Métricas de conectividade e vulnerabilidade em redes

Antonio C. Guimaraes, Anderson C. A. Nascimento e William F. Giozza

***Resumo* — As redes de telecomunicações são resistentes a falhas aleatórias, mas muito vulneráveis a desastres naturais ou a ataques, quando afetam seus pontos críticos. Este artigo investiga meios de se estimar a vulnerabilidade das redes a tais eventos, em termos de conectividade. Representando as redes em forma de grafos, pode-se obter medidas estruturais e espectrais, baseadas em invariantes subjacentes à topologia. Para validar os resultados, essas métricas são aplicadas a modelos de redes brasileiras, de maneira a identificar os nós e enlaces mais críticos.**

Palavras-Chave* — *infraestruturas críticas, segurança de redes, vulnerabilidade, métricas estruturais e espectrais

***Abstract* — Telecommunication networks are resistant to random faults, but they are highly vulnerable natural disasters or targeted attacks, which disturb their critical points. This paper investigates ways to estimate the vulnerability of networks, in terms of connectivity. By representing networks in form of graphs, we can derive structural and spectral measurements, based on invariants underlying the topology. To validate the results, these metrics are applied to models of Brazilian networks, in order to identify the most critical nodes and links.**

Keywords* — *critical infrastructure, network security, vulnerability, structural and spectral metrics

I. INTRODUÇÃO

A proteção das infraestruturas críticas de telecomunicações requer conhecer a vulnerabilidade de tais redes em face de perturbações. Eventos de vários tipos, como desastres, ataques físicos ou cibernéticos localizados podem ter efeitos globais. Por sua topologia particular, as redes de telecomunicações soem ser bem resistentes a falhas aleatórias, mas são altamente vulneráveis a falhas correlacionadas com a geografia ou a ataques dirigidos a seus pontos críticos [1]. O foco do presente estudo foi identificar tais pontos e quantificar seu impacto na conectividade global [2]. A hipótese é que a vulnerabilidade de uma rede a falhas e ataques pode ser estimada através de uma composição adequada de métricas de conectividade.

A relevância deste estudo vem da crescente dependência de governos, negócios e indivíduos das infraestruturas críticas de informação e comunicação [3]. Daí a importância de se conhecer os pontos vitais das redes de telecomunicações, com o fito de protegê-los. O método aqui usado é representar a rede em forma de grafo e medir o impacto da retirada de cada nó ou enlace, utilizando métricas de conectividade disponíveis na literatura [4]. Simulações mostram que a métrica composta aqui adotada captura adequadamente a influência das métricas individuais na conectividade, permitindo identificar os nós e enlaces mais críticos de uma rede.

O estudo de redes representadas por grafos é um ramo importante da matemática discreta. Tem amplo campo de aplicação em engenharia, biologia e sociologia, entre outros [5]. A teoria dos grafos oferece grande variedade de métricas que permitem avaliar o efeito da remoção de nós ou enlaces na conectividade da rede. Tais medidas podem ser aplicadas nos domínios estrutural e espectral, permitindo capturar diferentes características dos grafos. A teoria espectral dos grafos permite identificar seus principais invariantes. Assim, é possível obter propriedades relacionadas com a topologia de uma rede a partir do espectro do grafo. Tal espectro consiste em autovalores e autovetores de matrizes naturalmente associadas ao grafo [6].

Há vários trabalhos sobre a avaliação da vulnerabilidade em redes de telecomunicações. Gorman *et al.* [7] estudaram as vulnerabilidades de redes norte americanas a ataques dirigidos. Propuseram um método que combina suas topologias espaciais física e lógica. Motta [8] fez um estudo sobre *backbones* do Brasil, utilizando métricas estruturais, com ênfase em aspectos geográficos das redes. W. Liu *et al.* [9] fizeram um estudo muito abrangente, utilizando uma métrica estrutural e outra espectral, bem como uma composição entre ambas, para determinar a distribuição ótima da reserva de capacidade em caso de falha de elementos de rede. Long *et al.* [10] utilizaram múltiplas métricas para identificar os nós mais vulneráveis a falhas correlacionadas com a geografia. Como o resultado pode depender da métrica, analisaram extensivamente a correlação entre elas, concluindo que não há uma métrica universal.

De forma distinta dos trabalhos acima citados, o presente estudo inova ao combinar cinco métricas distintas, não somente para identificar os pontos críticos, mas também para comparar explicitamente várias redes. Diversas outras análises de redes de telecomunicações de dimensões continentais conhecidas (nos Estados Unidos e Europa) utilizaram-se de apenas uma ou duas métricas. Ademais, até onde sabemos, esta seria a primeira análise abrangente das redes de telecomunicações brasileiras, com o uso de métricas estruturais e espectrais.

Este artigo está estruturado como segue: a Seção II discute as métricas de vulnerabilidade; a Seção III apresenta os resultados da aplicação das métricas para identificar as vulnerabilidades em quatro redes, que são aproximações dos *backbones* de operadoras brasileiras; a Seção IV compara estas quatro redes entre si e com duas referências internacionais; a Seção V apresenta algumas conclusões.

II. MÉTRICAS DE CONECTIVIDADE

Há uma profusão de métricas de conectividade para redes complexas, em domínios estruturais e espectrais. Para capturar diferentes características dos grafos, foram selecionadas cinco métricas, de distintas classes, entre as mais encontradiças em trabalhos recentes, envolvendo redes de telecomunicações.

Para a obtenção das medidas, a rede é representada por um grafo binário $G(\boldsymbol{V}, \boldsymbol{E})$, onde $\boldsymbol{V}$ é o conjunto de nós (ou vértices) e $\boldsymbol{E}$ o conjunto de enlaces (ou arestas). A matriz de adjacência $\boldsymbol{A}(G)$ é gerada, fazendo seu (i, j)ésimo elemento a_{ij} =1, se o nó i estiver conectado ao nó j, ou 0 em caso contrário. Os elementos da diagonal principal de $A(G)$ serão 0, por definição. A matriz

$\boldsymbol{D}(G)$ é uma matriz diagonal n x n, onde $n = |\boldsymbol{V}|$, com seus elementos $d_{i,i}$ iguais ao grau do nó i respectivo, que é o número de enlaces a ele conectado. A matriz Laplaciana $\boldsymbol{L}(G)$ é:

$$\boldsymbol{L}(G) = \boldsymbol{D}(G) - \boldsymbol{A}(G) \quad (1)$$

O conjunto de autovalores da matriz Laplaciana $\boldsymbol{L}(G)$ de um grafo G é conhecido como o espectro Laplaciano de G [11]. Sendo $\boldsymbol{I}$ a matriz identidade de dimensões n x n, a matriz Laplaciana normalizada $\boldsymbol{N}(G)$ de um grafo G é definida como:

$$\boldsymbol{N}(G) = \boldsymbol{I} - \boldsymbol{D}(G)^{-1/2}\, \boldsymbol{A}(G)\, \boldsymbol{D}(G)^{-1/2} \quad (2)$$

O conjunto de autovalores da matriz Laplaciana normalizada $\boldsymbol{N}(G)$ é chamado de espectro normal de G [12].

A. Grau médio dos nós

A primeira métrica aqui adotada é o grau médio dos nós *AD* (*average degree*). Partindo-se da matriz $\boldsymbol{D}(G)$, pode-se mostrar que a média entre os graus dos nós de sua diagonal principal, para uma rede com $|\boldsymbol{V}|$ nós e $|\boldsymbol{E}|$ enlaces, é dado por:

$$AD = \frac{1}{n} \cdot \sum_i d_i = \frac{2\,|\boldsymbol{E}|}{|\boldsymbol{V}|} \quad (3)$$

Um maior valor de *AD* indica que, em média, há um maior número de enlaces incidentes em cada nó. Assim, a conectividade da rede é mais forte. Logo, menor será sua vulnerabilidade em caso de falhas ou ataques.

B. Distância média

A distância média *ASP* (*average shortest path*) é definida como a média entre o número mínimo de saltos h_{ij} entre todos os pares de nós (i,j) da rede. O caminho mais curto e o h_{ij} respectivo são calculados por algoritmos de mínima distância (algoritmo de Djiskstra, por exemplo). Isso resulta na fórmula:

$$ASP = \frac{1}{2\,n\,(n-1)} \cdot \sum_{i,j} h_{ij} \quad (4)$$

Para redes com o mesmo número de nós e enlaces, quanto menor for o valor de ASP, mais forte será a conectividade. Logo, menor será a vulnerabilidade esperada para essa rede.

C. Conectividade algébrica

A terceira métrica aqui usada é a conectividade algébrica *AC*. A conectividade algébrica *AC* deriva do espectro Laplaciano, isto é, dos autovalores $\lambda_0, \lambda_1, \ldots \lambda_n$ da matriz $\boldsymbol{L}(G)$. O menor autovalor λ_0 é sempre zero. Os demais serão sempre positivos, salvo se a rede for desconectada. *AC* é o segundo menor autovalor $\lambda_1(G)$, conhecido como valor de Fiedler [13]:

$$AC = \lambda_1(G) \quad (5)$$

Quanto maior *AC*, mais difícil será quebrar a rede em subredes desconectadas. Assim, menor será sua vulnerabilidade a falhas e ataques localizados [14].

D. Criticidade da rede

A quarta métrica utilizada é a criticidade média da rede *NC*, proposta por Tizghadam e Garcia [15]. É definida como a razão entre a intermediação de percurso aleatório e a soma dos pesos envolvidos. A criticidade de rede τ é uma quantidade global da rede, independente da posição de quaisquer nós ou enlaces específicos utilizados no cálculo. A métrica aqui usada será a criticidade de rede normalizada, definida como:

$$NC = \tau / \mathrm{n}\,(\mathrm{n}\text{-}1) = 2\,Tr\,(\boldsymbol{L}^{+}) / (n-1) \quad (6)$$

onde $\boldsymbol{L}^{+}$ é o inverso de Moore-Penrose da matriz laplaciana $\boldsymbol{L}$, Tr é o traço da matriz e n é o número de nós do grafo G. Quanto menor for *NC*, menos sensível a mudanças de topologia e a variações de tráfego será a rede [16].

E. Espectro ponderado

A última métrica aqui adotada é o espectro ponderado *WS*, que foi originalmente proposta por Fay et al. [17] para analisar a topologia da Internet. Long *et al.* [10] sugeriram usar a maxima variação de *WS* para quantificar a capacidade de sobrevivência de uma rede. *WS* é baseada no espectro normal, isto é, nos autovalores $\nu_0, \nu_1, \ldots \nu_n$ da matriz Laplaciana normalizada $\boldsymbol{N}(G)$. Essa métrica é dada pela expressão:

$$WS = \sum_i (1 - \nu_i)^{\varepsilon} \quad (7)$$

A propriedade medida depende do expoente ε escolhido. Aqui vamos usar *WS4*, isto é ε = 4, que mede ciclos de quatro, relacionados com número de caminhos disjuntos na rede.

F. Métrica composta

Liu, Pawlikowski e Sirisena propuseram em [9] uma métrica composta para comparar redes de diferentes topologias, tanto em termos de tamanho absoluto quanto de forma. A métrica é dada pelo quociente entre a distância média *ASP* e a conectividade algébrica *AC*. O presente estudo estende essa métrica composta, tornando-a mais abrangente. Para combinar os efeitos de múltiplos atributos, recorre-se à Teoria de Utilidade Multicritério (MAUT). Sendo as funções de utilidade individuais $U_1(x_1)$, $U_2(x_2)$, ... , $U_m(x_m)$ para m diferentes atributos e sendo $p_1, p_2, \ldots, p_m$ os pesos de cada um desses atributos, a função de utilidade aditiva é definida como:

$$U(x_1, x_2, \ldots x_m) = \sum_i p_i U_i(x_i) \quad (8)$$

Tomando-se como funções de utilidade individuais os logaritmos das variações das medidas *ASP, NC, WS,* 1/*ND e* 1/*AC,* com pesos unitários, chega-se a uma função de utilidade aditiva na forma do logaritmo do produto entre tais métricas. Assim, obtemos uma métrica composta *C* na forma:

$$C = \frac{ASP.\ NC\ .\ WS4}{AD\ .\ AC} \quad (9)$$

III. IDENTIFICAÇÃO DE VULNERABILIDADES

Simulações e análises foram conduzidas em 4 diferentes redes, utilizando as métricas acima descritas. Cada nó de rede foi associado a uma cidade ou região metropolitana brasileira, listadas em ordem decrescente de população [18] e identificadas por acrônimos com duas letras.

As redes analisadas são aproximações das redes reais de grandes operadoras brasileiras [19], aqui chamadas de Op_A, Op_B, Op_C e Op_D. Os grafos são tais que resistem falhas simples, isto é, a retirada de um único nó ou enlace não quebra a rede em subredes desconectadas. Além de ser o que é usual em *backbones*, isso evita incorrer na análise de casos triviais.

Para contar com referências internacionais, incluímos nas simulações duas redes transcontinentais bem conhecidas, com frequência encontradas em experimentos similares. A primeira é Cost266, a rede de fibra ótica pan-europeia definida no projeto *Lion & Cost action 266*, considerando sua topologia ampla (*large topology*), tal como definida em [20]. Essa rede possui 37 nós e 57 enlaces. A segunda é Janos US-CA, baseada na rede *US NSF* incluindo algumas extensões, tal como foi definida na tese de doutorado de János Tapolcai [21].

Operações com matrizes e cálculos das métricas foram feitos com MATLAB. A partir das medidas *AD*, *ASP*, *AC*, *NC* e *WS4* foi calculada a métrica composta *C* através da Equação 9. As entradas e saídas utilizaram planilhas MS-Excel. A métrica *C* é apresentada em forma gráfica. Nos casos em que nos interessa apenas o valor relativo, a escala foi omitida.

A. Experimento Op_A

Para a rede Op_A, representada na Fig. 1, os nós mais críticos são as regiões metropolitanas de SP (São Paulo-SP) e SA (Salvador-BA). São os maiores picos visíveis no primeiro gráfico, que representa os nós mais críticos. É fácil visualizar no mapa que a retirada desses nós tem forte impacto na conectividade das regiões Nordeste e Sul do Brasil.

De forma similar, os enlaces mais críticos da rede Op_A são PG-LA (Ponta Grossa-PR a Lages-SC) e BS-PL (Brasília-DF a Palmas-TO). No mapa é fácil visualizar que a perda de conectividade resultante da retirada desses enlaces é forte, mas é difícil dizer se são esses os dois mais críticos. De fato, há outros enlaces bem críticos, como FL-JO (Florianópolis-SC a Joinville-SC) ou PL-IM (Palmas-TO a Imperatriz-MA). A métrica composta *C* permite resolver esse impasse.

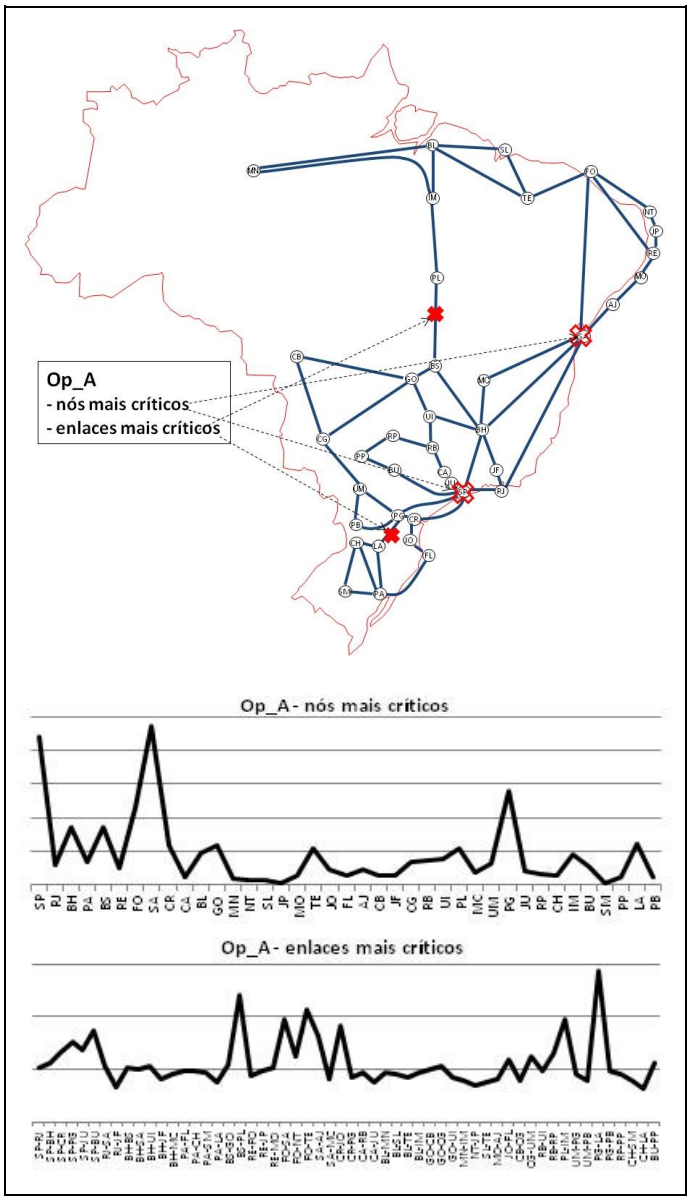

Fig. 1. Op_A – nós e enlaces mais críticos

B. Experimento Op_B

A Fig. 2 representa os resultados obtidos para a rede Op_B.

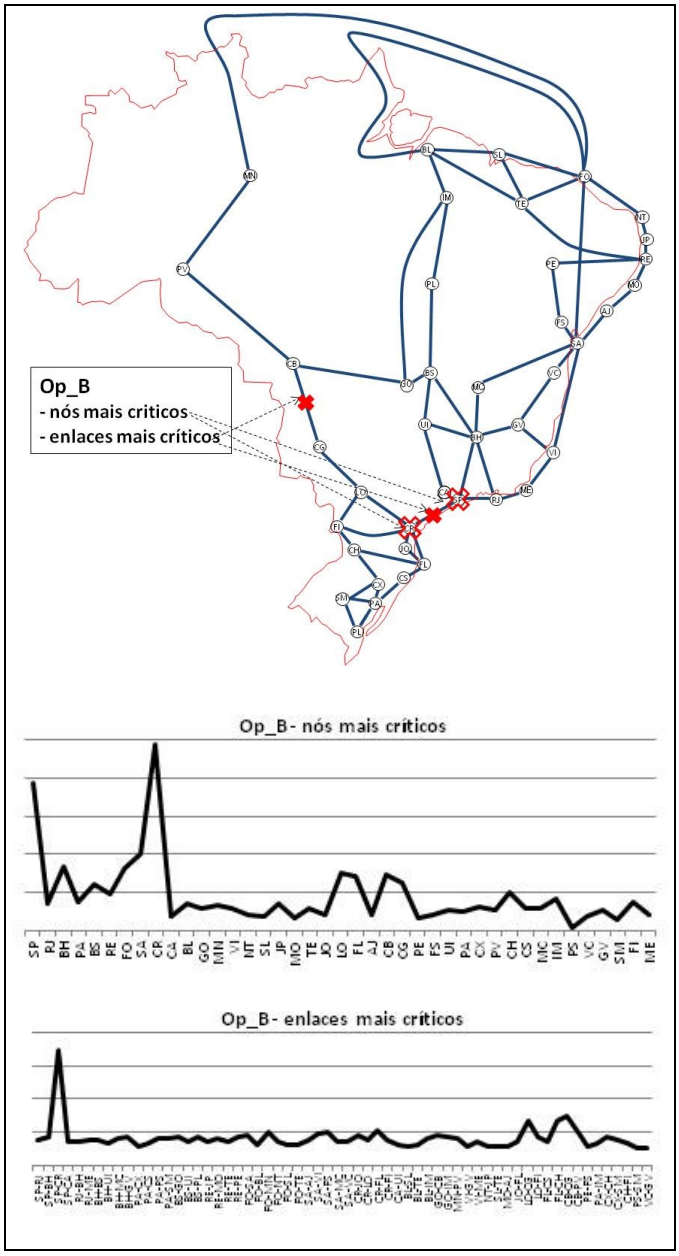

Fig. 2. Op_B – nós e enlaces mais críticos

Nesse caso, os nós mais críticos são CR (Curitiba-PR) e SP (São Paulo-SP), que correspondem aos dois maiores picos no primeiro dos dois gráficos da Fig. 2. É bem fácil ver no mapa o impacto na conectividade da retirada de qualquer desses nós.

É bem evidente no mapa da Fig. 2 que o enlace SP-CR (São Paulo-SP a Curitiba-PR) é crítico para conectividade da rede. No entanto, não é fácil reconhecer visualmente qual é o enlace que ocuparia o segundo lugar. Mais uma vez a métrica composta vem ao socorro, indicando que isso corresponde ao enlace CB-CG (Cuiabá-MT a Campo Grande-MS).

C. Experimento Op_C

Os resultados para a rede Op_C estão na Fig.3. A métrica indica que os dois nós mais críticos são SA (Salvador-BA) e CR (Curitiba-PA). Por simples observação do mapa isto não é evidente, mas é bastante crível a indicação da métrica quando aponta tais nós como os mais críticos para a conectividade.

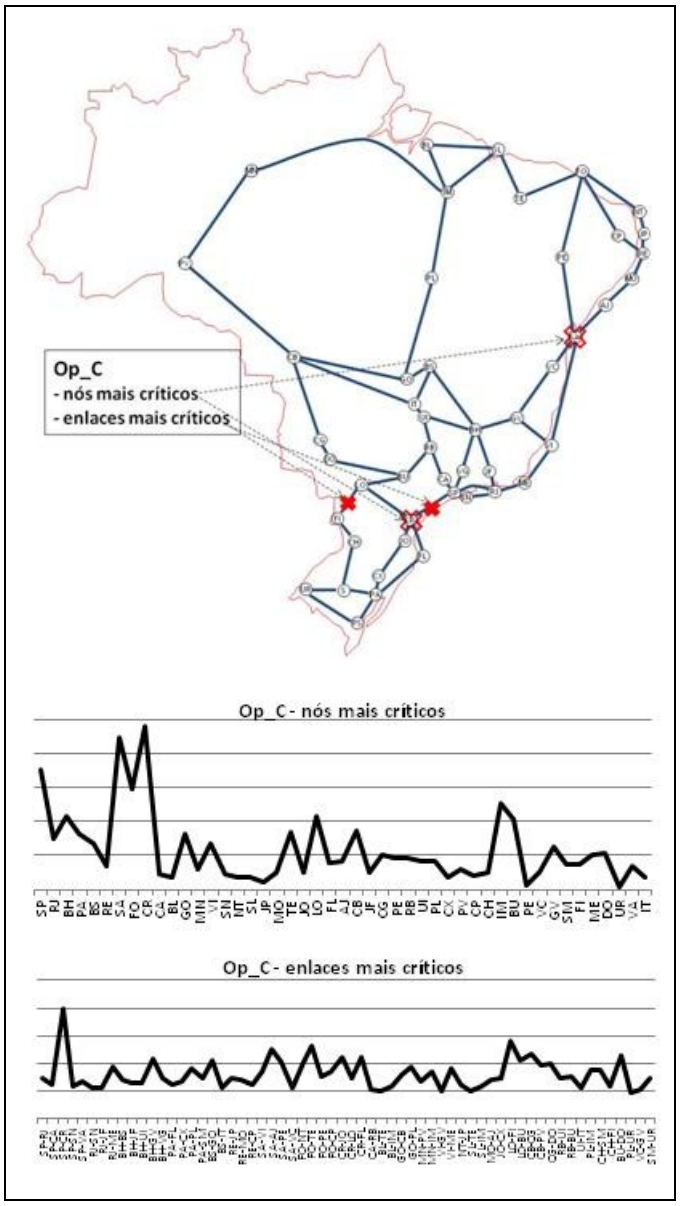

Fig. 3. Op_C – nós e enlaces mais críticos

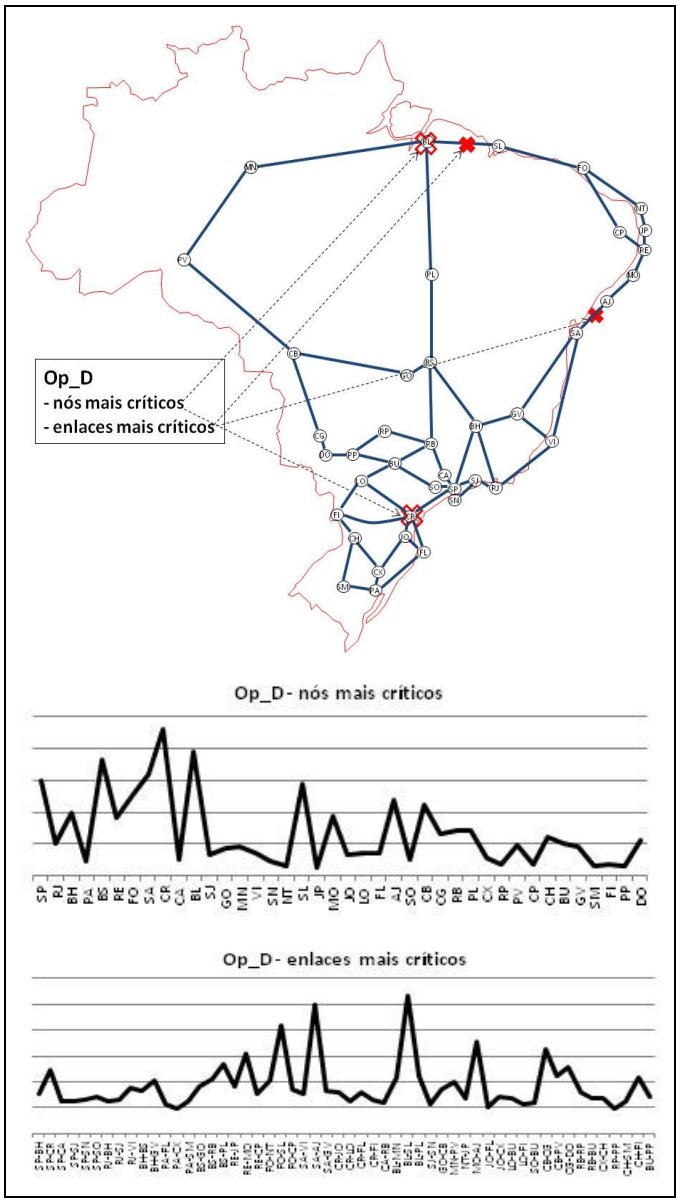

Fig. 4. Op_D – nós e enlaces mais críticos

Os dois enlaces mais críticos para a conectividade da rede são difíceis de identificar visualmente no mapa. A métrica *C* indica o enlace SP-CR (São Paulo-SP a Curitiba-PR), seguido pelo enlace LO-CG (Londrina-PR a Foz do Iguaçu-PR) como os dois mais críticos para a conectividade da rede Op_C.

D. Experimento Op_D

A rede Op_D, representada na Fig. 4, tem como nós mais críticos CR (Curitiba-PR) e BL (Belém-PA), de acordo com a indicação da métrica composta *C*. Por simples inspeção visual do mapa não seria fácil determinar que seriam esses dois os nós mais críticos. De fato, o primeiro gráfico tem vários picos, que correspondem a outros nós que estariam apenas ligeiramente abaixo em termos de criticidade.

De maneira similar, não é fácil reconhecer visualmente os dois enlaces mais críticos para a conectividade da rede Op_D. A métrica indica o enlace BL-SL (Belém-PR a São Luís-MA) seguido de SA-AJ (Salvador-BA a Aracaju-SE), como sendo os mais críticos. No entanto, o segundo gráfico tem igualmente vários outros picos, indicando outros há enlaces apenas um pouco menos críticos que os dois acima mencionados.

IV. COMPARAÇÃO DE VULNERABILIDADES

A Seção III apresentou resultados relativos à supressão de nós ou enlaces dentro de uma mesma rede. A presente Seção efetua uma comparação das vulnerabilidades de distintas redes entre si. Será tomada como base a variação relativa da métrica composta *C* obtida ao retirar o nó ou o enlace mais crítico de cada rede. A maior variação observada indicará a rede mais vulnerável a falhas ou ataques localizados.

O ponto de partida são as métricas individuais *AD*, *ASP*, *AC*, *NC* e *WS4*. A partir delas se obtém a métrica composta *C* por meio da Equação 9. A Tabela I mostra os valores da métrica *C* obtidos para cada modelo da Seção III, seguidos dos valores da mesma métrica obtidos com a supressão do enlace mais crítico (*C-enlace*) e do nó mais crítico (*C-nó*).

TABELA I. *MÉTRICAS COMPOSTAS, OBTIDAS PARA CADA REDE*

Métrica/ Rede	**Op_A**	**Op_B**	**Op_C**	**Op_D**	**Cost 266**	**Janos US-CA**
C	110	117	391	195	42	72
C-nó	965	1.051	1.884	1.012	319	154
C-enlace	240	417	801	513	81	109

A Tabela I inclui adicionalmente os valores da métrica *C* obtidos para as redes Cost266 [20] e Janos US-CA [21], duas redes de telecomunicações transcontinentais já apresentadas na Seção III, aqui utilizadas como referência. A variação relativa de *C* é mostrada no gráfico da Fig.5.

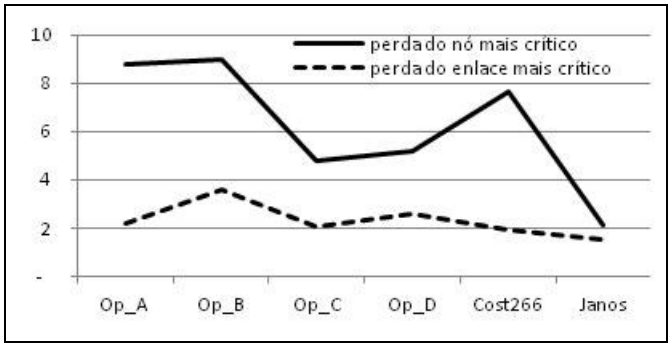

Fig. 5. Vulnerabilidade das redes, comparadas entre si

O gráfico da Fig. 5 mostra que, para a perda do nó mais crítico, a rede Op_B seria a mais vulnerável, seguida pelas redes Op_A, Cost266, Op_D, Op_C e Janos US-CA, nesta ordem. Para a perda do enlace mais crítico, os valores de *C* para uma mesma rede são mais baixos e o *ranking* de vulnerabilidades muda: Op_A, Op_C e Cost266 vão para o penúltimo lugar, praticamente empatadas.

V. CONCLUSÕES

A métrica composta aqui apresentada provê uma forma simples para se identificar os nós e enlaces mais críticos de uma rede. Pode-se assim avaliar sua vulnerabilidade a falhas ou a ataques dirigidos a tais pontos críticos, além de ser possível comparar distintas redes entre si quanto a sua vulnerabilidade. Para a verificação de sua praticidade, tal métrica foi aplicada a quatro redes de operadoras de telecomunicações brasileiras, modeladas em forma de grafos, representando sua topologia. Além disso, essas redes foram confrontadas com referências internacionais, encontradiças em estudos similares.

Observa-se que os pontos mais críticos encontrados nas redes não são mais óbvios ou aqueles observáveis à primeira vista. Por exemplo, os pontos mais críticos não correspondem necessariamente às metrópoles mais importantes, aos enlaces mais centrais da rede, nem a seus nós mais conectados. Da mesma forma, tampouco as redes com maior vulnerabilidade à perda de seu nó ou enlace mais crítico soem ser as mais óbvias. Não são necessariamente mais vulneráveis as redes menos densas, as que parecem menos simétricas, nem as que possuem mais aglomerações (*clusters*) e enlaces mais isolados.

Destarte, demonstra-se a utilidade do recurso a métricas estruturais e espectrais aplicadas a grafos que modelam as redes. Os métodos e ferramentas aqui utilizados podem ser aplicados a quaisquer redes, com modelos tão próximos à realidade quanto se queira. Os resultados podem ser úteis para se analisar possíveis aperfeiçoamentos na topologia das redes, incluindo suas interconexões. Além disso, dão subsídios a estudos sobre a mitigação de efeitos em cascata resultantes de desastres naturais ou provocados pelo homem, bem como de ameaças físicas ou cibernéticas, com miras à proteção das infraestruturas críticas de telecomunicações.

Antônio C. Guimarães: Anatel, mestrando do Departamento de Engenharia Elétrica, UnB, Brasília-DF; William F. Giozza: Departamento de Engenharia Elétrica, UnB, Brasília-DF; Anderson C. A. Nascimento: lnstitute of Technology, Center for Data Science, University of Washington, Tacoma, WA, USA. E-mails: guimaraa@aluno.unb.br; giozza@unb.br; andclay@unb.br

REFERÊNCIAS

[1] T. Grubesic and A. Murray, "Vital nodes, interconnected infrastructures, and the geographies of network survivability," Annals of The Association of American Geographers, vol. 96, no. 1, pp. 64–83, 2006.

[2] T. Matisziw, A. Murray, and T. Grubesic, "Exploring the vulnerability of network infrastructure to disruption," Annals of Regional Science, vol. 43, no. 2, pp. 307–321, Apr. 2008.

[3] Nações Unidas – "Creation of a global culture of cybersecurity and the protection of critical information infrastructures". Res. 58/199. 2004

[4] A. Bigdeli, A. Tizghadam, A. Leon-Garcia, "Comparison of network criticality, algebraic connectivity, and other graph metrics", Proceedings of 1st Annual Workshop on Simplifying Complex Network for Practitioners, Veneza, Itália, 2009.

[5] S. H. Strogatz, "Exploring complex networks" Nature 410, pp. 268–276, 2001.

[6] D. Spielman. "Spectral Graph Theory", in Combinatorial Scientific Computing", CRC Press. Cap. 18, p. 495–524, 2012.

[7] S. Gorman, et. Al. "The revenge of distance: vulnerability analysis of critical information infrastructure" School of Public Policy, George Mason University, 2004.

[8] M. Motta, "Topologia dos backbones de internet no Brasil", Revista Sociedade & Natureza, Uberlândia, ano 24, n.1, p. 21–36, 2012.

[9] W. Liu, K. Pawlikowski, H. Sirisena. "Algebraic connectivity metric for spare capacity allocation problem in survivable networks", Computer Comm. n.34, v.12, p. 1425–1435. 2011.

[10] X. Long, D.Tipper, and T. Gomes, "Measuring the survivability of networks to geographic correlated failures", Optical Switching and Networking. v.14, p. 117-133, 2014.

[11] B. Mohar. "The Laplacian Spectrum of Graphs", in Graph Theory, Combinatorics, and Applications, v. 2, Wiley, p. 871-898. 1991

[12] A. Seary, W. Richards, "Spectral methods for analyzing and visualizing networks: an introduction," Dynamic Social Networks Modeling and Analysis: Workshop Summary and Papers, National Academies Press, p. 1–20, 2003.

[13] M. Fiedler, "Algebraic connectivity of graphs", Czechoslovak Mathematical Journal. v.23, n. 2, p. 298–305, 1973.

[14] S. Jamakovic, S. Uhlig, "On the relationship between the algebraic connectivity and graph's robustness to node and link failures". 2007 Next Generation Internet Networks, p. 96–102, May 2007.

[15] A. Tizghadam, A. Leon-Garcia, "On robust traffic engineering in core networks", IEEE GlobeCom Proc., p.1-6. 2008.

[16] A. Tizghadam and A. Leon-Garcia, "Autonomic traffic engineering for network robustness", in IEEE Journal on Selected Areas in Comm., v. 28, n. 1, p. 39–50, 2010.

[17] D. Fay et al. "Weighted spectral distribution for internet topology analysis: theory and applications". IEEE/ACM Transactions on Networking, v.18, n. 1, p. 164–176, 2010.

[18] IBGE "Municípios com população residente superior a 50 000 pessoas, em ordem decrescente de população residente". *Sinopse do Censo Demográfico 2010*, Instituto Brasileiro de Geografia e Estatística, 2014

[19] Converge Comunicações, "Atlas Brasileiro de Telecomunicações", São Paulo, 2014. Disponível em: http://issuu.com/telaviva/docs/atlas2014_site_baix2

[20] S. Maesschalck et al. – "Pan-European optical transport networks: An availability-based comparison". *Photonic Network Communications*, Springer, v. 5, n. 3, p. 203–225, Maio 2003.

[21] J. Tapolcai. "Routing Algorithms in Survivable Telecommunication Networks". PhD thesis, Department of Computer Science and Information Theory, University of Technology and Economics, Budapest, Hungria, 2005.