, representando a solução do problema. Uma vez que o problema é solucionado, cada roteador virtual estará mapeado a um único roteador físico, e cada enlace virtual estará mapeado a um caminho no substrato físico. Tal caminho pode ser um único enlace físico, ou uma série de enlaces físicos consecutivos.

- $A_{i,r,j}^R \in \{0,1\}$ – Alocação de roteadores, indica se o roteador físico i está hospedando o roteador virtual j da rede virtual r.
- $A_{i,j,r,k,l}^L \in \{0,1\}$ – Alocação de enlaces, indica se o enlace físico (i,j) está hospedando o enlace virtual (k,l) da rede virtual r.

Por fim, é apresentada a função objetivo do modelo e suas restrições. A função objetivo visa minimizar a largura de banda física consumida pelos enlaces virtuais nas redes solicitadas, dessa forma minimizando custos e preservando largura de banda para alocações futuras. Por sua vez, as restrições garantem que os requisitos serão atendidos, e que as capacidades físicas não serão excedidas.

Objetivo:

$$min \sum_{(i,j)\in L^P} \sum_{r\in N^V,(k,l)\in L^V} A_{i,j,r,k,l}^L B_{r,k,l}^V$$

Sujeito a:

$$\sum_{r\in N^V, j\in R^V} C_{r,j}^V A_{i,r,j}^R \leq C_i^P \qquad \forall i \in R^P \quad \text{(R1)}$$

$$\sum_{r\in N^V, j\in R^V} M_{r,j}^V A_{i,r,j}^R \leq M_i^P \qquad \forall i \in R^P \quad \text{(R2)}$$

$$\sum_{r \in N^V, (k,l) \in L^V} B^V_{r,k,l} A^L_{i,j,r,k,l} \leq B^P_{i,j} \qquad \forall (i,j) \in L^P \quad \text{(R3)}$$

$$K^V_{r,j} A^R_{i,r,j} \leq K^P_i \qquad \forall i \in R^P, r \in N^V, j \in R^V \quad \text{(R4)}$$

$$\sum_{i \in R^P} A^R_{i,r,j} = 1 \qquad \forall r \in N^V, j \in R^V \quad \text{(R5)}$$

$$\sum_{j \in R^P} A^L_{i,j,r,k,l} - \sum_{j \in R^P} A^L_{j,i,r,k,l} = A^R_{i,r,k} - A^R_{i,r,l} \qquad \forall r \in N^V, (k,l) \in L^V, i \in R^P \quad \text{(R6)}$$

$$\sum_{q \in N^V, k \in R^V} A^R_{i,q,k} + \sum_{r \in N^V, l \in R^V} A^R_{i,r,l} \leq 1 \qquad \forall q, r \in X, i \in R^P \quad \text{(R7)}$$

$$\sum_{q \in N^V, (k,l) \in L^V} A^L_{i,j,q,k,l} + \sum_{r \in N^V, (o,p) \in L^V} A^L_{i,j,r,o,p} \leq 1 \qquad \forall q, r \in X, (i,j) \in L^P \quad \text{(R8)}$$

$$j A^R_{i,r,k} = l A^R_{i,r,k} \qquad \forall (i,j) \in S^P, r \in N^V, (k,l) \in S^V \quad \text{(R9)}$$

$$A^R_{i,r,j} = E^R_{i,r,j} \qquad \forall (i,r,j) \in E^R \quad \text{(R10)}$$

$$A^L_{i,j,r,k,l} = E^L_{i,j,r,k,l} \qquad \forall (i,j,r,k,l) \in E^L \quad \text{(R11)}$$

$$\sum_{j \in R^V} A^R_{i,r,j} \leq 1 \qquad \forall i \in R^P, r \in N^V \quad \text{(R12)}$$

As primeiras três restrições garantem que os requisitos de capacidade dos roteadores e enlaces virtuais serão atendidos. A restrição R1 garante que a quantidade de CPU requisitada por roteadores virtuais mapeados a um roteador físico não excederá sua capacidade máxima. A restrição R2 aplica o mesmo controle à capacidade de memória dos roteadores físicos, e a restrição R3, à largura de banda dos enlaces físicos.

A restrição R4 garante que todos os roteadores virtuais que devem realizar criptografia e decriptografia de pacotes serão mapeados a roteadores físicos que suportam tais operações. Tais roteadores virtuais são os roteadores de borda no caso de redes virtuais que solicitam criptografia fim-a-fim, e todos os roteadores no caso de redes virtuais que requerem criptografia ponto-a-ponto.

A restrição R5 garante que cada roteador virtual será mapeado a um roteador físico. De forma complementar, a restrição R6 garante que o caminho formado por um conjunto de enlaces físicos hospedando um enlace virtual será válido. Em outras palavras, o caminho físico hospedando um enlace virtual (a, b) deve ser um caminho válido entre o

roteador físico hospedando o roteador virtual *a* e o roteador físico hospedando o roteador virtual *b*.

As restrições R7 e R8 referem-se a pares de redes virtuais conflitantes – isto é, redes virtuais que não podem compartilhar recursos físicos. A restrição R7 não permite que roteadores virtuais que pertencem a redes virtuais conflitantes sejam mapeados aos mesmos roteadores físicos. De forma análoga, a restrição R8 garante que enlaces virtuais dessas redes conflitantes não compartilharão quaisquer caminhos físicos.

A restrição R9 garante que todo roteador virtual que possua um requisito de localidade será mapeado a um roteador físico na localidade solicitada. As restrições R10 e R11 garantem que os elementos das redes virtuais previamente alocadas continuarão alocados aos mesmos elementos físicos. A alocação dos roteadores será mantida pela restrição R10, enquanto que a alocação dos enlaces, pela restrição R11. Por fim, a restrição R12 impede que múltiplos roteadores virtuais de uma mesma rede virtual sejam hospedados no mesmo roteador físico.

4. Avaliação

Para avaliar o modelo em Programação Linear Inteira apresentado na seção anterior, o mesmo foi implementado e executado no *CPLEX Optimization Studio*[2] versão 12.3. Os experimentos foram realizados em uma máquina com quatro processadores AMD Opteron 6276, usando no máximo quatro *threads* simultâneas. A máquina possui 64 GB de RAM e usa o sistema operacional Ubuntu GNU/Linux Server 11.10 x86_64.

4.1. Cenários

Para realizar os experimentos, foi desenvolvido um simulador capaz de gerar requisições de redes virtuais de forma aleatória. O simulador é executado por 500 janelas de tempo, e são geradas em média cinco requisições em cada uma, seguindo uma distribuição de Poisson. Cada requisição permanece alocada por, em média, cinco janelas de tempo, seguindo uma distribuição exponencial. Ressalta-se que essa forma de instanciação, isto é, o emprego de janelas de tempo e os modelos de chegada de requisições e de duração de redes virtuais na infraestrutura, é empregada em trabalhos importantes da área, com destaque para o realizado por Yu et al. [Yu et al. 2008].

A topologia da rede física e de cada rede virtual é gerada por meio da ferramenta BRITE[3], usando o modelo Barabási-Albert (BA-2) [Albert and Barabási 2000]. A rede física possui 100 roteadores, cada um com capacidade total de CPU definida como 100%, e 256 MB de memória. Além disso, os roteadores são distribuídos uniformemente entre 16 localidades, e 95% suportam protocolos que os permitem oferecer serviços de criptografia. A largura de banda dos enlaces físicos é distribuída uniformemente entre 1 e 10 Gbps.

As requisições de redes virtuais possuem entre 2 e 5 roteadores cada. Em cada rede virtual, dois roteadores (os *end points* dessa rede) possuem requisitos de localidade, gerados aleatoriamente entre as 16 localidades existentes. 35% das requisições geradas não possuem requisitos de criptografia, enquanto que 35% requerem criptografia fim-a-fim, e as demais 30%, criptografia ponto-a-ponto. De forma independente, 5% das requisições possuem conflito com uma rede já alocada no substrato.

[2]http://www-01.ibm.com/software/integration/optimization/cplex-optimization-studio/

[3]http://www.cs.bu.edu/brite/

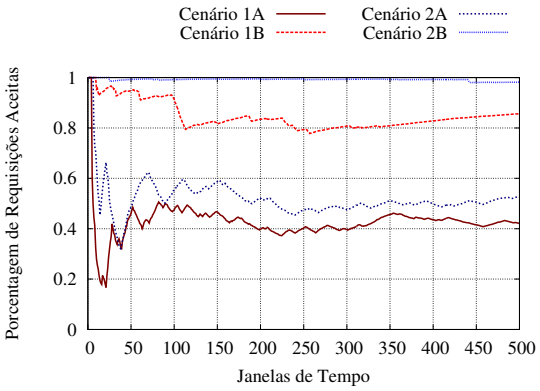


Figura 1. Porcentagem média de requisições aceitas nos experimentos realizados.

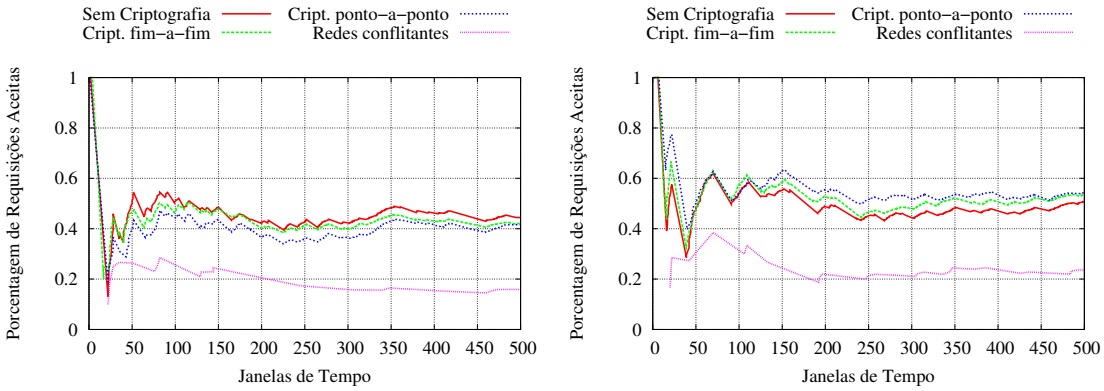
Foram criados dois cenários para avaliar o modelo, os quais se diferenciam pelos requisitos de capacidade dos elementos das redes virtuais. No primeiro, denominado *cenário 1*, cada roteador virtual requer entre 10 e 50% de CPU, e entre 32 e 128 MB de memória. Os enlaces das redes virtuais nesse cenário requerem entre 1 e 5 Gbps. Já no *cenário 2*, roteadores requerem entre 10 e 25% de CPU e entre 32 e 64 MB de memória, e enlaces requerem entre 1 e 2.5 Gbps. Os limites superiores dos requisitos do cenário 1 equivalem a 50% da capacidade disponível em roteadores e enlaces físicos, enquanto que no cenário 2, tais limites equivalem a 25% da capacidade dos elementos físicos. Todos os parâmetros previamente descritos seguem uma distribuição uniforme.

4.2. Resultados

Inicialmente, foram realizados experimentos seguindo os dois cenários descritos na subseção anterior. Em seguida, os experimentos foram repetidos, utilizando as mesmas redes físicas e as mesmas requisições geradas em cada janela de tempo, porém com uma versão modificada do modelo que desconsidera requisitos de segurança. As versões dos cenários 1 e 2 em que são considerados os requisitos de segurança são denominadas *1A* e *2A*. Já as versões modificadas para ignorar tais requisitos são denominadas *1B* e *2B*. Os resultados dos experimentos realizados com essas diferentes versões foram comparados para caracterizar o impacto causado pelo emprego de serviços relacionados à confidencialidade.

Analisou-se a taxa de aceitação de requisições de redes virtuais nos experimentos realizados. Ressalta-se que requisições somente são negadas caso não seja possível acomodar a rede virtual solicitada no substrato atendendo todos os seus requisitos. A Figura 1 ilustra a taxa média de aceitação obtida em cada cenário. Cada ponto no gráfico denota a taxa média de aceitação obtida desde o início do experimento até a janela de tempo em questão.

Analisando o gráfico, percebe-se, de forma clara, o impacto causado pelo fornecimento de serviços relacionados à confidencialidade. Nos cenários 1A e 2A, em que os requisitos de segurança são considerados, a taxa média ao fim dos experimentos é de, respectivamente, 42,2% e 52,5%. Já nos demais cenários, 1B e 2B, as taxas são de respectivamente 85,6% e 98,2%. Observa-se, ainda, uma taxa de aceitação maior nas variantes do cenário 2 em relação às do cenário 1, devido ao fato de que nos cenários 2A e 2B as requisições possuem requisitos de capacidade mais baixos. Além disso, é possível perceber que, em todos os casos, a taxa de aceitação inicial é de 100%, visto que o substrato



(a) Cenário 1A (b) Cenário 2A

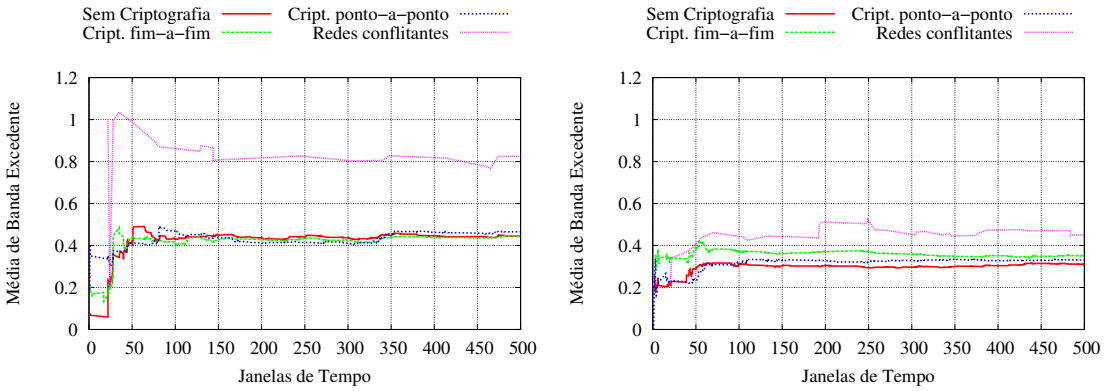
Figura 2. Porcentagem média de requisições aceitas nos cenários 1A e 2A, divididas por tipo de requisição.

encontra-se desocupado no início do experimento. Após algum tempo, devido à saturação dos elementos físicos, requisições passam a ser negadas, causando quedas na taxa média. A mesma, então, volta a subir conforme algumas das redes virtuais alocadas alcançam sua duração máxima e são removidas do substrato. Esse comportamento se repete ao longo dos experimentos, gradualmente convergindo para um valor médio.

A seguir, a Figura 2 apresenta, em maiores detalhes, a taxa de aceitação dos diferentes tipos de requisições presentes nos cenários 1A e 2A. Os gráficos exibem um comportamento em grande parte similar ao anterior, porém nota-se que em ambos a taxa de aceitação de requisições com conflitos é significativamente mais baixa do que a média geral. Isso se deve à dificuldade de alocar redes virtuais conflitantes sem que nenhum de seus roteadores e enlaces se sobreponham. A taxa média de aceitação de redes virtuais com conflitos é de 15,9% no cenário 1A, e de 23,6% no cenário 2A.

Ainda observando o gráfico ilustrado na Figura 2, percebe-se que não há uma grande diferença entre a porcentagem de redes aceitas sem criptografia, com criptografia fim-a-fim e com criptografia ponto-a-ponto. As taxas médias ao longo do cenário 1A são de, respectivamente, 44,4%, 42,1% e 41,6%. Já no cenário 2A, as médias são de, respectivamente, 50,8%, 53,3% e 54,2%. É importante salientar que, nos experimentos realizados, 95% dos roteadores da rede física oferecem suporte a protocolos que permitem a criptografia e decriptografia de pacotes, e que o modelo não considera custos adicionais de processamento e memória necessários para tais operações. Considerando-se uma taxa menor de equipamentos com suporte a tais operações, ou os custos adicionais associados às mesmas, julga-se que haveria uma diferença mais expressiva entre os diferentes tipos de requisições. Contudo, acredita-se conseguir, com o experimento realizado, oferecer uma boa visão global do custo associado para satisfazer requisitos de segurança no contexto investigado.

A próxima análise foca na largura de banda total necessária para alocar cada requisição em relação à largura de banda requisitada. A largura de banda ocupada por redes virtuais alocadas no substrato tende a ser mais alta do que a requisitada, visto que um único enlace virtual pode ser alocado em um caminho composto por uma série de enlaces físicos. A Figura 3 apresenta a média de largura de banda excedente das requisições aceitas nos cenários 1A e 2A, separadas pelo nível de confidencialidade solicitado. Ressalta-



(a) Cenário 1A (b) Cenário 2A

Figura 3. Média de largura de banda excedente necessária para acomodar as requisições de diferentes tipos aceitas nos cenários 1A e 2A.

se que o modelo visa minimizar a largura de banda consumida pelas redes virtuais alocadas, e que todas as soluções resultantes dos experimentos realizados são ótimas. Nota-se que requisições com conflitos tendem a consumir uma banda significativamente maior em relação às demais. No cenário 1A, tais requisições consomem em média 82,5% de largura de banda além do solicitado, e no cenário 2A, 45,1%. Em outras palavras, o custo da alocação de redes conflitantes para provedores de infraestrutura torna-se muito maior. Isso ocorre devido à necessidade de se utilizar caminhos mais longos para evitar a sobreposição dos elementos dessas redes.

Quanto à largura de banda excedente dos demais tipos de requisições, no início do experimento 1A há uma diferença visível entre as mesmas. Até a vigésima janela de tempo, requisições sem criptografia possuem banda média excedente de 6,7%, enquanto que requisições com criptografia fim-a-fim, 13,4%, e as com criptografia ponto-a-ponto, 35,1%. Ou seja, até esse momento, requisições com níveis mais altos de criptografia exigem uma quantidade maior de recursos para serem alocadas. No entanto, de forma similar aos gráficos da Figura 2, ao longo da execução tais valores convergem para porcentagens muito próximas. Ao término da execução, as médias de largura de banda excedente situam-se entre 44,3% e 46,5%. No cenário 2A, há sobreposições entre tais médias desde o início do experimento, e ao término do mesmo, novamente as médias encontram-se muito próximas, entre 31,1% e 35,1%.

Por fim, é apresentado o tempo médio necessário para encontrar a alocação ótima de cada requisição aceita nos experimentos realizados. Em todos os cenários, a média permanece abaixo dos 4,5 segundos do início ao fim dos experimentos. Apesar de pequena, é possível notar uma diferença na média de tempo entre os diferentes cenários. Os cenários em que os requisitos de segurança são considerados possuem média de tempo mais baixa do que os cenários nos quais os mesmos são ignorados. De forma similar, os cenários com requisitos de capacidade mais altos são resolvidos mais rapidamente do que os cenários em que tais requisitos são mais baixos. Tais diferenças podem ser explicadas pela diminuição no espaço de busca causada tanto por restrições relacionadas à segurança quanto pelos requisitos de capacidade mais altos. A presença de um número maior de restrições ou requisitos de capacidade tendem a diminuir o espaço de soluções factíveis, o que pode a tornar a busca pela solução ótima mais rápida. Nos cenários 1A e 1B, o tempo médio é de respectivamente 2,29 e 2,75 segundos, enquanto que nos cenários 2A e 2B os

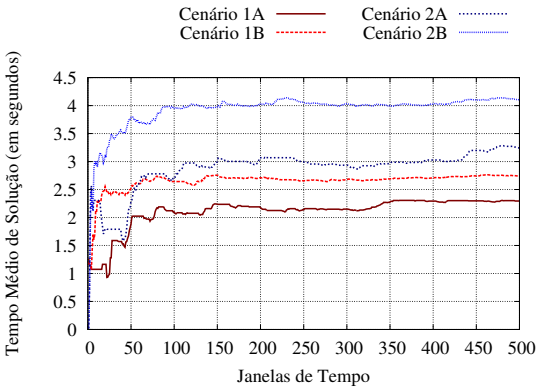


Figura 4. Tempo médio necessário para encontrar a alocação ótima nos experimentos realizados.

mesmos são de 3,24 e 4,1 segundos.

Em resumo, os resultados apresentados mostram que há um impacto significativo em termos de aceitação de requisições de redes virtuais e consumo de banda por parte das requisições aceitas ao se considerar o emprego de serviços de segurança. Esses fatores afetam negativamente a possibilidade de lucro que um provedor de infraestrutura pode obter, visto que haverá menos redes alocadas no substrato, e o custo das mesmas tenderá a ser mais alto. Portanto, julga-se importante considerar o custo necessário para prover segurança às redes virtuais no momento da alocação. Além disso, a avaliação do tempo de resolução do problema mostra que a implementação do modelo proposto é capaz de produzir resultados ótimos em um tempo adequado para uso em ambientes de produção.

5. Conclusões

Virtualização de redes é um tópico importante e que tem recebido atenção da comunidade científica e da indústria, resultando na proposta de uma série de abordagens de alocação. Mais recentemente, surgiram propostas visando prover segurança a ambientes de redes virtuais. No entanto, os autores desconhecem tentativas anteriores de combinar ambas as áreas, provendo alocação ótima e orientada a segurança de recursos de redes virtuais.

Considerando que a alocação de recursos e a segurança são igualmente importantes, desenvolveu-se um modelo que combina restrições de CPU, memória, largura de banda e localidade com requisitos de segurança. Redes virtuais podem solicitar diferentes níveis de criptografia em comunicações entre seus roteadores, visando prover confidencialidade às mesmas, ou podem exigir que seus roteadores e enlaces virtuais não compartilhem dispositivos e caminhos físicos com outras redes virtuais específicas.

Os resultados obtidos demonstram o impacto significativo causado pelo aprovisionamento de serviços de segurança na alocação de redes virtuais, salientando a importância de considerá-los no processo de mapeamento. Além disso, o modelo proposto mostra-se capaz de produzir resultados ótimos em um tempo adequado. Ainda que não sejam considerados custos adicionais de processamento e memória associados aos processos de criptografia e decriptografia, os resultados são capazes de prover uma boa visão global desse impacto. Pretende-se realizar uma revisão mais profunda de trabalhos relacionados à segurança, visando obter medidas reais de tais custos para incorporá-los no modelo. Acredita-se que isso permitirá analisar as consequências do fornecimento de serviços de segurança com uma granularidade mais fina.

Outra perspectiva para trabalhos futuros é permitir a reotimização de redes virtuais já alocadas, migrando recursos virtuais entre roteadores e enlaces do substrato. O processamento de requisições em tempo real pode levar à fragmentação dos recursos físicos, visto que as requisições não são conhecidas *a priori*. Por esse motivo, a reotimização periódica pode beneficiar o provedor de infraestrutura, diminuindo custos e permitindo que uma quantidade maior de requisições sejam atendidas. No entanto, o tempo necessário para avaliar possíveis realocações pode tornar proibitiva a obtenção de soluções ótimas. Por esse motivo, pretende-se criar um algoritmo baseado em metaheurísticas, produzindo soluções sub-ótimas porém minimizando o tempo necessário para obtê-las.

Referências

Albert, R. and Barabási, A.-L. (2000). Topology of evolving networks: Local events and universality. http://link.aps.org/doi/10.1103/PhysRevLett.85.5234. *Phys. Rev. Lett.*, 85:5234–5237.

Alkmim, G. P., Batista, D. M., and Fonseca, N. L. S. (2011). Optimal mapping of virtual networks. In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pages 1–6.

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

Anderson, T., Peterson, L., Shenker, S., and Turner, J. (2005). Overcoming the internet impasse through virtualization. *Computer*, 38(4):34–41.

Cabuk, S., Dalton, C. I., Ramasamy, H., and Schunter, M. (2007). Towards automated provisioning of secure virtualized networks. In *Proceedings of the 14th ACM conference on Computer and communications security*, CCS '07, pages 235–245, New York, NY, USA. ACM.

Cheng, X., Su, S., Zhang, Z., Wang, H., Yang, F., Luo, Y., and Wang, J. (2011). Virtual network embedding through topology-aware node ranking. In *SIGCOMM Computer Communication Review*, volume 41, pages 38–47, New York, NY, USA. ACM.

Chowdhury, N., Rahman, M., and Boutaba, R. (2009). Virtual network embedding with coordinated node and link mapping. In *INFOCOM 2009, IEEE*, pages 783 –791.

Davy, S., Serrat, J., Astorga, A., Jennings, B., and Rubio-Loyola, J. (2011). Policy-assisted planning and deployment of virtual networks. In *Network and Service Management (CNSM), 2011 7th International Conference on*, pages 1 –8.

Fernandes, N., Moreira, M., Moraes, I., Ferraz, L., Couto, R., Carvalho, H., Campista, M., Costa, L., and Duarte, O. (2010). Virtual networks: Isolation, performance, and trends. In *Annals of Telecommunications*.

Huang, D., Ata, S., and Medhi, D. (2010). Establishing secure virtual trust routing and provisioning domains for future internet. In *GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference*, pages 1–6.

Kent, S. and Seo, K. (2005). Rfc 4301: Security architecture for the internet protocol. http://tools.ietf.org/rfc/rfc4301.txt.

Yu, M., Yi, Y., Rexford, J., and Chiang, M. (2008). Rethinking virtual network embedding: substrate support for path splitting and migration. *SIGCOMM Comput. Commun. Rev.*, 38(2):17–29.

