MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE MESTRADO EM SISTEMAS E COMPUTAÇÃO

DONATO ANTONIO MARINO JUNIOR

ESTRATÉGIAS E MÉTRICAS PARA RESILIÊNCIA EM REDES DE COMPUTADORES

Rio de Janeiro
2009

INSTITUTO MILITAR DE ENGENHARIA

DONATO ANTONIO MARINO JUNIOR

ESTRATÉGIAS E MÉTRICAS PARA RESILIÊNCIA EM REDES DE COMPUTADORES

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientador: Ronaldo Moreira Salles -

Rio de Janeiro
2009

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80-Praia Vermelha
Rio de Janeiro-RJ CEP 22290-270

M339e Marino Jr., D. A.
Estratégias e Métricas para Resiliência em Redes de Computadores, Donato Antonio Marino Junior.
– Rio de Janeiro: Instituto Militar de Engenharia, 2009.
84 p.: il, graf., tab.

Dissertação: (mestrado) – Instituto Militar de Engenharia, Rio de Janeiro, 2009.

1. Redes de Computadores. 2. Resiliência em Redes. 3. Tolerância a Ataques em Redes. 4. Segurança em Redes. I. Título. II. Instituto Militar de Engenharia.

CDD 004.68

INSTITUTO MILITAR DE ENGENHARIA

DONATO ANTONIO MARINO JUNIOR

ESTRATÉGIAS E MÉTRICAS PARA RESILIÊNCIA EM REDES DE COMPUTADORES

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientador: Ronaldo Moreira Salles - Aprovada em 13 de Agosto de 2009 pela seguinte Banca Examinadora:

Ronaldo Moreira Salles - Ph.D. do IME - Presidente

Prof. Nilton Alves Júnior - D.Sc. do CBPF

Prof. Sidney Cunha de Lucena - D.Sc. da UNIRIO

Profª. Raquel Coelho Gomes Pinto - D. Sc. do IME

Rio de Janeiro
2009

Dedico este trabalho a minha esposa e filha,
a minha família e a todos os amigos que me
apoiaram neste árduo caminho.

AGRADECIMENTOS

À minha esposa Fátima, agradeço o amor, compreensão, apoio e constante incentivo ao meu trabalho, por suportar minha ausência em vários finais de semana, por me ensinar a ser um ser humano melhor nestes 25 anos que estamos juntos. Agradeço a minha filha Isadora, minha linda princesa, que soube compreender e dar apoio ao pai neste período de estudos.

À minha mãe Wanda, também pelo apoio em tudo que faço e pelo conhecimento transmitido ao longo de sua vida. Ao meu pai Donato, que certamente está orgulhoso do filho e olhando por ele em outro plano. Saudades, meu pai, mas Deus sabe o que que faz.

Ao meu orientador, Ronaldo Moreira Salles, por acreditar que um profissional que presta consultoria a 7 empresas, dá aula quase todos os dias à noite como professor universitário e ainda tem uma família para dar atenção, poderia terminar o curso e ainda submeter artigo. Agradeço sua disponibilidade e prontidão em atender e esclarecer minhas dúvidas, o conhecimento transmitido ao longo destes dois anos, seja nas aulas, nas reuniões de trabalho ou na convivência diária no final do mestrado.

Ao colega David Moura, pela agradável companhia nos vários dias, finais de semana e feriados em que trabalhamos juntos, pelas conversas sobre os mais variados assuntos para acalmar os neurônios, pelos "bizus" do Latex.

Aos meus clientes de consultoria, que me liberaram por diversas vezes para que eu pudesse cumprir com as tarefas do mestrado.

Por fim, agradeço a todos os professores e funcionários do IME - Instituto Militar de Engenharia, em especial do nosso Departamento de Engenharia de Computação (SE/8).

Donato Antonio Marino Junior

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ACK	-	Acknowledgement
AISPL	-	Average Inverse Shortest Path Lenght
ASPL	-	Average Shortest Path Lenght
BC	-	Betweeness Centrality
CC	-	Closeness Centrality
DC	-	Degree Centrality
DoS	-	Denial of Service
DDoS	-	Distributed Denial of Service
FR	-	Fator de Resiliência
FTP	-	File Transfer Protocol
HTTP	-	Hypertext Transfer Protocol
ICMP	-	Internet Control Message Protocol
LCC	-	Largest Connected Component
SA	-	Sistema Autônomo
SYN	-	Synchronize
TCP	-	Transmission Control Protocol
UDP	-	User Datagram Protocol

RESUMO

O uso da Internet para aplicações críticas e aplicações de tempo real está crescendo a cada dia. As falhas nos roteadores ou nos enlaces e ataques direcionados contra as redes afetam todo o tipo de tráfego, principalmente as aplicações de tempo real. A lenta recuperação e convergência da infraestrutura de rede causada por estas falhas podem tornar estes serviços inviáveis. Esta dissertação propõe uma medida de robustez de redes, baseada em métricas selecionadas a partir de estudos em teoria dos grafos. O proposto fator de resiliência reflete o grau de tolerância a falhas e ataques de uma rede, servindo de medida para novos projetos ou alterações na topologia já existente, objetivando a melhoria da confiabilidade e robustez. Este trabalho mostra que o fator de resiliência indica de forma eficaz a robustez de uma topologia, comparando-o com métricas utilizadas em trabalhos anteriores. Testes utilizando topologias reais, em simulações de ataques aos nós de maior centralidade da rede, validam o fator de resiliência apresentado. Este trabalho também apresenta duas estratégias de alteração de topologias, envolvendo o remanejamento e a inserção de enlaces, utilizando o fator proposto como indicador do aumento da resiliência das topologias alteradas. Os resultados obtidos com as estratégias sugeridas indicam uma melhoria na tolerância a falhas e ataques nas topologias testadas.

ABSTRACT

The Internet use for business-critical and real-time services is growing day after day. Random node or link failures and targeted attacks against the networks affect all types of traffic, but mainly real-time services. The slow recovery and network convergence caused by these failures can make those services not feasible. We propose a measure of network robustness, based on selected metrics of graph theory studies. The proposed resilience factor reflects the network fault and attack tolerance degree, which will be used as a measure for new projects or topology modifications, improving network reliability and robustness. This work shows that the resilience factor indicates on an effective form the topology robustness, comparing it with metrics used on previous works. Tests using real topologies, simulating attacks to the most centrality nodes of the network, validate the presented resilience factor. This work also presents two topologies change strategies, involving link rewiring and link addition, using the proposed factor as the resilience indicator of the modified topologies. The obtained results with the proposed strategies indicate fault and attack tolerance increase for the tested topologies.

1 INTRODUÇÃO

A resiliência em redes é tema de grande relevância, devido ao aumento da complexidade das infraestruturas de comunicação. O crescimento exponencial da Internet e o aumento do tráfego multimídia, serviços de missão crítica e outras necessidades de comunicação ininterrupta, nos remetem a criar e manter redes mais robustas e tolerantes a falhas e ataques. O ataque a redes de telecomunicações é um dos causadores desta interrupção de serviços, desta forma procuramos avaliar a capacidade de uma rede suportar estes ataques.

O tema resiliência também está ligado à preocupação com as falhas causadas por agentes da natureza, tais como terremotos, furacões e outras catástrofes naturais. O terrorismo e as guerras também são questões que demandam a preocupação em possibilitar a rápida recuperação das redes de comunicações e outras redes ligadas à infraestrutura das cidades. A resiliência em redes não é tema exclusivo da área de tecnologia de tratamento da informação, mas encontra eco nas áreas de Biologia, Geologia, Eletricidade, Engenharia de Transportes e outras.

Este trabalho situa-se na avaliação de redes reais, com métricas baseadas no estudo da teoria dos grafos. Métricas estas que refletem a resiliência de uma rede, permitindo sua avaliação e comparação com outras topologias. O fator proposto poderá servir de base para o desenho de novas topologias ou a alteração de redes já implantadas, visando melhorar sua robustez. A contribuição deste trabalho visa permitir a avaliação das redes que compõe os sistemas autônomos da Internet, com certa tolerância a falhas em dispositivos e enlaces, porém bastante vulnerável a ataques direcionados. Nesta dissertação é proposto o cálculo do Fator de Resiliência de redes, utilizando como base a métrica da k-conectividade. O Fator de Resiliência é validado em simulações de ataques aos nós de maior importância da rede, utilizando

conceitos de redes sociais. A outra contribuição deste trabalho é a apresentação de duas estratégias para a alteração de topologias, visando a melhoria de sua robustez ante a ataques e falhas aleatórias. As estratégias são testadas em três topologias escolhidas, utilizando o Fator de Resiliência para mostrar sua eficácia.

Esta dissertação está organizada da seguinte forma: após esta breve introdução, são abordados no Cap.2 os conceitos relacionados a resiliência em redes. São discutidos os trabalhos que abordaram o tema resiliência e robustez de redes, especificamente os que procuram quantificar esta característica. Em métricas de topologias, são detalhadas as principais métricas utilizadas para a análise destas topologias, identificando a melhor ou as melhores métricas para calcular a capacidade de uma rede de se recobrar de falhas ou ataques. Neste mesmo capítulo são discutidos os ataques a topologias de redes, causas da queda de um nó ou mais nós da rede, focando nos ataques cibernéticos e ataques físicos. Ao final do Cap.2, são apresentadas as medidas de centralidade, baseadas em conceitos de redes sociais, que foram usadas nas simulações de ataques a redes.

No Cap.3 é apresentada a proposta do Fator de Resiliência e sua forma de cálculo, com exemplos e simulações de ataques indicando a consistência da métrica proposta. São utilizadas topologias de redes reais nos testes, os resultados são analisados e as conclusões apresentadas.

No Cap.4 são propostas duas estratégias para a melhoria da resiliência de uma topologia, utilizando os mesmos conceitos de redes sociais usados nos testes. O Fator de Resiliência proposto é usado como base para esta verificação. Os testes e resultados são analisados com as devidas conclusões.

Por fim, no Cap.5 são realizadas as considerações finais e apresentadas sugestões de trabalhos futuros.

2 RESILIÊNCIA EM REDES DE COMPUTADORES

O conceito de resiliência em redes é descrito na definição 2.1 (AGGELOU, 2008).

Definição 2.1. *Resiliência em redes é a habilidade de uma entidade de tolerar (resistir e automaticamente se recuperar de) desafios nas condições da rede, ataques coordenados e anomalias no tráfego.*

Em um dos primeiros trabalhos que apresentou um método para medir a tolerância a falhas de uma rede, (NAJJAR, 1990) define como medida de tolerância da rede a quantidade de falhas que a mesma pode sofrer antes de ficar desconexa. Utiliza como métrica uma aproximação analítica da probabilidade da rede ficar desconexa, e faz a validação deste método de cálculo utilizando a simulação de Monte Carlo. Como cenário para os testes, os autores consideraram 3 classes de grafos como topologias, o *cube connected-cycles*, o *torus* e o cubo n-binário. Como característica principal das topologias usadas nos testes, todas são baseadas na classe n-regular, na qual o grau dos nós é constante.

O objetivo de (LIU, 2009) é quantificar a resiliência da rede, de forma que possamos comparar duas redes e dizer qual delas é mais resiliente, através de informações como quantidade de nós, enlaces, topologia, custos, etc. Utiliza como parâmetro de resiliência o percentual de perda de tráfego na ocorrência de falhas. Utiliza ainda um parâmetro de escalabilidade, que é a taxa de crescimento de tráfego perdido em respeito ao tamanho da rede, probabilidade de falhas e tráfego na rede. A principal avaliação de resiliência do artigo leva em conta o tráfego na rede e, para este cálculo, derivam a resiliência e escalabilidade de redes regulares sob tráfego uniforme, com falhas dependentes ou independentes nos enlaces, com ou sem proteção. Em outra avaliação,

insere na topologia um modelo de tráfego de entrada de pacotes descrito por um processo de Poisson. Concluem nesta avaliação que a topologia completa tem a maior confiabilidade e, dentre as topologias regulares, que possuem o mesmo número de nós e enlaces, a mais confiável é o grafo de Moore.

Os trabalhos de (NAJJAR, 1990) e, posteriormente, o de (LIU, 2009) apresentam métricas de robustez baseadas em cálculo de probabilidades, analisam ambientes com tráfego uniforme e utilizam como foco de seus testes topologias com características específicas, cenários que este trabalho procurou evitar, através de uma abordagem mais realista das métricas e topologias utilizadas.

O trabalho de (DEKKER, 2004b) avalia se uma rede é mais robusta ou confiável do ponto de vista de estar preparada contra ataques ou falhas nos nós. Faz um paralelo com a conectividade do nó e a simetria da topologia, avaliando métricas que traduzem a robustez de uma rede. O artigo foca na robustez da rede do ponto de vista da topologia, o que foi também o foco deste trabalho. Não avalia somente um grupo de topologias, mas topologias simétricas, livres de escala, aleatórias e outras. Apresenta a conectividade do nó e a similaridade entre os nós como principais métricas para a avaliação da robustez da topologia. Outras métricas como a conectividade do enlace, menor distância de menor caminho entre nós, regularidade (mesmo grau para todos os nós) e outras baseadas na teoria dos grafos são avaliadas.

Como principal trabalho relacionado desta dissertação, (BEYGELZIMER, 2005) considera três importantes métricas para avaliar a robustez de uma rede diante de falhas aleatórias e ataques direcionados. Uma delas é o maior componente conectado (LCC - *Largest Connected Component*), que indica o maior subgrafo resultante da desconexão da topologia, no caso de um ataque ou falha. A outra métrica é o tamanho médio do menor caminho (ASPL - *Average Shortest Path Length*), que varia de acordo com a alteração da topologia. Os autores optaram por usar a média inversa (AISPL - *Average Inverse Shortest Path Length*) para não causar divergências no cálculo, pois a

remoção de nós pode causar a desconexão de outros. O diâmetro da rede foi a outra métrica utilizada, que corresponde ao maior valor de menor caminho de todos os nós da rede. Estas três métricas de avaliação de robustez da rede serão utilizadas na validação do Fator de Resiliência apresentado neste trabalho e são detalhadas na próxima seção.

O artigo de (DEKKER, 2004b) também utiliza grupos de topologias, porém algumas com características mais próximas da realidade da Internet, como a livre de escala. A topologia livre de escala (BARABASI, 2000), na qual o grau de seus nós segue a distribuição lei de potência (FALOUTSOS, 1999), tem a característica principal de possuir uma pequena quantidade de nós com grande quantidade de conexões e uma grande quantidade de nós com uma pequena quantidade de conexões. O trabalho de (BEYGELZIMER, 2005) utilizou topologias de redes dinâmicas, como a Gnutella e outras obtidas de geradores de topologia, e as avaliou com o LCC, o AISPL e o diâmetro, apesar destas métricas não refletirem totalmente as diferenças de robustez em uma alteração de topologia, objeto de seu estudo.

Este trabalho utiliza, portanto, idéias presentes em todos os trabalhos mencionados, como a quantificação da resiliência de uma topologia com a utilização de métricas baseadas na teoria dos grafos. Além disso, topologias de redes reais foram usadas para analisar a métrica proposta em simulações de ataques, comparando-a com as métricas utilizadas no artigo de (BEYGELZIMER, 2005).

2.1 MÉTRICAS DE TOPOLOGIAS

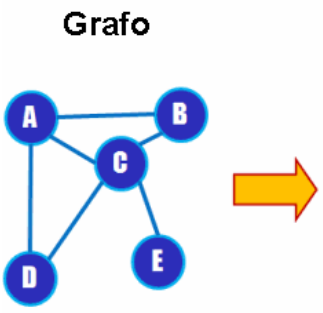
Vários trabalhos publicados avaliam métricas de topologias, procurando caracterizá-las. Esta caracterização é utilizada para a construção de geradores de topologia, utilizados em estudos de novos protocolos, engenharia de tráfego e outros. O estudo das características de uma topologia também permite o projeto e construção de redes mais tolerantes a falhas e ataques, sejam

estes últimos causados por ataques cibernéticos ou ataques físicos, oriundos de guerras, sabotagem ou terrorismo.

Conceitos de teoria dos grafos foram utilizados como base para a escolha das métricas utilizadas neste trabalho. Usando a definição 2.2 (GROSS, 2003):

Definição 2.2. *Um grafo G = (V,E) é composto por dois conjuntos V (vértices ou nós) e E (arestas ou arcos).*

Na modelagem de uma topologia de rede em um grafo, os vértices são os nós e as arestas os enlaces. A matriz de conectividade da rede (ou matriz de adjacências) indica como esta topologia está conectada e, a partir desta matriz, são calculadas as métricas da topologia. A Fig. 2.1 apresenta o exemplo de um grafo e matriz de conectividade correspondente.



Matriz de Conectividade

	A	B	C	D	E
A	0	1	1	1	0
B	1	0	1	0	0
C	1	1	0	1	1
D	1	0	1	0	0
E	0	0	1	0	0

FIG. 2.1: A representação de um grafo e sua matriz de conectividade

Este trabalho propõe uma métrica que possa indicar a resiliência de uma rede e discute estratégias para melhorar esta característica. Inicialmente, serão discutidas as principais métricas já apresentadas em trabalhos publicados, avaliando qual delas representa a melhor alternativa para medir o grau de tolerância a falhas e ataques de uma rede.

De acordo com (ALVES, 2008), não há no meio acadêmico um consenso sobre qual métrica é mais importante para caracterizar uma topologia. As métricas mais utilizadas são informações sobre a composição da topologia

(número de nós e enlaces), grau dos nós e derivados (tais como distribuição de grau nos nós e grau médio), distância entre os nós e derivados (média dos menores caminhos, diâmetro) e conectividade (k-conectividade, maior componente conectado, medidas de centralidade).

Os próximos itens detalham as métricas de topologia mais utilizadas como base para o entendimento da métrica e das estratégias propostas neste trabalho. Estas métricas foram apresentadas nos trabalhos de (BEYGELZIMER, 2005; DEKKER, 2004b; ALVES, 2008; TANGMUNARUNKIT, 2002; BEZERRA, 2009).

2.1.1 COMPOSIÇÃO DA TOPOLOGIA E GRAU DOS NÓS

Como composição da topologia, identifica-se o número de nós, o número de enlaces e a matriz de conectividade, esta última indicando como os nós estão conectados entre si. De acordo com a definição 2.3 (DIESTEL, 2005):

Definição 2.3. *O grau de um vértice v, em um grafo G, é o número de arestas de G incidentes em v, ou o número de vizinhos de v em G.*

O valor do grau dos nós de uma topologia influencia diretamente outras métricas, como as de distância e as de conectividade. O valor do grau máximo ou o valor do grau mínimo são informações importantes no cálculo de métricas de conectividade, como por exemplo a k-conectividade, que será definida mais adiante. Baseado na definição do grau do nó e em outros conceitos de teoria dos grafos, são apresentadas as métricas a seguir.

2.1.1.1 GRAU MÉDIO

O grau médio da topologia é calculado pela equação 2.1 (DIESTEL, 2005):

$$d(G) \;=\; \frac{1}{|V|}\sum_{v\in V} d(v) \tag{2.1}$$

A equação 2.1 indica que o grau médio de um grafo ($d(G)$) é a soma do grau de todos os nós ($d(v)$) pertencentes ao grafo, dividido pelo número de vértices do grafo (V). Outra forma de cálculo do grau médio é realizada pela equação $\bar{k} \;=\; \frac{2m}{n}$, onde m é o número de enlaces e n o número de nós de uma topologia.

2.1.1.2 DISTRIBUIÇÃO DE GRAU NOS NÓS

A distribuição de grau dos nós de uma topologia é a probabilidade que um nó escolhido aleatoriamente possua um grau de valor k. É calculada pela equação 2.2 (MAHADEVAN, 2005)

$$P(k) \;=\; \frac{n(k)}{n} \tag{2.2}$$

O valor de $n(k)$ indica o número de nós com grau k, e n o número de nós. Esta métrica é utilizada principalmente na caracterização de topologias. Estudos recentes indicam a distribuição lei de potência (*power-law distribution*) como uma das característica da *World Wide Web*, de acordo com o trabalho de (BARABASI, 2000). Maiores informações sobre a caracterização de redes complexas são encontradas em (ALVES JR., 2007).

2.1.1.3 DENSIDADE

Um grafo é considerado completo se todo vértice é adjacente a todos os outros vértices do grafo. O número de arestas de um grafo completo é calculado pela equação $\frac{n(n-1)}{2}$, sendo n o número de vértices. A densidade de uma topologia é a proporção da quantidade máxima de enlaces possíveis, calculada pela equação 2.3 (WASSERMAN, 1994).

$$\Delta = \frac{2m}{n(n-1)} \tag{2.3}$$

O valor de m refere-se ao número de nós da topologia e n ao número de nós. Uma topologia com apenas um nó ou um nó desconexo de uma topologia possui densidade igual a zero. Em uma topologia completa (ou grafo completo), o valor da densidade é igual a um.

2.1.2 DISTÂNCIA ENTRE OS NÓS

Para o conjunto de métricas distância entre os vértices, utiliza-se o conceito de caminho geodésico, descrito na definição 2.4 (WASSERMAN, 1994):

Definição 2.4. *O caminho geodésico é o número de enlaces existentes no caminho mais curto entre dois nós.*

O menor caminho é calculado pelo algoritmo de Dijkstra, utilizado por uma variedade de protocolos de roteamento na construção de tabelas de rota nos roteadores. Existe uma grande quantidade de métricas ligadas à distância entre os nós, mas serão abordadas apenas as que são mais utilizadas para medir a resiliência, objeto de estudo desta dissertação.

2.1.2.1 EXCENTRICIDADE

A excentricidade de um vértice é o maior caminho geodésico entre um vértice e qualquer outro vértice do grafo, ou $e(n_i) = max_j\ d(i,j)$ (WASSERMAN, 1994). Esta métrica indica se o nó está mais ao centro da topologia ou mais à borda. O valor da excentricidade mínima de um vértice no grafo é definida como o raio da rede, ou $R(G) = min\ e(n_i)$. Já o valor da excentricidade máxima de um vértice no grafo é definida como diâmetro da rede, ou $D(G) = max\ e(n_i)$. A excentricidade está na categoria de medidas de centralidade, oriundas de conceitos utilizados em redes sociais, que serão abordadas posteriormente na seção 2.3.

2.1.2.2 DIÂMETRO

Além da definição obtida do conceito de excentricidade, o diâmetro da rede é definido como o maior caminho geodésico entre i e j, para todo i e para todo j (ou $max_i\ max_j\ d(i,j)$) (WASSERMAN, 1994). Calcula-se para cada nó a tabela de caminhos geodésicos para todos os outros nós. A maior distância entre dois nós em todas as tabelas de caminhos geodésicos será o diâmetro da rede.

2.1.2.3 *AVERAGE INVERSE SHORTEST PATH LENGTH (AISPL)*

O ASPL, ou *Average Shortest Path Length*, é a média do tamanho de todos os caminhos geodésicos de uma rede. Para cada nó da rede é gerada uma tabela de caminhos geodésicos para todos os outros nós. Da tabela de cada nó é calculada a média destes caminhos e com a média de cada nó, a média de toda a topologia. Para a avaliação da resiliência de uma rede, à medida que nós são removidos, o menor caminho entre os pares de nós

tende a crescer. Um nó desconexo (distância ∞) vai influenciar diretamente no cálculo da média dos menores caminhos, fazendo com que seu valor fique muito alto. Para anular esta influência utiliza-se o AISPL, ou média inversa do tamanho dos menores caminhos, na qual o valor do inverso da distância ∞ representa zero no cálculo final. Esta métrica foi objeto de estudo no trabalho de (BEYGELZIMER, 2005) e será utilizada na comparação com a métrica proposta neste trabalho.

2.1.3 CONECTIVIDADE ENTRE OS NÓS

As métricas de conectividade são calculadas de acordo com a interligação dos nós de uma topologia, ou seja, baseadas na sua matriz de conectividade. A resiliência em redes de computadores tem por objetivo manter a topologia conexa para os mais variados tipos de ataques e falhas. Como conceito de grafo conexo, este trabalho utilizou a definição 2.5 (GROSS, 2003).

Definição 2.5. *Um grafo é conexo se existe uma caminhada (seqüência de vértices e arestas) entre qualquer par de vértices.*

São analisadas a seguir algumas métricas de conectividade, com especial atenção à k-conectividade, base da métrica proposta nesta dissertação.

2.1.3.1 COEFICIENTE DE CLUSTERIZAÇÃO

O coeficiente de clusterização é a métrica usada para medir a conectividade de um vértice aos seus adjacentes, representando a probabilidade de dois vizinhos de um vértice estarem conectados entre si. Calcula-se o coeficiente de um vértice pela equação 2.4 (LUIS, 2004).

$$c(v) \;=\; \frac{E(v)}{k_v(k_v-1)} \tag{2.4}$$

O valor de k_v representa o número de vizinhos de v e $E(v)$ é o número de arestas entre estes vizinhos. Um alto coeficiente de clusterização de um nó indica que seus vizinhos tendem a formar cliques. O clique é um subgrafo completo de um grafo, ou seja, um subgrafo em que todo vértice é adjacente a todos os outros vértices. É possível calcular o coeficiente de clusterização da rede através da média do coeficiente de todos os nós. Da mesma forma que a análise do nó, um alto valor de coeficiente de clusterização em uma topologia indica uma tendência na formação de cliques, servindo como um parâmetro na avaliação da robustez de uma rede, apesar de não levar em conta o arranjo topológico. Ou seja, um alto valor de coeficiente de clusterização não é indicativo final da resiliência de uma rede.

2.1.3.2 *LARGEST CONNECTED COMPONENT (LCC)*

O maior componente conectado é o diâmetro do maior subgrafo resultante da remoção de nós. Na ocorrência de um ataque ou falhas aleatórias, se um determinado número de nós for removido, a rede pode se transformar em pequenas redes desconexas. A fração de nós restante no maior componente conectado indicará a disponibilidade da rede após o ataque. O LCC não indica quantos subgrafos foram gerados por uma falha ou ataque, apenas a fração do maior subgrafo em relação a todos os nós da rede, por isso não pode ser utilizado em separado de outros parâmetros. Esta métrica também foi objeto de estudo no trabalho de (BEYGELZIMER, 2005) e será utilizada na comparação com a métrica proposta neste trabalho.

2.1.3.3 K-CONECTIVIDADE

De acordo com Bertsekas (BERTSEKAS, 1987), uma medida comum de confiabilidade de uma rede é a k-conectividade, um importante conceito no estudo da teoria dos grafos. Referenciada em vários trabalhos publicados (JIA, 2005; BREDIN, 2005; YANG, 2006), a propriedade da k-conectividade é baseada no Teorema de Menger, apresentado no teorema 2.1 (MENGER, 1927; DIESTEL, 2005).

Teorema 2.1. *Seja G = (V,E) um grafo e $A, B \subseteq V$. Então o número mínimo de vértices que separam A de B em G é igual ao número máximo de caminhos disjuntos entre A e B em G.*

Derivada do teorema apresentado, é definida a k-conectividade (SKIENA, 2008):

Definição 2.6. *Seja G um grafo k-conexo. Então para qualquer par de vértices, A e B, existem pelo menos k caminhos vértice-disjuntos entre A e B.*

É possível afirmar então que dois vértices, A e B, de um grafo não dirigido[1] são k-conexos se existe um caminho conectando A e B em todos os subgrafos obtidos removendo-se $k-1$ vértices diferentes de A e B em conjunto com suas arestas adjacentes. Pode-se deduzir da definição que um grafo é k-conexo se todo par de nós é k-conexo. O valor de k é a quantidade de nós de um grafo que, se removidos, o deixarão desconexo.

Para a avaliação da k-conectividade de um grafo, são removidas combinações de $k-1$ vértices, testando a conectividade entre os vértices restantes. Por exemplo, um grafo qualquer é 2-conexo se dele for possível remover qualquer um dos vértices, e este continuar conexo para todos os vértices restantes.

[1] Um grafo é dito não dirigido se um arco(x, y) implica em outro arco(y,x)

Na sequência do exemplo, para a verificação da 3-conectividade de um grafo, são necessários testes removendo qualquer combinação de dois vértices e assim por diante.

O teste da k-conectividade tem alto custo computacional, a quantidade de combinações possíveis é exponencial e diretamente ligada a quantidade de vértices de um grafo. De acordo com o número de vértices, as possíveis combinações a serem testadas são calculadas pela equação 2.5.

$$C_{(m,p)} = \frac{m!}{(m-p)!p!} \tag{2.5}$$

Sendo m o número de vértices do grafo e p o número de nós contidos no subconjunto a ser testado. O valor de $C_{(m,p)}$ será a quantidade de combinações de p elementos em m vértices.

Para reduzir a complexidade deste cálculo, vários artigos foram publicados. Baseado no teorema de Menger, Ford e Fulkerson apresentaram o *Max-Flow Min-Cut*, descrito no teorema 2.2 (FORD, 1962; DIESTEL, 2005):

Teorema 2.2. *Em qualquer rede, o valor máximo de seu fluxo é igual à capacidade de seu corte mínimo.*

O teorema 2.2 indica que o máximo fluxo em uma rede baseia-se na capacidade de seu *bottleneck*. O algoritmo de Ford-Fulkerson também avalia a k-conectividade. O corte mínimo calculado no algoritmo de Ford-Fulkerson está diretamente ligado a k-conectividade, pois o corte mínimo é a menor quantidade de vértices que, se removidos, deixarão o grafo desconexo (KAMMER, 2004). Utilizando-se do *Max-Flow Min-Cut*, Kleitman apresentou em seu trabalho um algoritmo que permite a verificação da k-conectividade, reduzindo a quantidade de verificações necessárias (KLEITMAN, 1969).

2.2 ATAQUES A TOPOLOGIAS DE REDES

Os ataques a estruturas de redes são detectados diariamente em vários pontos de gerência da Internet e são em grande parte culpados pela interrupção do funcionamento destas estruturas. Os trabalhos de (LEE, 2004, 2006) e vários outros publicados indicam que as redes que compõem a estrutura da Internet são mais vulneráveis a ataques do que a falhas. As falhas são representadas pela interrupção do funcionamento de nós e enlaces aleatórios e os ataques são normalmente direcionados aos nós mais importantes da rede. No que se refere ao crescimento das redes na Internet, a tendência é a conectividade preferencial, indicando uma probabilidade maior de conexão de um novo enlace em um nó com maior número de enlaces (BARABASI, 2000).

Este modelo de crescimento é responsável pela criação de pontos centrais de ataques, mais vulneráveis para a rede pois a sua remoção causa a desconexão da topologia. Estes nós, por serem mais importantes, normalmente possuem uma maior preocupação com falhas, utilizando sistemas ininterruptos de energia, maior segurança física, maior tolerância a falhas no hardware e outras redundâncias sob os mais variados aspectos. As catástrofes naturais (terremotos, maremotos, etc.) também podem ser identificadas como falhas devido a sua aleatoriedade. O tema falhas em topologias de redes não está no escopo principal deste trabalho, mas poderá haver alguma referência eventual.

Este trabalho sintetiza os tipos de ataques a topologias e algumas de suas técnicas. Os tipos de ataques e seus derivados são definidos a seguir, contextualizando o assunto para o tema resiliência em redes de computadores.

2.2.1 ATAQUES CIBERNÉTICOS

O trabalho apresentado sobre rastreamento de ataques, (CASTELUCIO, 2008) define como principal objetivo do ataque de negação de serviço (DoS - *Denial of Service*) fazer com que uma rede ou serviço fique inacessível a usuários legítimos. Existem ataques do tipo DoS ou DDoS (*Distributed Denial of Service*), que geram uma quantidade de requisições muito maior do que o serviço ou infraestrutura tem a capacidade de lidar, causando o travamento ou extinção dos recursos para os usuários.

Em uma topologia de rede, o ataque (D)DoS afeta os serviços executados nos roteadores e utiliza toda a banda dos enlaces disponível. Em publicação da Cisco Systems, (DEAL, 2004) faz referência a três ataques (D)DoS comumente sofridos pelos roteadores.

O TCP SYN Flooding, inundação de mensagens TCP SYN, procura sobrecarregar um ou mais serviços TCP que estão sendo executados em um dispositivo, servidor ou estação de trabalho, tal como um serviço HTTP ou FTP. No processo de estabelecimento de conexão do TCP, também conhecido como *three-way handshake*, um segmento com o bit SYN (*SYNchronize*) setado é enviando de um host de origem para um host de destino como primeiro passo desta conexão. No passo seguinte, o host de destino que recebeu este segmento aceita o pedido de conexão enviando um segmento também com o bit SYN setado, dando 'carona' para o reconhecimento do segmento anterior (*ACKnowledgement*). O ataque consiste em enviar uma inundação de segmentos TCP SYN, no intuito de fazer com que o serviço que está respondendo a estas solicitações fique sobrecarregado e saia de operação. Em muitos casos o atacante falsifica um endereço de origem para esconder seu rastro ou possivelmente criar outro ataque a uma segunda vítima. No prosseguimento do *three-way handshake*, este processo falha, pois o serviço envia um SYN+ACK

para um endereço inválido ou falso, nunca completando a conexão. Durante este período, recursos são disponibilizados para cada um destes pedidos de conexão, fazendo com que o serviço fique lento e pare de responder a novas conexões, inclusive às legítimas.

No ataque *Smurf*, o atacante envia uma inundação de mensagens ICMP a um refletor, ou conjunto de refletores, com o endereço IP de origem da vítima. Os refletores respondem a estas mensagens enviando respostas à vítima. Na maioria dos casos, o endereço de origem é um endereço de *broadcast*, permitindo o ataque a um segmento de rede ao invés de um equipamento específico.

O ataque *Fraggle*, derivado do ataque *Smurf*, utiliza o envio de datagramas UDP ao invés de mensagens ICMP. Como os datagramas UDP podem ser filtrados, o ataque *Fraggle* não tem o mesmo impacto do ataque *Smurf*.

2.2.2 ATAQUES FÍSICOS

Os ataques físicos às redes são causados pela destruição do nó, e podem ser causados por guerras, sabotagem ou terrorismo. O ataque terrorista de 11 de setembro de 2001, que causou a destruição do *World Trade Center* em Nova Iorque, deixou várias redes de telecomunicações inoperantes, levantando a questão da resiliência a estes eventos, como abordado no trabalho de (DEKKER, 2004a). O trabalho citado aborda a dependência da civilização com as redes de infraestrutura críticas, tais como redes de comunicação, energia elétrica, trens, distribuição de combustíveis e outras. A destruição de alguma destas redes afeta o funcionamento de vários serviços, como escolas, hospitais, delegacias de polícia, poder público e inúmeros outros serviços necessários à nossa sociedade. O ataque físico a estas redes torna-se alvo preferido nas guerras e dos terroristas.

O trabalho de (DEKKER, 2004a) analisa aspectos da topologia das redes de comunicações face a estes ataques e reforça a idéia de que a métrica mais importante para a sua robustez é a conectividade do nó.

2.3 MEDIDAS DE CENTRALIDADE

A Internet, representada pela interligação de SA's (Sistemas Autônomos), segue de maneira geral um modelo de crescimento baseado na conexão preferencial, indicando que quanto mais conectado é um nó mais propenso ele é para receber novas conexões. Do ponto de vista da robustez, os SA's possuem boa resiliência em relação a falhas aleatórias, mas como concentram muitas conexões em poucos nós, acabam sendo muito vulneráveis a ataques.

Explorando esta vulnerabilidade, os testes realizados neste trabalho utilizam simulações de ataques aos nós de maior importância da rede. Para verificar a importância destes nós, foram utilizas medidas de centralidade, baseadas em conceitos de redes sociais (FREEMAN, 1979; WASSERMAN, 1994). As medidas de centralidade calculam a importância do nó de acordo com vários parâmetros. Estas medidas foram utilizadas em vários artigos que avaliam a robustez de uma topologia ante a ataques (CRUCITTI, 2004; FRANTZ, 2005; HOLME, 2002). Levando a idéia para um conceito mais abrangente e explorando outros tipos de redes, as medidas de centralidade podem orientar a captura de um membro de uma rede terrorista, visando a sua desagregação ou um ataque a um centro de distribuição de energia, com o mesmo intuito, apenas para citar alguns exemplos. As medidas de centralidade utilizadas nas simulações foram adaptadas para o ambiente das redes de telecomunicações e Internet.

A primeira delas, a *Degree Centrality* (DC), define que o nó com mais enlaces possui um maior grau de centralidade em relação a toda a topologia.

Isto se deve ao fato de que o nó que possui o maior número de enlaces conectados a ele, possui conexão direta a um maior número de nós. A equação 2.6 define a *Degree Centrality*.

$$C_D(n_i) \;=\; d(n_i) \;=\; \sum_{i=1}^{g} x_{ij} \;=\; \sum_{j=1}^{g} x_{ji} \tag{2.6}$$

O grau do nó é obtido com a soma dos enlaces incidentes no nó. A equação 2.6 indica que a soma dos valores 1 da linha i de uma matriz de conectividade ou de uma coluna j da mesma matriz indica o DC do nó. O valor de x_{ij} ou x_{ji} indica posição de linha/coluna (ij) ou coluna/linha (ji) de uma matriz de conectividade. O valor de x igual a 1 indica que existe um enlace entre os nós i e j. A soma dos valores de x_{ij} ou x_{ji} indica o valor do grau do nó ou de seu DC. O valor g representa o número total de nós ou de linhas/colunas da matriz de adjacências.

A segunda medida de centralidade utilizada foi a *Closeness Centrality* (CC), que define o grau com que o nó está mais próximo de todos os outros nós. Quanto menor a soma dos menores caminhos de um nó em relação aos demais, este nó estará mais próximo do centro do que outros. Deste fato conclui-se que, se um nó possui menos nós intermediários para chegar a todos os outros, ele está mais próximo de todos, consequentemente mais ao centro. A equação 2.7 define a *Closeness Centrality*.

$$C_C(n_i) \;=\; \left[\sum_{j=1}^{g} d(n_i, n_j)\right]^{-1} \tag{2.7}$$

A variável $d(n_i, n_j)$ representa a distância geodésica entre i e j. A proximidade do centro da topologia será o inverso da soma das distâncias de i para todos os outros nós, sendo $i \neq j$, apresentado pela equação 2.7. Esta

propriedade indica quais nós são mais importantes na troca de informações entre os nós da topologia. O nó com maior CC da topologia indica o "atalho" para todos os outros nós da rede.

A terceira medida de centralidade utilizada nas simulações de ataques foi a *Betweeness Centrality* (BC), que define o grau que o nó recebe os menores caminhos de todos os outros nós. Ou seja, o nó com maior BC (ou grau de intermediação), está no caminho de mais menores caminhos de todos os nós da rede. A equação 2.8 define a *Betweeness Centrality*.

$$C_B(n_i) \;=\; \sum_{j<k} \frac{g_{jk}(n_i)}{g_{jk}} \tag{2.8}$$

Sendo g_{jk} o número de todos os caminhos geodésicos que ligam os nós j e k, e $g_{jk}(n_i)$ o número de tais caminhos, no total de g_{jk}, que passa pelo nó n_i. A equação 2.8 calcula para determinado nó n_i a soma das probabilidades de o mesmo estar no caminho geodésico entre todos os demais nós da topologia. Os nós com maior BC da rede são os que estão no caminho geodésico entre nós não adjacentes. Esta propriedade indica que um ataque ao nó de maior BC da topologia pode, com maior chance, desconectar uma topologia por estar no caminho entre outros nós. Caso a topologia possua caminhos resilientes, ou caminhos disjuntos entre pares de nós, a remoção de um nó com alto grau de BC vai influenciar outros aspectos como diâmetro ou AISPL, mas não vai causar a desconexão da topologia.

3 MÉTRICA DE RESILIÊNCIA PROPOSTA

A análise das métricas apresentadas indica que a k-conectividade é um dos parâmetros mais importantes para a avaliação da tolerância a falhas ou ataques de uma rede. Das métricas estudadas, algumas apenas indicam a resiliência de maneira parcial, como a densidade, que calcula a fração de enlaces de uma topologia completa, mas não leva em conta o arranjo topológico da rede. Duas métricas usadas para resiliência em redes, a média inversa dos menores caminhos e o maior componente conectado, também não permitem a avaliação da resiliência sozinha, mas somente para alguns casos e combinadas com outras métricas. Artigos publicados sobre ataques a topologias reforçam a idéia da escolha desta métrica, indicando que a conectividade do nó é o parâmetro mais importante, já que um ataque físico ou cibernético aos nós mais importantes pode desconectar uma rede (SAM, 2006; DEKKER, 2004b,a; FRANTZ, 2005).

Utilizando a métrica da k-conectividade na avaliação de redes reais, entre elas redes de empresas, *backbones* comerciais e acadêmicos, de uma forma geral encontra-se uma grande quantidade de topologias com a característica de 2-conectividade ou 3-conectividade, indicando a resiliência destas redes na perda de um nó e dois nós, respectivamente.

Mas, como comparar duas topologias de rede que são 2-conexas? Este trabalho propõe uma métrica baseada na k-conectividade, a ***k-conectividade parcial***, na qual todas as combinações que mantêm o grafo conexo são computadas, mesmo que a k-conectividade "completa" não seja verdadeira.

Para ilustrar a idéia, este trabalho analisa a topologia da NSFNET (Fig.

3.1), um dos primeiros *backbones* da Internet, com 14 nós. Para a análise da topologia, algumas importantes propriedades de grafos conexos são consideradas. Todo grafo conexo por definição é 1-conexo. Significa dizer que se forem removidos 'zero' vértices o grafo permanece conexo. Outra característica importante é a propriedade de ser n-conexo, sendo n o número total de vértices. Ou seja, na remoção de qualquer combinação de $n-1$ vértices de um grafo, sempre restará um único vértice que, por definição, é considerado um grafo conexo.

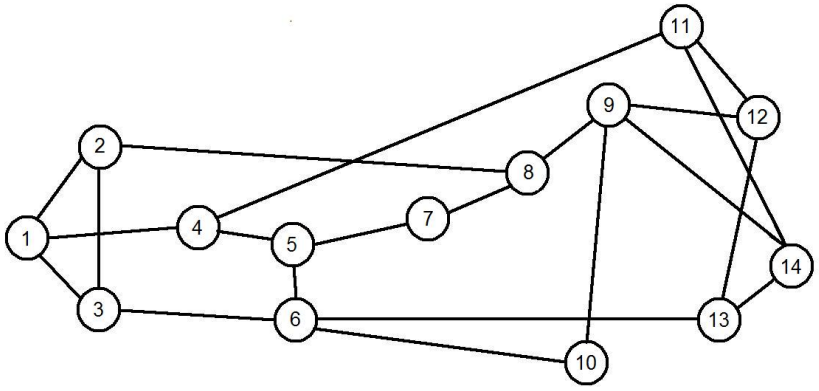


FIG. 3.1: Topologia da NSFNET

Na análise da topologia da NSFNET, afirma-se que ela é 1-conexa e 14-conexa. Portanto os testes devem ser realizados para 2-conectividade (retirando um nó de cada vez) até 13-conectividade (retirando qualquer combinação de doze nós). Para o teste da 2-conectividade desta topologia, remove-se um nó de cada vez e um teste de conectividade entre os nós restantes é realizado cada vez que um nó é removido, totalizando 14 testes. Caso a topologia se mantenha conexa em todos os testes de conectividade realizados, pode-se afirmar que a topologia possui 2-conectividade. Para o teste de 3-conectividade, são removidas combinações de 2 nós e realizado teste de conectividade depois que cada combinação for removida. Caso a topologia se mantenha conexa nos setenta e oito testes (calculado pela equação 2.5),

pode-se afirmar que a topologia possui 3-conectividade. O próximo passo é calcular a 4-conectividade da topologia e assim por diante. A não ser que a topologia seja similar a um grafo completo, com $\frac{n(n-1)}{2}$ enlaces, em algum momento do teste de remoção de nós a topologia ficará desconexa. Analisa-se então a quantidade de combinações conexas para aquele teste até o teste da 13-conectividade, computando percentuais de nós conexos para cada um dos testes. Desta forma obtêm-se o percentual de testes que mantêm a rede conexa, comparando-o com o melhor caso que seria de um grafo completo. A equação obtida da proposta do cálculo do Fator de Resiliência é:

$$FR = \frac{\sum_{i=2}^{n-1} k(i)}{(n-2)} \tag{3.1}$$

O valor de n refere-se ao número de nós da topologia, $(n-2)$ indica que foi excluída a 1-conectividade e n-conectividade, e $k(i)$ refere-se ao percentual de combinações conexas de i-conectividade.

A Fig. 3.2 apresenta um exemplo com uma topologia de apenas cinco nós, para melhor visualização do Fator de Resiliência.

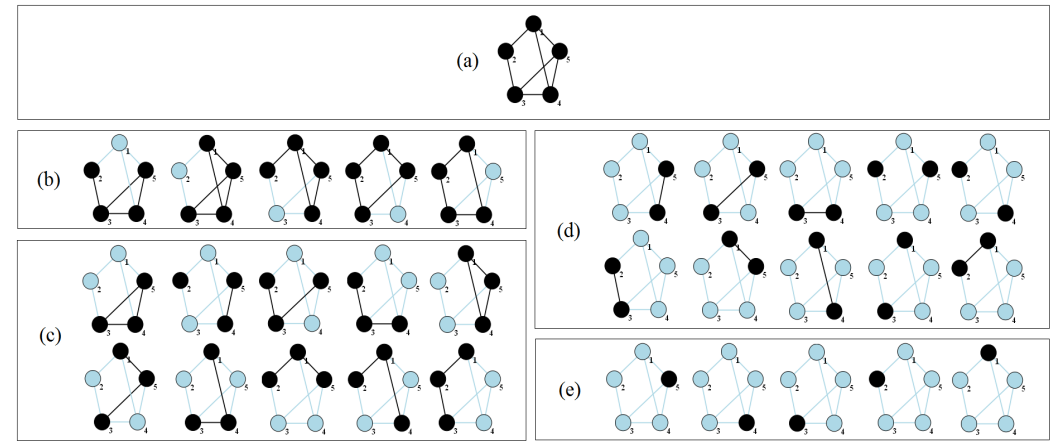


FIG. 3.2: Combinações para uma topologia de cinco nós

A topologia de cinco nós, não completa, possui 1-conectividade (Fig. 3.2a). No primeiro teste (Fig. 3.2b), é removido um nó de cada vez e verifica-se que a topologia permanece conexa em todos os testes. Desta forma é possível afirmar que a topologia é, até aqui, 2-conexa, indicando o valor de $k(2)$. No segundo teste (Fig. 3.2c), de 3-conectividade, das dez combinações possíveis na remoção de dois nós, uma combinação desconecta a topologia, a que remove os nós 1 e 3. Porém, nos outros nove testes a rede se mantém conexa. Desta forma, afirma-se que a topologia é noventa por cento 3-conexa, ou o valor de $k(3)$. No próximo teste (Fig. 3.2d), das dez combinações possíveis, três testes desconectam a topologia, permitindo concluir que ela é setenta por cento 4-conexa, indicando o valor de $k(4)$. O último teste (Fig. 3.2e) demonstra a propriedade discutida anteriormente, a n-conectividade. Removendo combinações de quatro nós a topologia resultante de apenas um nó é considerada conexa.

Desta forma, calcula-se as combinações conexas de 2-conectividade (1), 3-conectividade (0,9) e 4-conectividade (0,7), ignorando o primeiro e último testes. Somando os testes, obtêm-se o valor de 2,6 ($k(2) + k(3) + k(4)$), e usando a equação 3.1, calcula-se, como resultado do Fator de Resiliência da topologia, o valor de 0,8666, obtido de $\frac{k(2)+k(3)+k(4)}{3}$. O cálculo é, na realidade, o percentual de combinações conexas para todos os testes. O Fator de Resiliência é capaz de obter resultados diferentes mesmo se for inserido apenas um enlace, permitindo a comparação da resiliência entre topologias. Caso a topologia de cinco nós tivesse dez enlaces, ela seria completa e seu Fator de Resiliência seria 1. Neste caso, que seria o melhor caso de resiliência, a topologia se manteria conexa em todas as combinações de remoção de nós possíveis.

3.1 TESTES COM AS MÉTRICAS

3.1.1 METODOLOGIA

Como metodologia usada nos testes, foram realizadas simulações de ataques removendo nós da topologia, no intuito de avaliar o impacto na robustez destas redes. Para a escolha dos nós a serem atacados, foram utilizadas as métricas de centralidade apresentadas para analisar seis topologias escolhidas segundo vários aspectos, variando-se a característica dos nós e a quantidade de remoções. Foram avaliados os resultados obtidos com o Fator de Resiliência (FR) e as métricas utilizadas no trabalho de (BEYGELZIMER, 2005). As métricas do trabalho referenciado são: a média inversa do tamanho dos menores caminhos (AISPL), o maior componente conectado (LCC) e o diâmetro da rede.

Para cada uma das quatro métricas de resiliência (AISPL, LCC, diâmetro e FR) foram gerados três gráficos de barras (Figs. 3.9 a 3.20). Nas três variações, foram utilizadas as medidas de centralidade, simulando ataques ao nó de maior grau de métrica (DC, CC e BC) e em 10% e 20% dos nós de maior grau de medida de centralidade, comparando-os sempre com o estado original da topologia. Em algumas topologias, o nó de maior DC pode ser o mesmo para o CC ou ainda igual para o BC, mas este fato não influenciou as comparações e conclusões deste trabalho. A constatação de que alguns nós podem acumular mais de uma métrica de centralidade pode, no futuro, guiar o estudo no caminho da alteração de uma topologia ou no seu projeto, sugerido nos trabalhos futuros.

Foi também realizada comparação, em outros seis gráficos (Figs. 3.21 a 3.26), do FR com cada uma das três métricas do trabalho referenciado. As topologias utilizadas na comparação entre as métricas de resiliência foram escolhidas de acordo com as restrições que algumas destas métricas possuem, conforme exposto na análise de resultados.

3.1.2 TOPOLOGIAS UTILIZADAS NOS TESTES

Foram utilizadas nos testes seis topologias de *backbones* reais da estrutura da Internet. A Cost-239 (Fig. 3.3), rede européia de cooperação em Ciência e Tecnologia, com desenho de topologia durante a "Action 239". A JaNet (Fig. 3.4, disponível em http://www.ja.net/company/the-janet-network/index.html), Renater (Fig. 3.5, disponível em http://www.renater.fr/spip.php?rubrique12) e RNP (Fig. 3.6, disponível em http://www.rnp.br/backbone/index.php), redes nacionais de educação e pesquisa, respectivamente da Grã-Bretanha, França e do Brasil. Por fim, as redes comerciais Telcordia (Fig. 3.7), rede de abrangência metropolitana localizada em New Jersey, USA, e a UKNet (Fig. 3.8), *backbone* nacional localizado na Grã-Bretanha, vendido posteriormente à PsiNet.

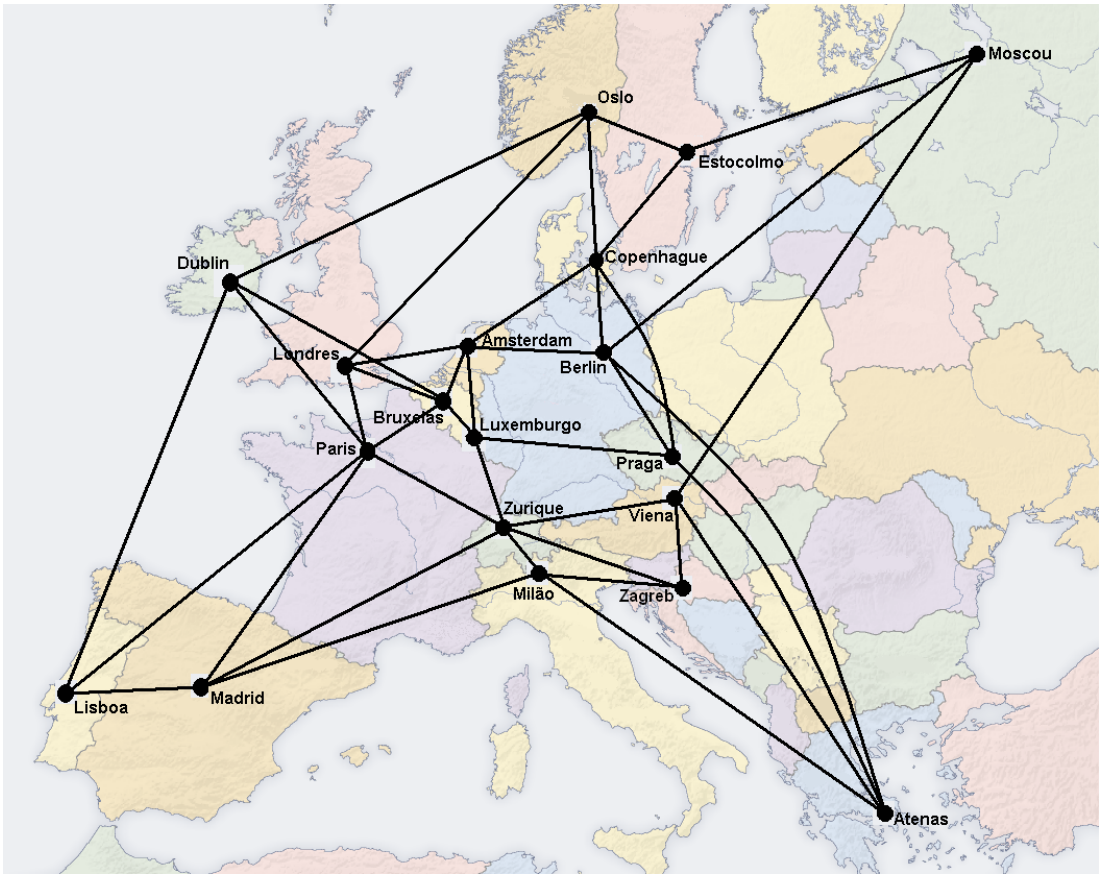


FIG. 3.3: Cost-239 - 19 nós e 40 enlaces

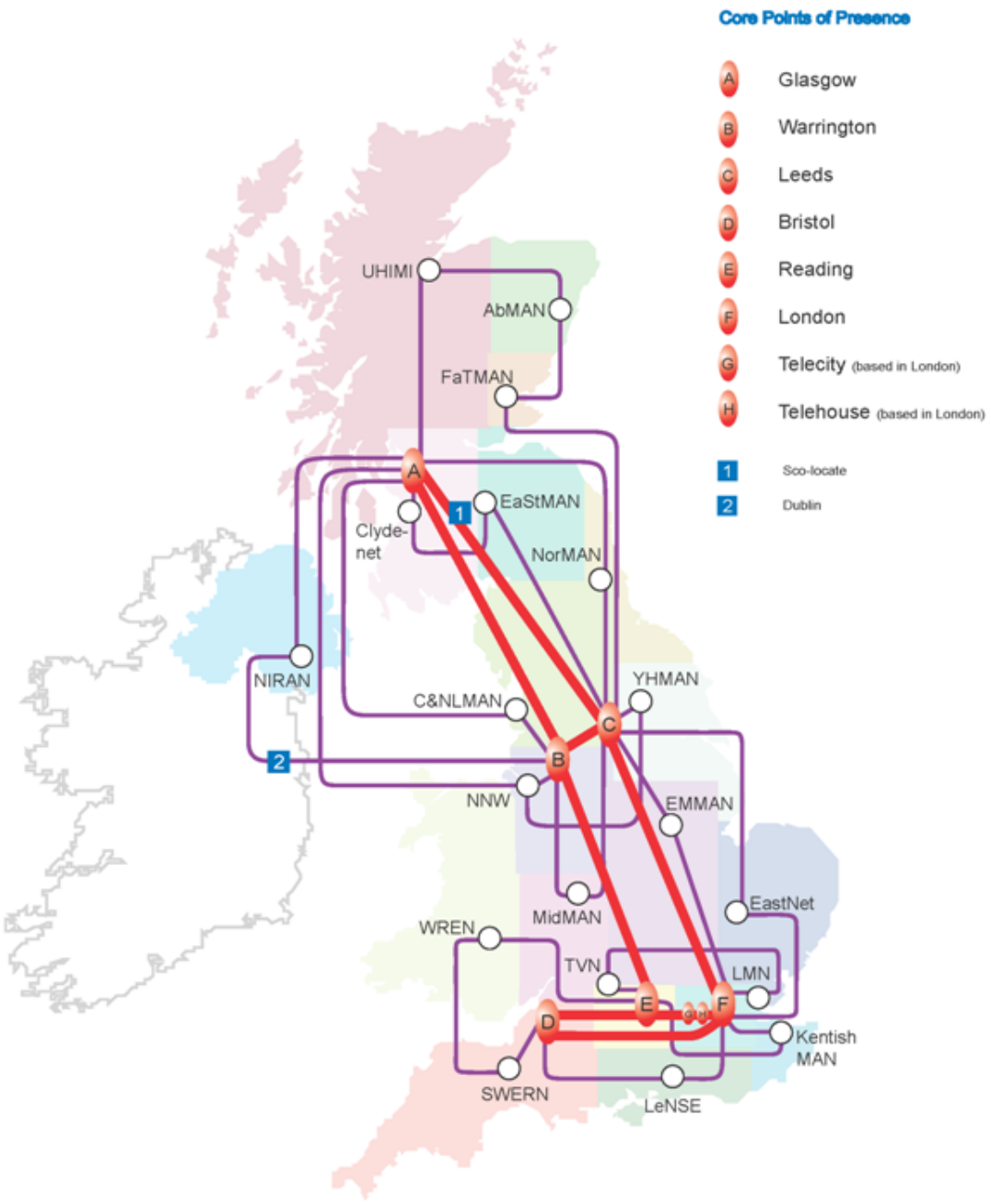


FIG. 3.4: JaNet - 29 nós e 45 enlaces

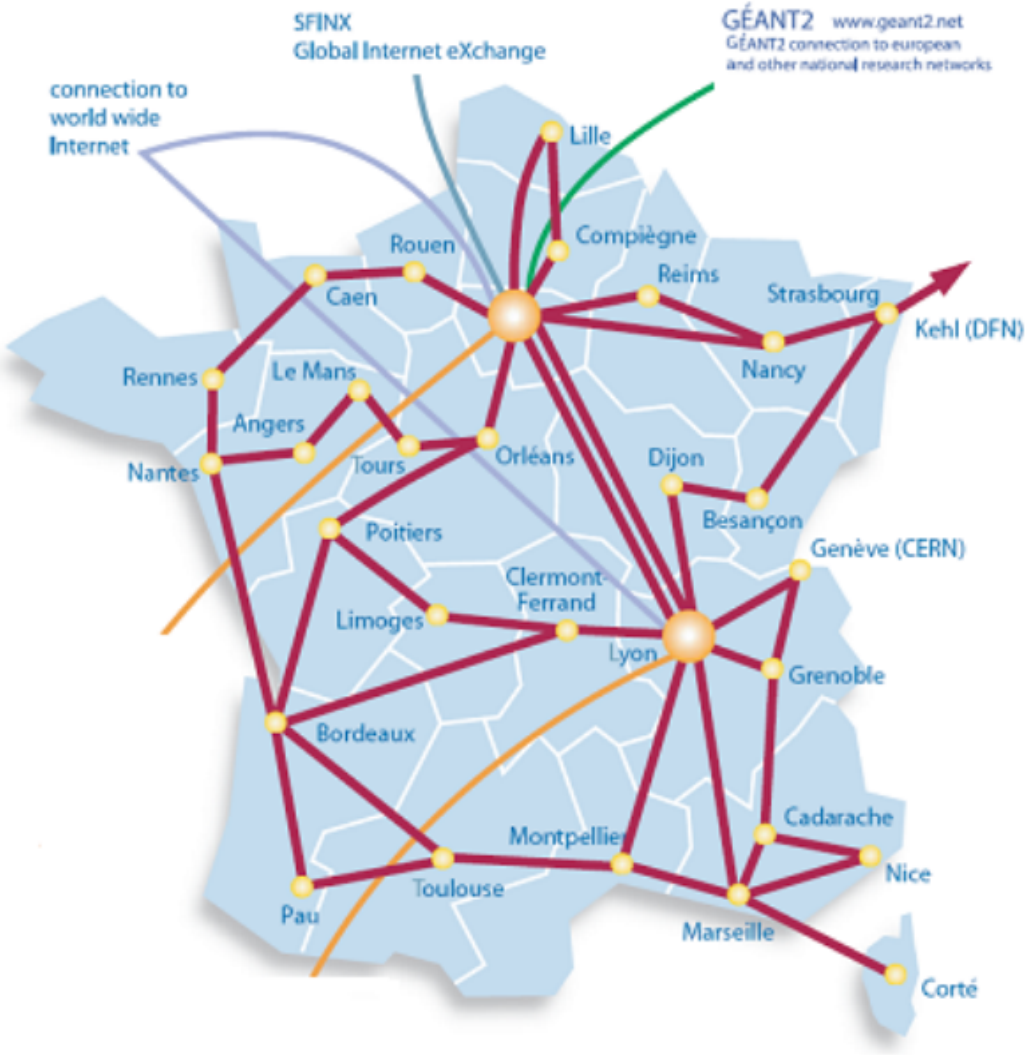


FIG. 3.5: Renater - 30 nós e 42 enlaces

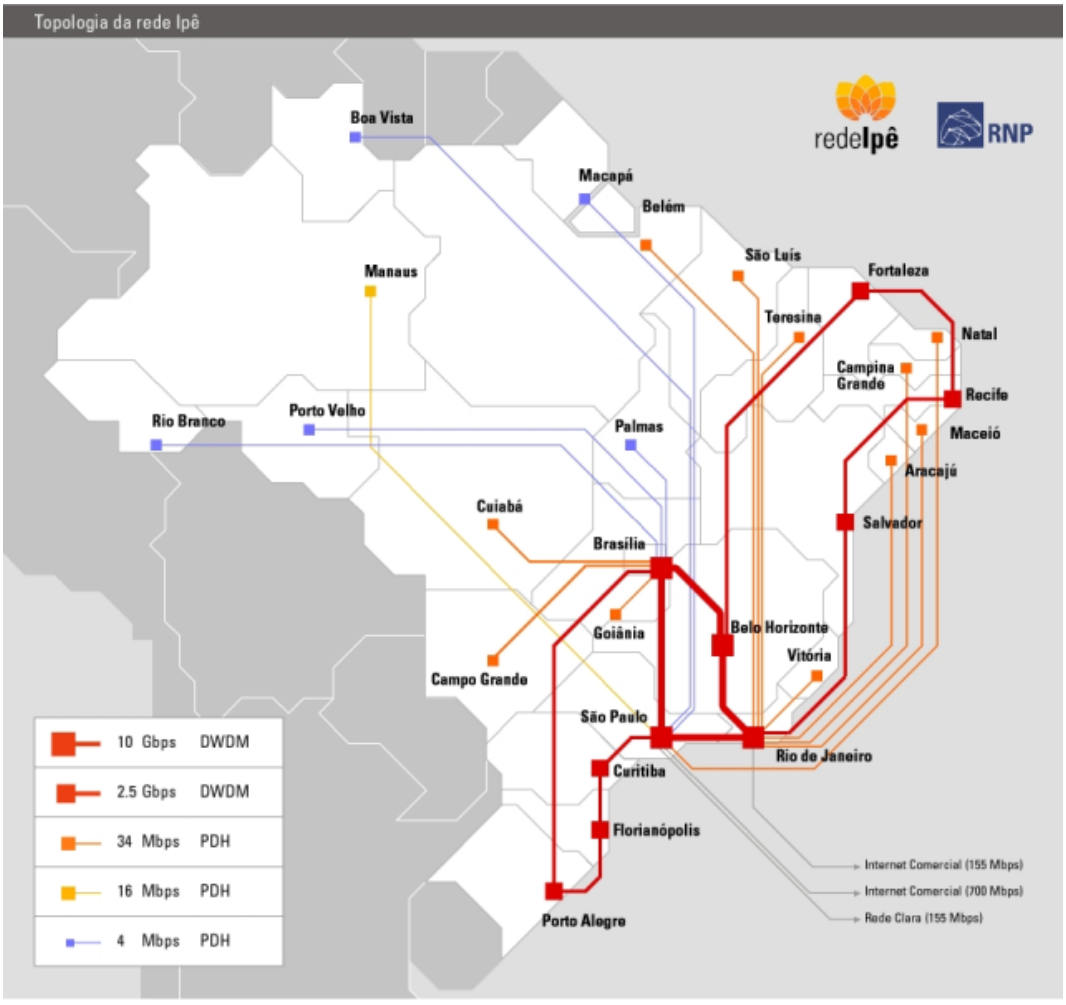


FIG. 3.6: RNP - 27 nós e 26 enlaces

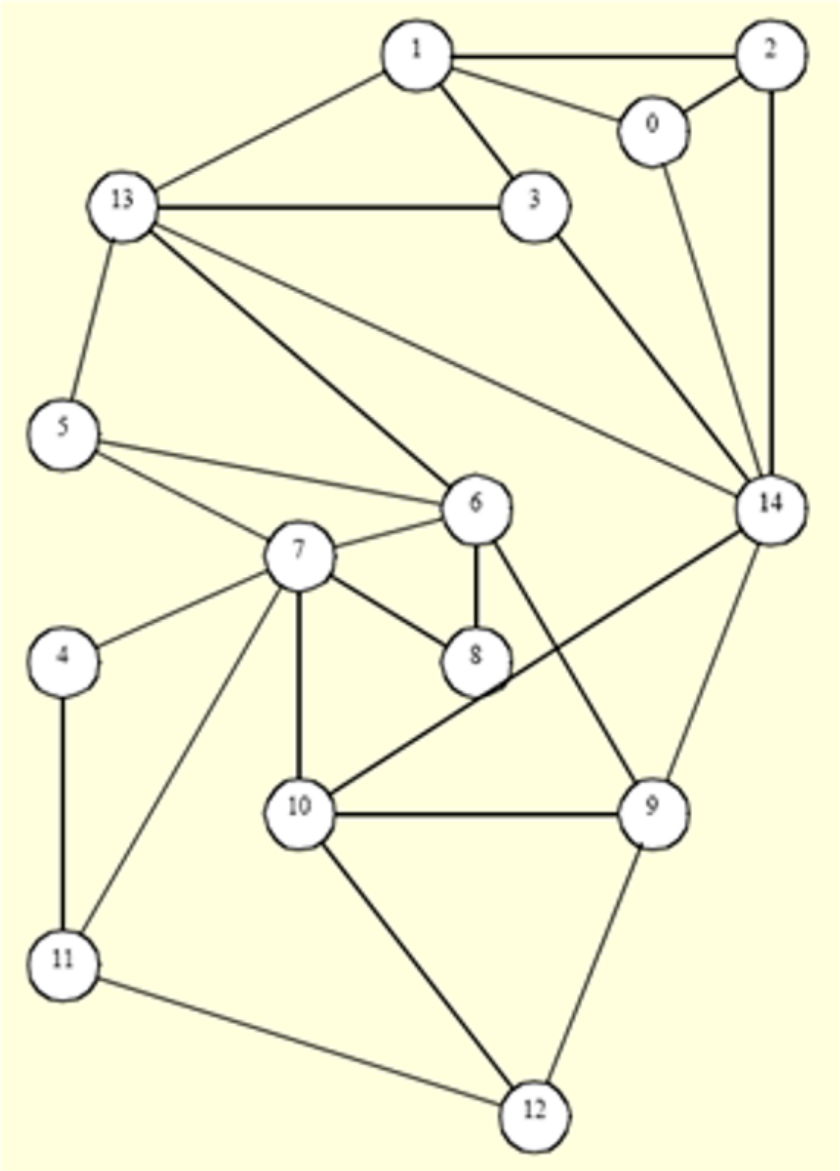


FIG. 3.7: Telcordia - 15 nós e 28 enlaces

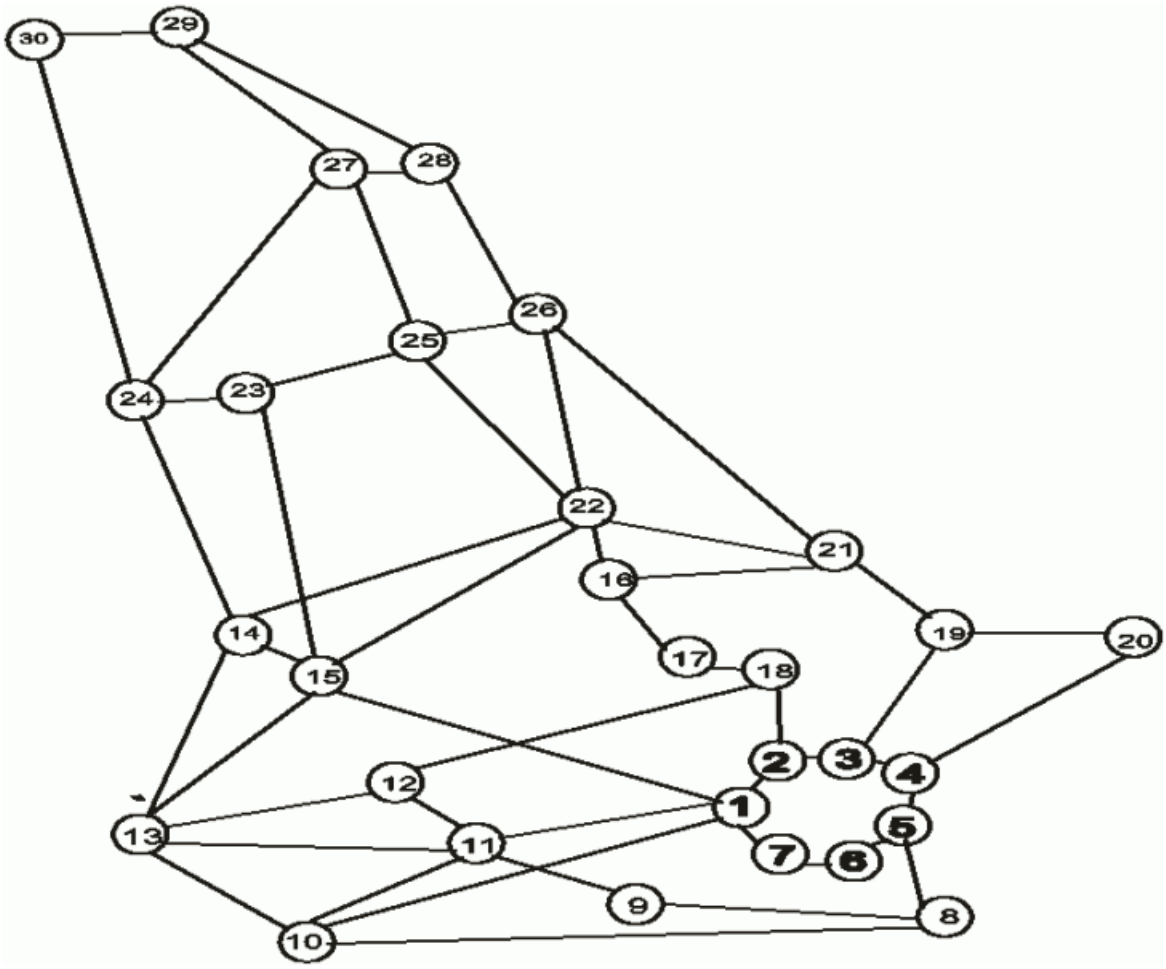


FIG. 3.8: UKNet - 30 nós e 51 enlaces

3.1.3 SOFTWARES UTILIZADOS NOS TESTES

Foram utilizados três softwares para os testes. O primeiro deles, código desenvolvido em linguagem C e batizado com o nome de Vertex, foi criado especialmente para o cálculo do Fator de Resiliência proposto nesta dissertação. O Vertex lê a matriz de conectividade de uma topologia de um arquivo no formato sociomatrix (MORENO, 1946). Utilizando como base a equação 3.1, realiza os testes de 2-conectividade até $(n-1)$-conectividade de uma topologia. Para cada combinação, calcula a quantidade de topologias conexas decorrentes dos testes. Computa percentual de testes conexos para cada combinação, totalizando o Fator de Resiliência. Indica se a topologia é conexa ou não, se é completa, e seu resultado detalhado permite identificar a k-conectividade "completa" da topologia.

O segundo software utilizado foi o SocNetV, na versão 0.51 (disponível em http://socnetv.sourceforge.net). SocNetV é o acrônimo para *Social Network Visualizer*, software de código aberto para visualização e análise de redes sociais. Permite desenhar um grafo e manipulá-lo, inserindo e removendo vértices e arestas. Foi extremamente útil para todos os testes de validação do Fator de Resiliência e para os testes com as estratégias de alteração de topologias. Para este trabalho, o SocNetV foi utilizado no cálculo dos parâmetros de *Degree Centrality*, *Closeness Centrality*, *Betweeness Centrality*, diâmetro, *Average Shortest Path*, além de mostrar as tabelas de menor caminho de todos os nós. O SocNetV possui um gerador de redes randômicas de Erdos-Renyi, gerador de redes *Small-World*, calcula o coeficiente de clusterização, densidade, *stress*, excentricidade, permite importação de dados de vários formatos, além de outros recursos.

O outro software utilizado neste trabalho foi desenvolvido em linguagem C e batizado com o nome de Random. Sua função foi de dar apoio a estratégia

de Remanejamento Preferencial de (BEYGELZIMER, 2005), na qual remove-se um enlace aleatório do nó de maior DC da rede para conectá-lo a um nó aleatório. O Random recebe na entrada a identificação numérica do nó com maior DC, a quantidade de enlaces conectados a este nó, a quantidade de nós da topologia e quantas combinações eram desejadas na saída. Sua saída gera uma quantidade de combinações (pseudo) aleatórias contendo cada uma a identificação numérica do enlace a ser removido do nó de maior DC e o enlace aleatório ao qual este enlace é reconectado.

3.1.4 AVALIAÇÃO DE RESULTADOS

A cada simulação de ataque, a topologia poderia indicar um novo estado. Esta verificação a cada teste foi importante para as avaliações, pois permitiu aferir a consistência de cada métrica, independente do estado da topologia. As tabelas 3.1, 3.2 e 3.3 indicam o estado de cada topologia após cada simulação de ataque.

TAB. 3.1: Status das topologias após cada simulação de ataque aos nós de maior DC

Topologias	**Ataque ao nó de maior DC**	**Ataque a 10% dos nós de maior DC**	**Ataque a 20% dos nós de maior DC**
Telcordia	Conexa	Conexa	Desconexa
Cost-239	Conexa	Conexa	Conexa
JaNet	Conexa	Desconexa	Desconexa
Renater	Desconexa	Desconexa	Desconexa
RNP	Desconexa	Desconexa	Desconexa
UKNet	Conexa	Conexa	Conexa

TAB. 3.2: Status das topologias após cada simulação de ataque aos nós de maior CC

Topologias	**Ataque ao nó de maior CC**	**Ataque a 10% dos nós de maior CC**	**Ataque a 20% dos nós de maior CC**
Telcordia	Conexa	Conexa	Desconexa
Cost-239	Conexa	Conexa	Conexa
JaNet	Conexa	Desconexa	Desconexa
Renater	Conexa	Desconexa	Desconexa
RNP	Desconexa	Desconexa	Desconexa
UKNet	Conexa	Desconexa	Desconexa

TAB. 3.3: Status das topologias após cada simulação de ataque aos nós de maior BC

Topologias	**Ataque ao nó de maior BC**	**Ataque a 10% dos nós de maior BC**	**Ataque a 20% dos nós de maior BC**
Telcordia	Conexa	Conexa	Desconexa
Cost-239	Conexa	Conexa	Conexa
JaNet	Conexa	Desconexa	Desconexa
Renater	Conexa	Desconexa	Desconexa
RNP	Desconexa	Desconexa	Desconexa
UKNet	Conexa	Conexa	Desconexa

Os gráficos apresentados nas Figs. 3.9, 3.10 e 3.11 utilizam como métrica de resiliência o AISPL. Foi identificada uma boa variação na remoção de nós de maior importância, porém foram detectadas algumas inconsistências. Inicialmente, percebeu-se que para várias topologias, foram encontrados valores similares de resiliência, o que não atende à necessidade de uma métrica que possa diferenciar estas estruturas. As inconsistências percebidas ocorreram quando a remoção de nós deixou a topologia desconexa, fato que foi identificado na remoção de 20% dos nós de maior DC, CC e BC para a topologia Telcordia, JaNet, Renater, RNP e UKNet. O valor do AISPL foi incrementado, o que daria a falsa impressão de melhoria na resiliência. Isto

ocorre devido ao fato do AISPL ser calculado no LCC, ou no maior subgrafo resultante da topologia desconexa. Esta forma de cálculo do AISPL segue fielmente o método do trabalho de (BEYGELZIMER, 2005). Isto mostra que o AISPL é consistente apenas em avaliações de topologias conexas, ou seja, caso um ataque desconecte a topologia, o AISPL fornecerá um valor não condizente com a situação da rede.

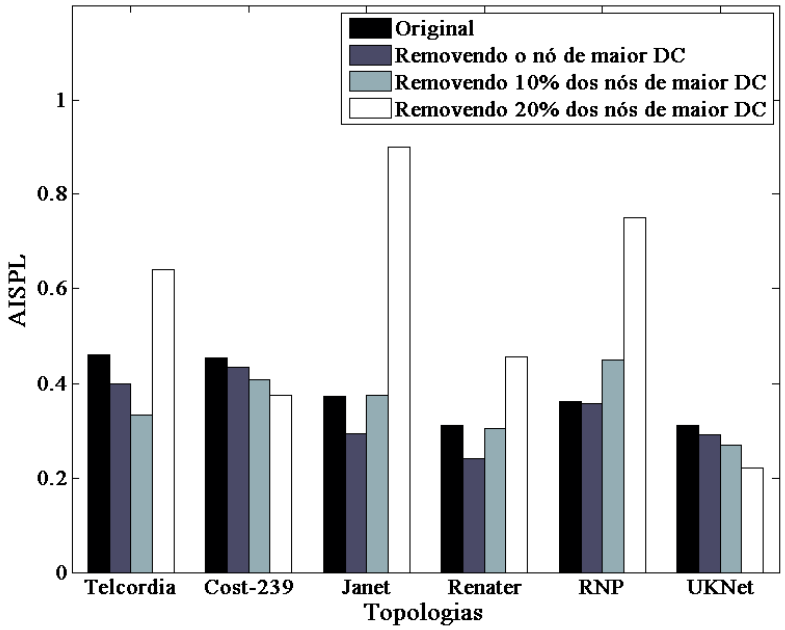


FIG. 3.9: AISPL em ataques ao nó de maior DC

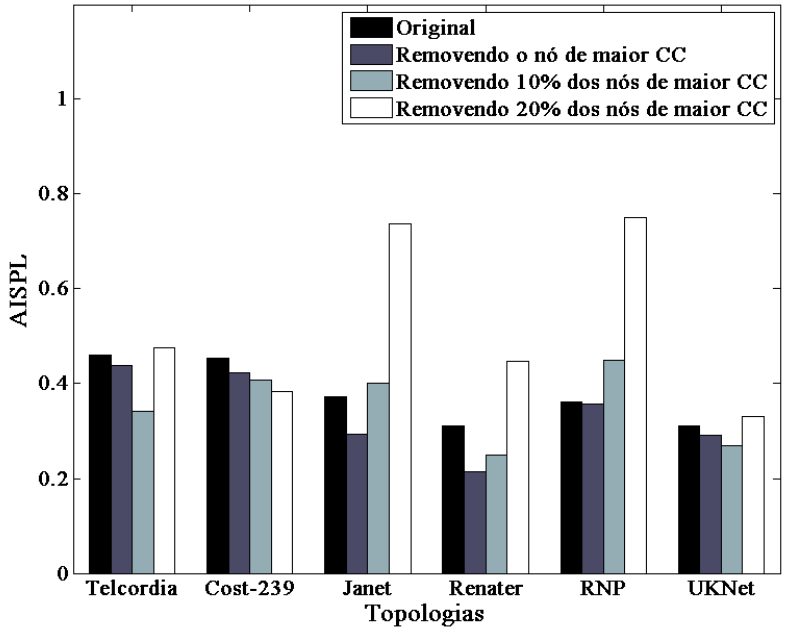


FIG. 3.10: AISPL em ataques ao nó de maior CC

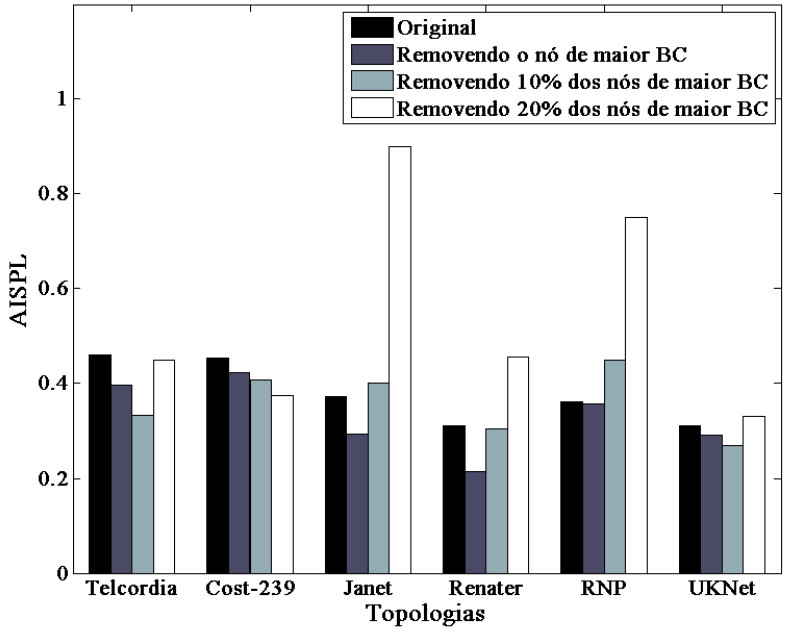


FIG. 3.11: AISPL em ataques ao nó de maior BC

Os resultados obtidos utilizando a métrica LCC, verificados nos gráficos das Figs. 3.12, 3.13 e 3.14, indicaram que nas situações que a rede se torna desconexa, ela reflete as variações, com uma queda mais acentuada nestes casos. Porém, no caso de uma comparação entre as topologias enquanto conexas, não existe diferença entre estas. O valor será o mesmo para todas as topologias originais. Ainda na comparação entre topologias conexas, ao serem removidos nós na simulação de ataques, o valor do LCC é decrementado de acordo com o percentual de nós atacados, impossibilitando uma comparação mais detalhada.

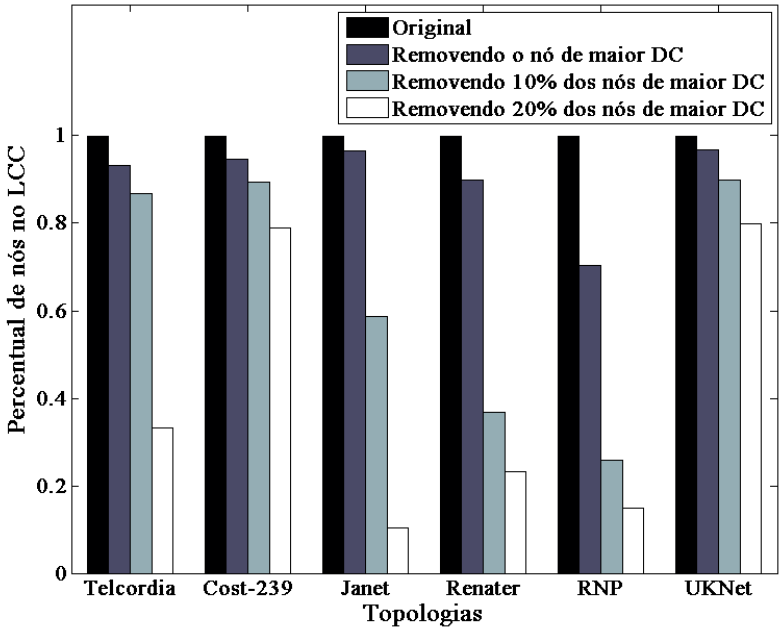


FIG. 3.12: LCC em ataques ao nó de maior DC

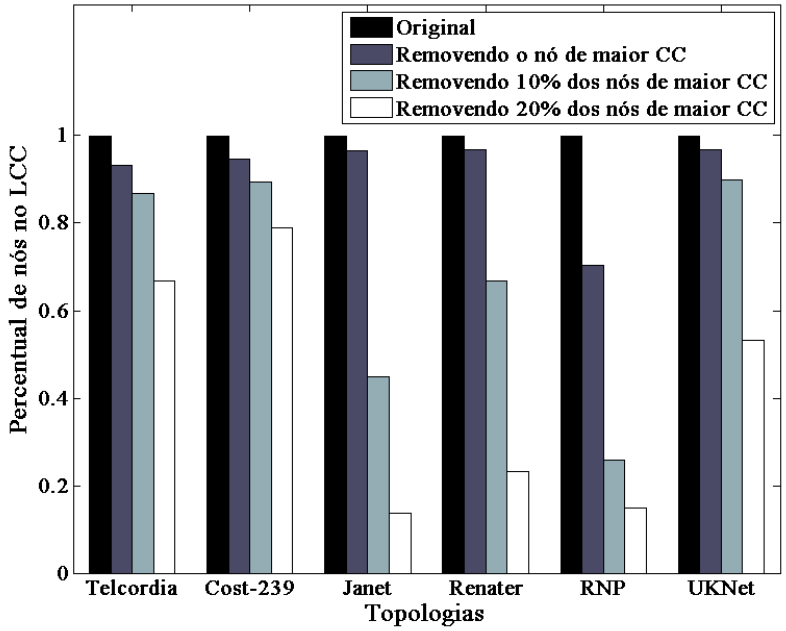


FIG. 3.13: LCC em ataques ao nó de maior CC

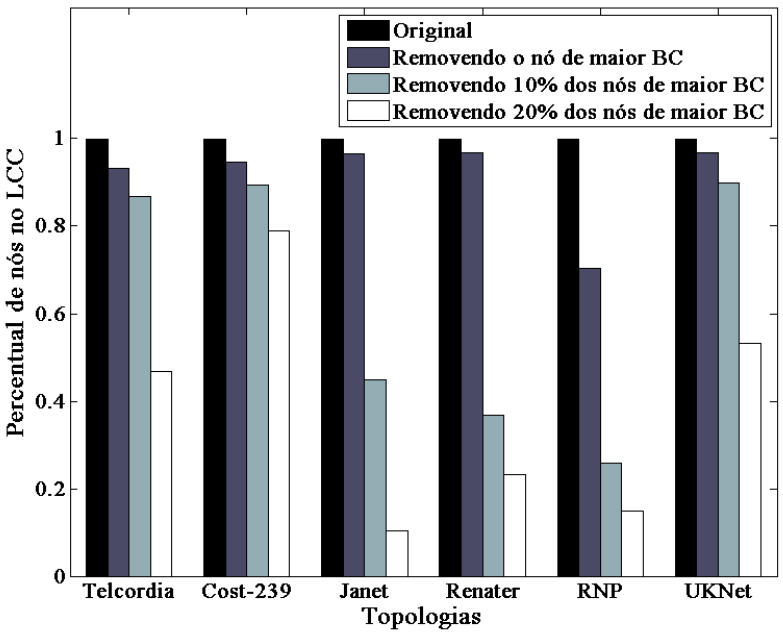


FIG. 3.14: LCC em ataques ao nó de maior BC

As avaliações realizadas utilizando a métrica diâmetro (Figs. 3.15, 3.16 e 3.17) indicaram que, da mesma forma que o AISPL, o diâmetro foi inconsistente ao avaliar situações em que a topologia se tornou desconexa. Isto se deve também ao fato do diâmetro ser calculado no LCC. Nas situações em que o diâmetro se mostrou consistente, apresentou valores similares para várias topologias, da mesma forma que as métricas até aqui apresentadas.

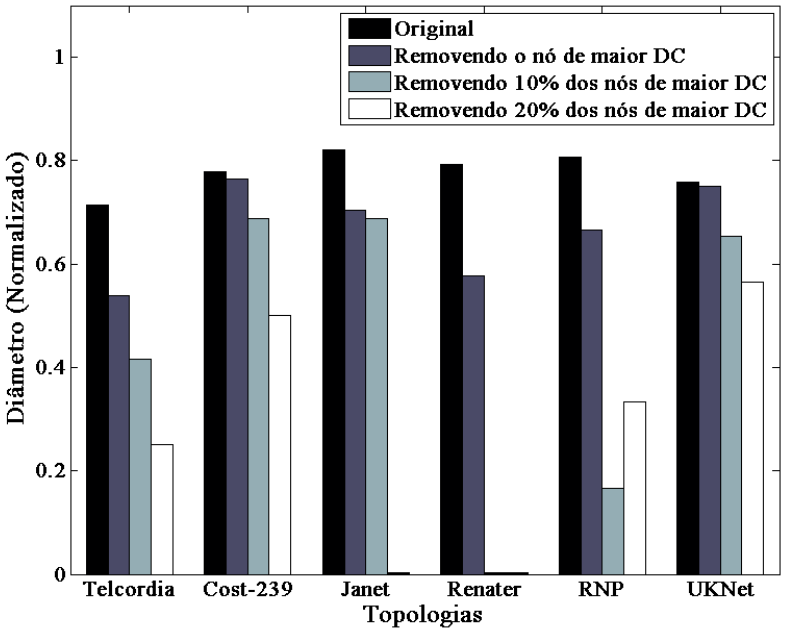


FIG. 3.15: Diâmetro em ataques ao nó de maior DC

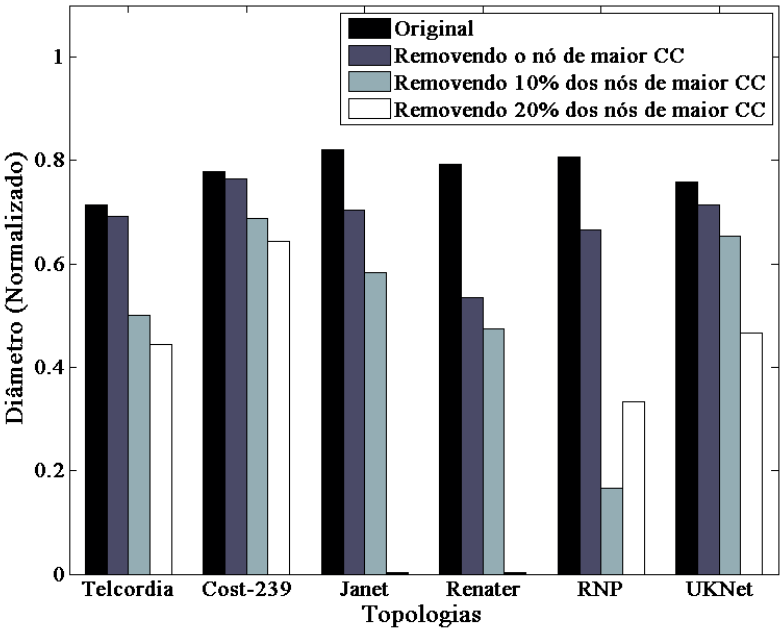


FIG. 3.16: Diâmetro em ataques ao nó de maior CC

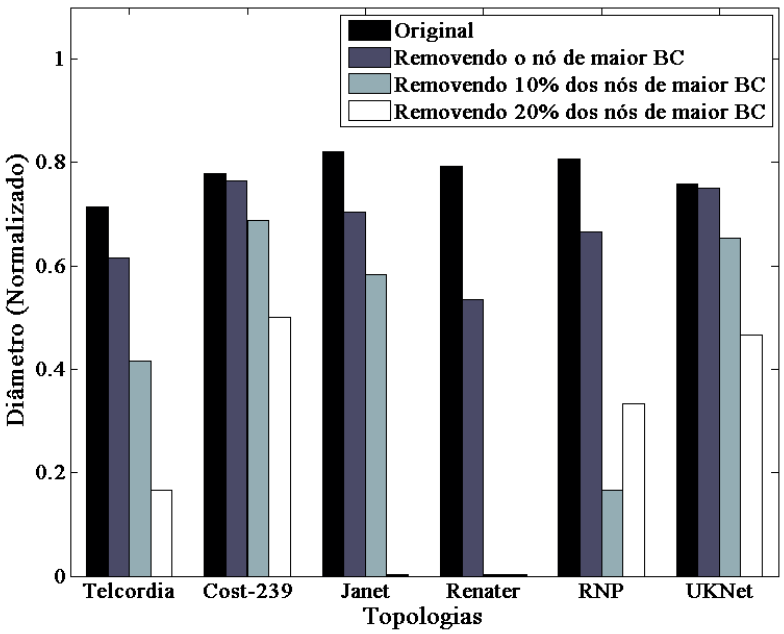


FIG. 3.17: Diâmetro em ataques ao nó de maior BC

O Fator de Resiliência foi a métrica mais consistente em todos os testes, nas variações de ataques, estando conexa ou desconexa, e ainda apresentou uma boa variação nas simulações e no próprio estado original da topologia, permitindo a comparação entre várias redes. As Figs. 3.18, 3.19 e 3.20 mostram os testes com o FR.

A Telcordia apresentou FR no valor de 0,4534, indicando que, de todos os testes com as combinações de 2-conectividade a 14-conectividade (são 15 nós no total), em 45,34% ela se manteve conexa, o que representa uma boa resiliência se comparada com as outras que foram testadas. Apenas nos testes com a remoção de 20% dos nós de maior DC, CC e BC, a topologia ficou desconexa, o que pode ser percebido com a queda acentuada do FR, mostrada nos gráficos.

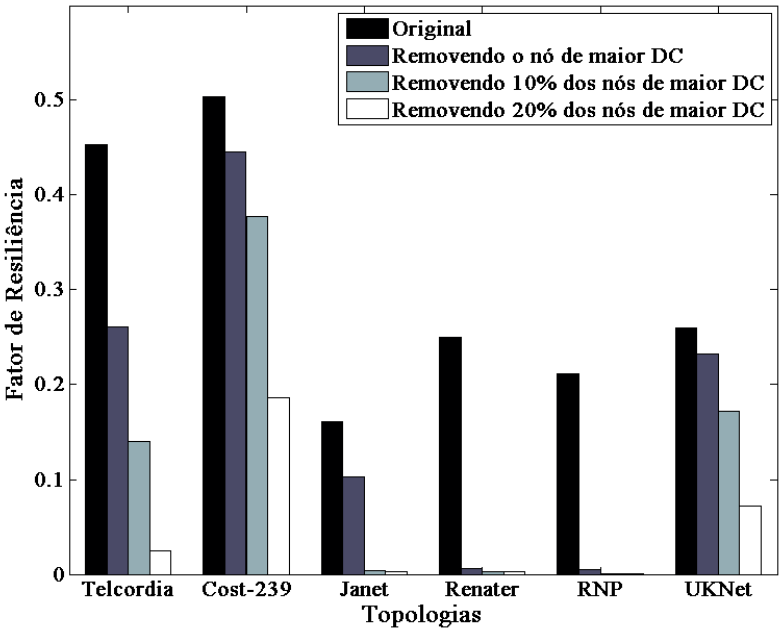


FIG. 3.18: FR em ataques ao nó de maior DC

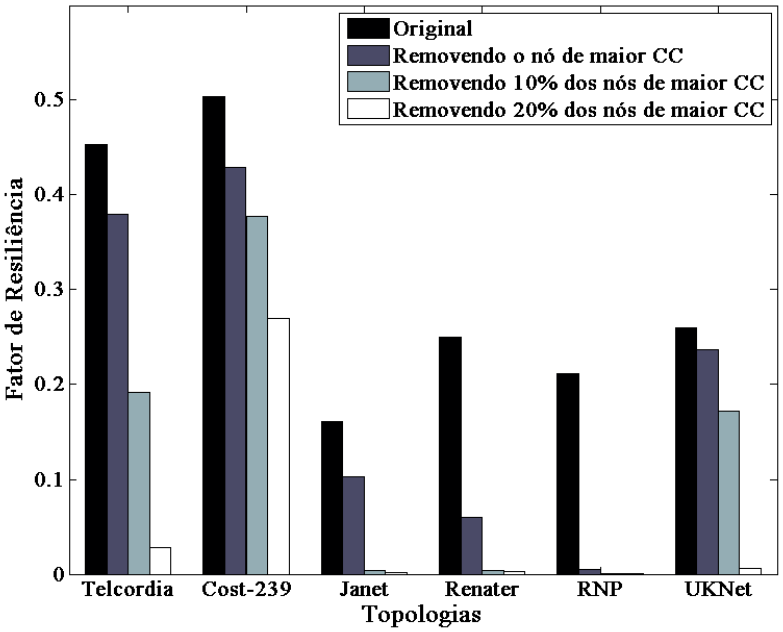


FIG. 3.19: FR em ataques ao nó de maior CC

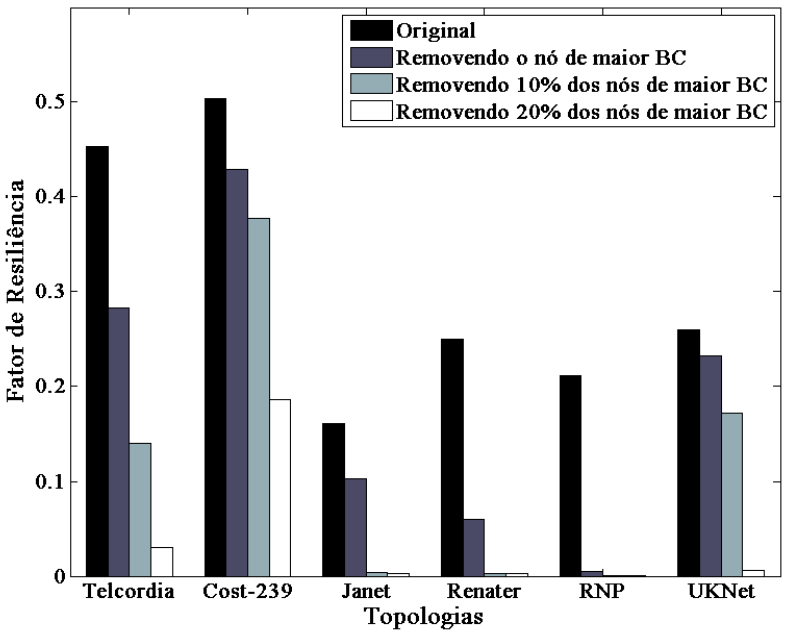


FIG. 3.20: FR em ataques ao nó de maior BC

A Cost-239 foi a topologia de maior FR, com 0,5042 e a que se manteve conexa em todos os testes de remoção de nós, para todos os tipos de medidas de centralidade. Apresentou variações no FR quando das simulações de ataques. Uma importante informação acerca da Cost-239 é que a topologia foi planejada para ser usada pelo meio acadêmico europeu, o que pode explicar seu bom FR e boa tolerância a ataques.

Em contraste com a Cost-239, a JaNet foi a topologia de menor FR, com 0,1608, e demonstrou uma grande dependência do nó Leeds, identificado como nó de maior DC, CC e BC. A remoção do nó Leeds ocasionou a desconexão da topologia, demonstrado pela queda no FR. Outra importante informação, percebida nas topologias em geral, é que a queda pode não ser tão acentuada com a desconexão da topologia, pois, dependendo do desenho da mesma, a quantidade de nós desconectados pode ser pequena, permitindo uma grande quantidade de nós restantes no LCC. A indicação de uma queda no FR, aliada ao estado da topologia (conexa/desconexa), pode fornecer uma melhor avaliação da rede.

A Renater apresentou FR com valor de 0,2505. Mostrou baixa tolerância a ataques ao ser muito dependente dos nós Paris e Lyon. A remoção do nó Paris (nó com maior DC da rede) causou a desconexão da topologia. O gráfico refletiu corretamente as simulações de ataque.

A brasileira RNP tem FR com valor de 0,2120 e uma grande dependência do nó Rio de Janeiro, sendo o maior DC, CC e BC da rede. A queda do nó Rio de Janeiro causou a desconexão de outros 7 nós (Vitória, Salvador, Aracaju, Campina Grande, Belém, São Luiz e Teresina). Uma análise visual da RNP mostra que a topologia possui uma grande quantidade de subgrafos acíclicos, o que causa uma baixa tolerância a ataques.

Por fim, a UKNet possui FR com valor de 0,2601. Nas simulações de

ataque, tornou-se desconexa apenas no teste de 20% dos nós com maior DC, CC e BC.

3.2 COMPARAÇÃO DE MÉTRICAS

Na comparação direta das métricas, foram escolhidas situações em que elas se mostraram consistentes. A razão desta escolha foi a de utilizar as métricas nos seus melhores casos e compará-las com o FR, mostrando que o fator proposto é tão bom quanto as métricas enquanto consistentes. O AISPL e o diâmetro foram consistentes nas simulações que não desconectavam a topologia e o LCC foi consistente mesmo quando a simulação de ataques desconectou a rede.

No caso da comparação entre a FR e a AISPL, comparamos as situações em que a rede se manteve conexa mesmo na remoção de nós. Desta forma, foram utilizadas as topologias Telcordia (Fig. 3.7) e Cost-239 (Fig. 3.3) na remoção dos nós de maior DC, CC e BC, além da remoção de 10% dos nós de maior DC, CC e BC.

Nos testes comparativos realizados com a topologia Telcordia (Fig. 3.21), o Fator de Resiliência refletiu corretamente a remoção dos nós, com boa diferença nos testes. Da mesma forma, a AISPL sofreu queda na remoção de nós, apesar da pouca variação. Nos testes com a Cost-239 (Fig. 3.22), também foi conferida a mesma tendência de variação para o FR e para o AISPL.

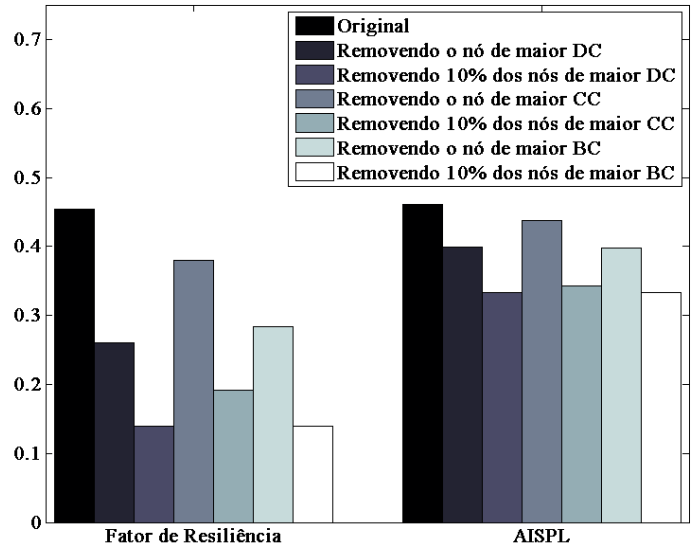


FIG. 3.21: Telcordia - Comparação entre o Fator de Resiliência e o AISPL

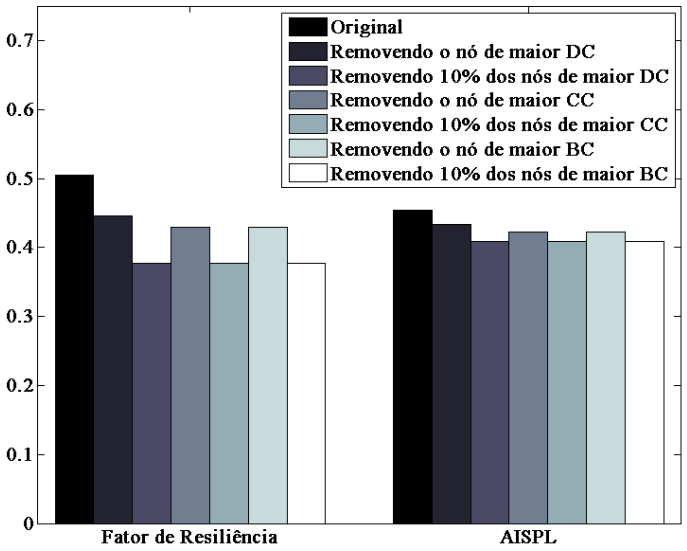


FIG. 3.22: Cost-239 - Comparação entre o Fator de Resiliência e o AISPL

Os testes de DC, CC e BC tanto para o FR como para o AISPL foram

muito similares, pois nestas topologias alguns nós possuem mais de uma característica de centralidade.

Na comparação direta entre o FR e o LCC, foram utilizadas topologias que se tornaram desconexas após a remoção de nós. A JaNet e a Renater foram as escolhidas para esta comparação. Mais uma vez o Fator de Resiliência foi mais significativo na diferenciação dos resultados. A topologia JaNet ficou desconexa com a remoção de 10% dos nós de maior DC, CC e BC (Fig. 3.23). O LCC sofreu queda, mas não se mostrou tão significativa. O mesmo nó na topologia Janet é o maior DC, CC e BC. No caso da Renater, o gráfico mostrou comportamento semelhante (Fig. 3.24), indicando uma maior variação quando a topologia fica desconexa.

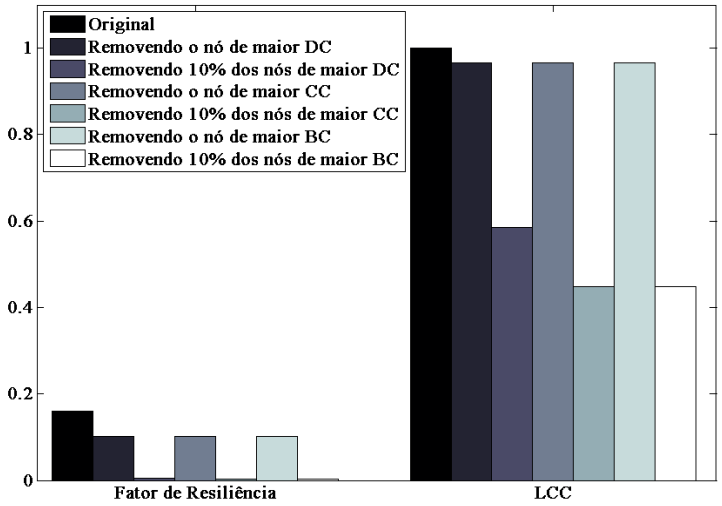


FIG. 3.23: JaNet - Comparação entre o Fator de Resiliência e o LCC

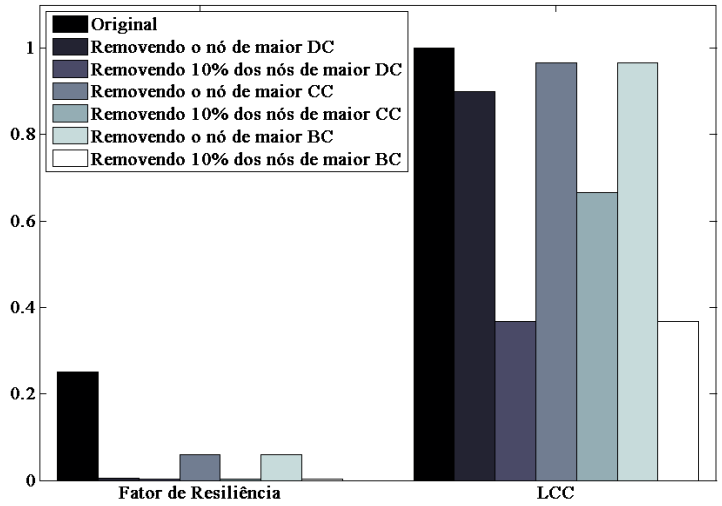


FIG. 3.24: Renater - Comparação entre o Fator de Resiliência e o LCC

Na comparação do FR com o diâmetro, foram utilizadas novamente as topologias Telcordia e Cost-239, através dos gráficos das Figs. 3.25 e 3.26.

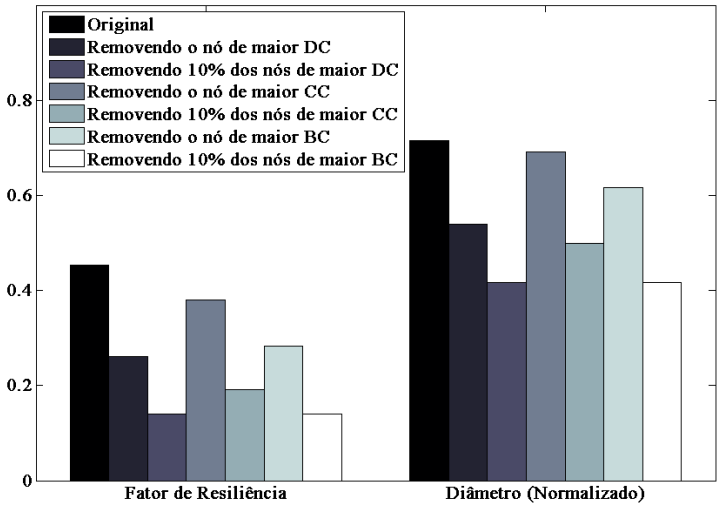


FIG. 3.25: Telcordia - Comparação entre o Fator de Resiliência e o Diâmetro

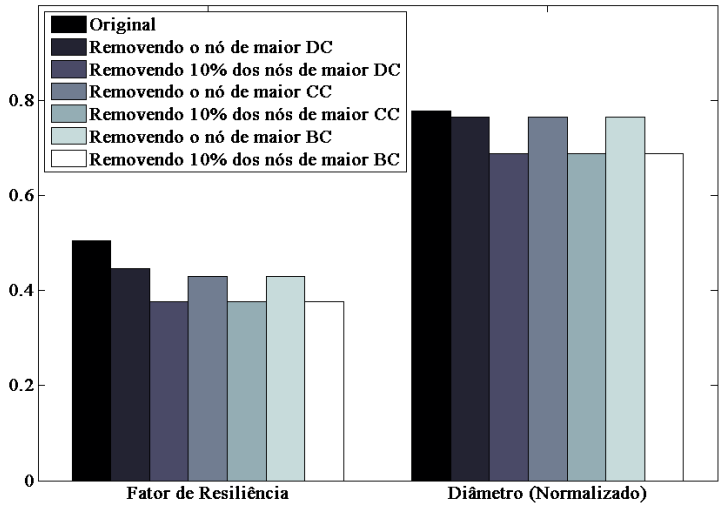


FIG. 3.26: Cost-239 - Comparação entre o Fator de Resiliência e o Diâmetro

O diâmetro também mostrou inconsistência em redes desconexas, da mesma forma que o AISPL.

Analisando os resultados obtidos, verificou-se que o Fator de Resiliência foi consistente em todos os testes apresentados, para qualquer estado da topologia. O cálculo do Fator de Resiliência indicou um valor que reflete a robustez de uma rede. Além disso, foi mais preciso que outras métricas na comparação de topologias, permitindo a diferenciação da resiliência entre elas. As métricas do trabalho de (BEYGELZIMER, 2005) apresentaram vários problemas, principalmente relacionados ao estado da topologia após sofrer um ataque ou devido a falha em um nó importante da rede. Os resultados obtidos das métricas AISPL, LCC e diâmetro não indicaram de forma correta a resiliência de uma rede, podendo ser utilizados apenas em conjunto com outros parâmetros e em situações específicas. Por este motivo, o Fator de Resiliência foi utilizado como métrica para avaliação das estratégias de alteração de topologia que são abordadas no próximo capítulo.

4 ESTRATÉGIAS PROPOSTAS PARA A ALTERAÇÃO DE TOPOLOGIAS

Neste capítulo são discutidas as abordagens utilizadas no trabalho de (BEYGELZIMER, 2005) para alteração de topologias e, em seguida, apresentadas as estratégias propostas nesta dissertação.

4.1 ESTRATÉGIAS UTILIZADAS POR BEYGELZIMER ET AL.

O trabalho citado apresenta seis abordagens diferentes de modificação de topologias. Duas estratégias inserem novos enlaces e outras quatro remanejam enlaces já existentes. São elas:

- Inserção
  - Inserção Aleatória de Enlaces - Adiciona novo enlace conectando dois nós aleatórios, não conectados entre si.
  - Inserção Preferencial de Enlaces - Adiciona novo enlace conectando dois nós, não conectados entre si, que possuam o menor grau na rede.
- Remanejamento
  - Remanejamento Aleatório de Enlaces - Remove um enlace aleatório entre dois nós e o insere aleatoriamente entre dois nós não conectados entre si.
  - Remanejamento Aleatório de Enlace Vizinho - Escolhe um nó aleatório, deste nó escolhe um vizinho aleatório e remove o en-

lace entre eles. Insere o enlace removido entre dois nós aleatórios, não conectados entre si.

- Remanejamento Preferencial de Enlaces - Desconecta um enlace aleatório do nó de maior grau e reconecta a um nó aleatório.
- Remanejamento Preferencial de Enlace Aleatório - Escolhe um enlace aleatório, o desconecta do nó com maior grau e o reconecta a um nó aleatório.

O trabalho referenciado utiliza as métricas descritas anteriormente para avaliar as alterações sugeridas em seu trabalho. As topologias usadas em seus testes foram a Gnutella, rede P2P de topologia dinâmica, em dois *snapshots* parciais, um com 435 nós e 459 enlaces, e outro com 737 nós e 803 enlaces. A outra topologia usada nos testes foi criada pelo gerador de topologias Inet 3.0, com 3.500 nós e 5.667 enlaces, utilizando dados de distribuição de grau da Internet. Cada abordagem proposta foi testada em condições específicas e de acordo com a métrica usada, refletindo as restrições e inconsistências destas métricas para indicar a robustez de uma rede. Esta dissertação apresenta um resumo dos resultados encontrados no trabalho referenciado para possibilitar o confronto com as estratégias propostas.

4.1.1 ESTRATÉGIAS DE REMANEJAMENTO DE ENLACES

Para os testes com a métrica LCC, foi utilizada topologia gerada pelo Inet 3.0 em três níveis de ataque, 0%, 1%, 10% e 20% dos nós de maior grau. Das quatro estratégias de remanejamento, a de Remanejamento Preferencial foi superior a todas. Foram também realizados testes com falhas aleatórias em 1%, 10% e 20% dos enlaces e, na comparação entre o Remanejamento Preferencial e o Remanejamento Aleatório de Enlaces, o primeiro confirmou os melhores resultados.

Para os testes com a métrica AISPL, foi utilizado um *snapshot* da Gnutella com 737 nós e 803 enlaces. Na simulação de ataques, testou o AISPL com a remoção de 1%, 3% e 5% dos nós de maior grau. Na simulação de falhas, utilizou os mesmos percentuais na remoção de nós aleatórios. Em todas as estratégias de remanejamento utilizadas, o Remanejamento Preferencial também foi o melhor resultado.

4.1.2 ESTRATÉGIAS DE INSERÇÃO DE ENLACES

Para os testes com a métrica LCC, foi utilizada a mesma topologia gerada pelo Inet 3.0 em três níveis de ataque, em 1%, 10% e 20% dos nós de maior grau. Da mesma forma que os testes de remanejamento, a estratégia de escolha preferencial de enlaces foi superior à estratégia de escolha aleatória. Portanto, a estratégia de Inserção Preferencial foi a de melhor resultado.

Para os testes com a métrica AISPL, o trabalho referenciado utilizou 3 *snapshots* da Gnutella com 435 nós e 459 enlaces. Simulou ataques em 5% dos nós de maior grau e inseriu gradualmente enlaces na topologia. A estratégia de Inserção Preferencial também foi a melhor opção nos testes.

4.1.3 ANÁLISE DOS RESULTADOS E MÉTODO DE TESTES

Nos testes com as duas métricas, as estratégias de Remanejamento Preferencial e Inserção Preferencial obtiveram os melhores resultados. A estratégia de remanejamento aleatório só obteve bons resultados depois de uma grande quantidade de passos. A estratégia de inserção aleatória só atingiu bons valores de resiliência (usando as métricas escolhidas) a medida que aproximavam a topologia de um grafo completo.

Em análise ao método utilizado nos testes, verificamos que tanto no re-

manejamento como na inserção e para qualquer das topologias utilizadas, a quantidade de passos de testes era sempre duas vezes a quantidade de enlaces das topologias. Por exemplo, analisando o teste de remanejamento de enlaces na topologia gerada pelo Inet 3.0, a quantidade de remanejamentos foi superior a 10.000, sendo que a topologia possuía 5.667 enlaces. Esta simulação não é viável na prática, servindo apenas de base teórica e demonstração das estratégias utilizadas pelos autores.

4.2 ESTRATÉGIAS PROPOSTAS

Como estratégias propostas, é utilizado o remanejamento e a inserção de enlaces com diferentes abordagens. Da mesma forma que nos testes realizados com simulações de ataques que utilizamos para validar o Fator de Resiliência, as medidas de centralidade apresentadas anteriormente são utilizadas como base para as estratégias de modificação de topologias.

Um ponto importante nas estratégias propostas nesta dissertação é a quantidade de modificações necessárias para o aumento da resiliência. Nos testes realizados por (BEYGELZIMER, 2005) foram feitas simulações em redes criadas por geradores de topologia, ou em *snapshots* da rede Gnutella, nas quais centenas de enlaces eram remanejados ou inseridos. A mudança contínua da topologia utilizando qualquer uma das estratégias, tanto as propostas pelo trabalho referenciado como as propostas nesta dissertação, tende a estabilizar a rede retirando a importância de alguns nós e aumentando a importância de outros. Esta estabilização tornará a rede mais resiliente. Um dos diferenciais das estratégias propostas neste trabalho ocorre na quantidade necessária de alterações para a melhoria da resiliência. Os testes realizados com as estratégias propostas indicaram que uma pequena quantidade de alterações na topologia pode tornar a rede mais robusta se comparadas com

as outras.

Os próximos tópicos apresentam o detalhamento destas estratégias e em seguida uma análise dos testes e resultados obtidos.

4.2.1 PROPOSTA DE REMANEJAMENTO DE ENLACES

O remanejamento de enlaces é uma alternativa de alteração de topologia que possivelmente gera menor custo financeiro para as empresas, comparada com a contratação de um novo enlace. Esta abordagem porém, pode não alcançar bons resultados em alguns desenhos de topologias, pois pode alterar redundâncias que foram inseridas no projeto da infraestrutura. Além da proposta de uma nova estratégia de remanejamento de enlaces, pondera-se que, caso este remanejamento não seja satisfatório, o enlace será retornado ao estado anterior e uma segunda ou terceira alternativa será utilizada buscando a melhoria da resiliência.

O trabalho referenciado utilizou em suas estratégias preferenciais o conceito de DC (*Degree Centrality*) que indica o grau do nó. No Remanejamento Preferencial, um enlace aleatório conectado a um nó de maior DC era removido para ser conectado a outro nó também aleatório. Esta abordagem indica que o nó escolhido teria um decréscimo no seu grau, permitindo concluir que a estratégia procura diminuir a importância do nó de maior DC. Caso a conexão deste enlace removido fosse feita a um nó de menor DC, e não aleatoriamente como propõem os autores, seria possível a equalização do grau dos nós a medida que novos remanejamentos ocorressem. Desta forma, a topologia teria uma melhor regularidade de grau em seus nós, e consequentemente melhoraria o Fator de Resiliência.

Outro ponto a ser questionado na estratégia de Remanejamento Prefe-

rencial é a escolha aleatória de um enlace conectado ao nó de maior DC. Caso fosse feita uma análise dos vizinhos do nó de maior DC, poderíamos escolher o enlace que seria removido para que esta estratégia tivesse melhores resultados. Utilizando uma outra medida de centralidade, o CC (*Closeness Centrality*), ou proximidade do centro, este trabalho propõe uma melhor escolha de enlace a ser desconectado do nó com maior DC da rede. Os nós com maior grau de proximidade do centro possuem uma menor distância geodésica para todos os nós da rede. Estes nós funcionariam como "atalhos" para os outros nós da topologia. A proposta é desconectar do nó com maior DC o enlace conectado ao nó de maior CC e ligando este enlace ao nó de menor DC da rede. Portanto, como estratégia de Remanejamento Proposto:

Estratégia .1. *Desconectar do nó de maior degree centrality o enlace conectado ao nó adjacente de maior closeness centrality e reconectá-lo ao nó de menor degree centrality da rede.*

Desta forma, procura-se atingir os seguintes objetivos:

- Diminuir o grau do nó com maior DC da rede, consequentemente diminuir também a dependência da topologia deste;
- Aumentar o grau do nó com menor DC da rede, visando regularizar a topologia;
- Diminuir o diâmetro da rede, já que um nó com maior CC possui menor caminho para todos os outros nós da rede.

A estratégia de remanejamento pode, em alguns casos, causar um decréscimo na resiliência da topologia. Redes com topologia em anel diminuiriam o anel e introduziriam subgrafos acíclicos, o que causaria uma quantidade maior de combinações que deixariam a rede desconexa. Portanto,

caso o remanejamento de enlaces cause a diminuição do Fator de Resiliência, conclui-se que a estratégia não é indicada.

4.2.2 PROPOSTA DE INSERÇÃO DE ENLACES

A melhor estratégia de aumento de resiliência é, sem dúvida, a inserção de enlaces. O grau dos nós da rede é uma importante métrica na avaliação de sua robustez. Os nós de menor DC da rede serão sempre um ponto de redução da resiliência pois a sua queda ou a queda de um enlace conectado a ele poderá causar a desconexão de uma topologia. O grau do nó é um limitador da k-conectividade "completa". Por exemplo, se o grau mínimo dos nós de uma topologia for igual a 2, a rede poderá ser 1-conexa ou 2-conexa, mas nunca 3-conexa, pois um nó que tenha grau 2 ficará desconexo quando removermos uma determinada combinação de 2 nós no teste da 3-conectividade. (DEKKER, 2004b) apresenta em seu trabalho um teorema retirado do livro de (GIBBONS, 1985):

Teorema 4.1. *Para todo e qualquer grafo,* $\kappa \leq \lambda \leq d_{min}$.

O valor de κ refere-se à k-conectividade, λ refere-se à k-aresta-conectividade e d_{min} ao grau mínimo dos nós de um grafo. A k-aresta-conectividade é conceito similar ao da k-conectividade, mas considerando a aresta e não o vértice. (DEKKER, 2004b) afirma que, caso um grafo tenha a característica de $\kappa = \lambda = d_{min}$ ele é um grafo "otimamente conectado", por possuir as características de um grafo completo. Portanto, a simples inserção de enlaces, na estratégia de aumentar o grau dos nós de menor DC da rede, torna a rede mais resiliente.

Na estratégia de Inserção Preferencial de (BEYGELZIMER, 2005), é inserido um enlace entre os nós de menor DC da rede. Esta abordagem procura

regularizar o grau dos nós da rede da mesma forma que na abordagem anterior, e consequentemente insere redundância nos caminhos para todos os nós da topologia. Porém, a melhoria da resiliência da rede pode não ser siginificativa, pois os nós conectados podem estar situados na extremidade da rede, o que não causaria impacto no diâmetro e nas tabelas de roteamento dos nós. A estratégia proposta utiliza novamente o conceito de proximidade do centro (CC). Ao invés de conectar os dois nós de menor grau da rede, é inserido enlace entre o nó de menor DC da rede e o nó de menor CC. Portanto, como estratégia de Inserção Proposta:

Estratégia .2. *Inserir enlace conectando o nó de menor degree centrality com o nó de menor closeness centrality da rede.*

Desta forma procura-se atingir os seguintes objetivos:

- Aumentar o grau do nó com menor DC da rede, visando regularizar o grau da topologia;
- Aumentar a proximidade do nó de menor CC da rede, caso o nó de menor DC esteja na borda da topologia ou mesmo se este estiver mais ao centro, diminuindo o diâmetro da rede.

4.3 TESTES COMPARATIVOS DAS ESTRATÉGIAS

Os testes foram realizados em três topologias reais, já utilizadas nos testes do Fator de Resiliência. As escolhidas foram a Cost-239 (Fig. 3.3), a Telcordia (Fig. 3.7) e a RNP (Fig. 3.6), cada uma com uma característica específica. A Cost-239 foi escolhida por ter um grau médio alto (4,21), e permitir avaliar se as estratégias apresentadas podem melhorar o Fator de Resiliência de uma rede já robusta. A Telcordia foi escolhida por ser um

textitbackbone comercial, e a RNP por sua grande quantidade de subgrafos acíclicos e grande concentração de conexões em dois nós da rede, Rio de Janeiro e São Paulo. Foi utilizado o Fator de Resiliência (FR) como métrica para verificar se as alterações realizadas surtiram o efeito desejado.

Os testes compararam as estratégias escolhidas pelo trabalho referenciado com as estratégias propostas nesta dissertação. As estratégias de (BEYGELZIMER, 2005) são referenciadas como Inserção Beygelzimer et al. e Remanejamento Beygelzimer et al., chamado pelos autores respectivamente de Inserção Preferencial e Remanejamento Preferencial. As estratégias propostas nesta dissertação também baseiam-se em abordagens preferenciais e, por este motivo, sua referência foi alterada. As estratégias propostas são referenciadas por Inserção Proposta e Remanejamento Proposto.

O método de testes do trabalho referenciado foi integralmente respeitado nesta dissertação, sendo as únicas diferenças a métrica de resiliência e a quantidade de passos para cada estratégia utilizada. Para cada uma das topologias testadas foi utilizado o Fator de Resiliência inicial, sendo recalculado a cada passo de alteração realizada. Foram testadas as quatro estratégias para cada topologia, sendo que cada estratégia executou cinco passos. Os resultados auferidos para cada topologia são apresentados em um gráfico contendo quatro curvas de variação do Fator de Resiliência em cinco passos de alterações.

Em todos os testes das estratégias propostas foram encontrados nós com caraterísticas similares, ou seja, dois ou mais nós de mesmo valor de DC ou CC. Em todos estes casos foram realizados testes com todas as possibilidades, excluindo as inserções ou remanejamentos de enlaces já conectados. Desta forma foi escolhido o melhor fator de resiliência resultante, dentro da estratégia apresentada.

Nos testes das topologias foram geradas matrizes de conectividade no

formato sociomatrix (MORENO, 1946) pelo software SocNetV versão 0.51. Os cálculos do fator de resiliência foram realizados pelo software desenvolvido para este fim, o Vertex.

4.3.1 TESTES COM A TOPOLOGIA COST-239

Os testes de Remanejamento Beygelzimer et al. foram iniciados com a escolha do nó de maior DC da rede. O próximo passo seria a escolha de um enlace aleatório deste nó, desconectando-o para ligá-lo a um nó aleatório da rede. Para estas escolhas foi utilizado o código Random, desenvolvido para dar suporte a esta estratégia. Não está explícito no trabalho de (BEYGELZIMER, 2005) como esta escolha de enlace foi feita, por isto os enlaces do nó de maior DC foram numerados da esquerda para a direita, no sentido horário. Cinco passos desta estratégia foram executados e seus resultados de FR armazenados.

Uma questão importante levantada durante os testes foi a utilização dos parâmetros da topologia na sequência das alterações. Duas abordagens eram possíveis. Em uma delas, a cada passo do teste seriam levantados novos parâmetros da topologia (tais como nós de maior DC ou CC) para, em seguida, utilizar novamente a estratégia escolhida. Em outra abordagem, os parâmetros utilizados no início dos testes seriam utilizados em toda a sequência de verificações. A abordagem utilizada pelo trabalho de (BEYGELZIMER, 2005) também não foi especificada, desta forma foi arbitrado que a cada passo de alteração de topologia, nova verificação de parâmetros da topologia seria realizada.

Nos testes com o Remanejamento Proposto, inicialmente foram verificados dois nós de maior DC, os nós 9 e 14. Dos adjacentes a estes nós, verificou-se qual dos vizinhos possuía o maior CC. Para o nó 9 foi encon-

trado o enlace conectado ao nó 14 como o adjacente de maior CC. No caso do nó 14, foram encontrados dois adjacentes com maior CC, os nós 9 e 11. Como nó de menor DC da rede foram encontradas 4 possibilidades, os nós 4, 5, 16 e 19. Com estas informações foram geradas 10 matrizes de conectividade com as alterações possíveis e para cada matriz foi calculado o FR. Das 10 matrizes geradas, a que apresentou o melhor fator de resiliência foi a que desconectava do nó 14 o enlace conectado ao nó 9 e em seguida conectava o nó 9 ao nó 16. No segundo passo, foi recalculado o nó de maior DC, o nó adjacente de maior CC e verificamos os nós de menor DC. Três possibilidades foram encontradas, o FR foi calculado para todas elas e foi escolhida a melhor opção. Esta operação foi repetida até o quinto passo (no qual foram testadas 60 possibilidades apenas para este último), verificando sempre o melhor FR.

A próxima estratégia a ser testada foi a Inserção Beygelzimer et al., na qual era inserido um enlace entre os dois nós de menor DC da rede. Não está explícito no trabalho referenciado como eram escolhidos os nós de menor DC caso houvesse mais de dois nós com esta característica. Nos casos em que esta situação ocorreu, foram escolhidos os dois nós de menor identificação numérica. A cada passo os parâmetros eram novamente verificados e novos nós eram escolhidos. Foram executados os cinco passos e os valores de FR calculados para cada um deles.

Nos testes com a Inserção Proposta, no primeiro passo foram encontrados 4 nós com menor DC e um nó de menor CC. Retiradas as repetições de nós, foram feitos 3 testes e escolhida a inserção que obteve o melhor resultado. Este processo foi repetido até a quinta iteração.

A Fig. 4.1 apresenta o gráfico resultante dos testes com as 4 estratégias. Comparando inicialmente as estratégias de inserção de enlaces, a Inserção Proposta obteve melhores resultados em todos os passos. Ao final de cinco iterações, a estratégia proposta aumentou o FR em 23% e foi 8% maior com-

parado com a estratégia do trabalho referenciado. Comparando as estratégias de remanejamento, o Remanejamento Proposto também alcançou os melhores resultados. Ao final de cinco iterações, a estratégia proposta aumentou o FR em 11%, 9% superior a estratégia do trabalho referenciado. Ressalta-se o fato de que em apenas cinco iterações foi possível melhorar a resiliência da rede, mesmo no remanejamento de enlaces.

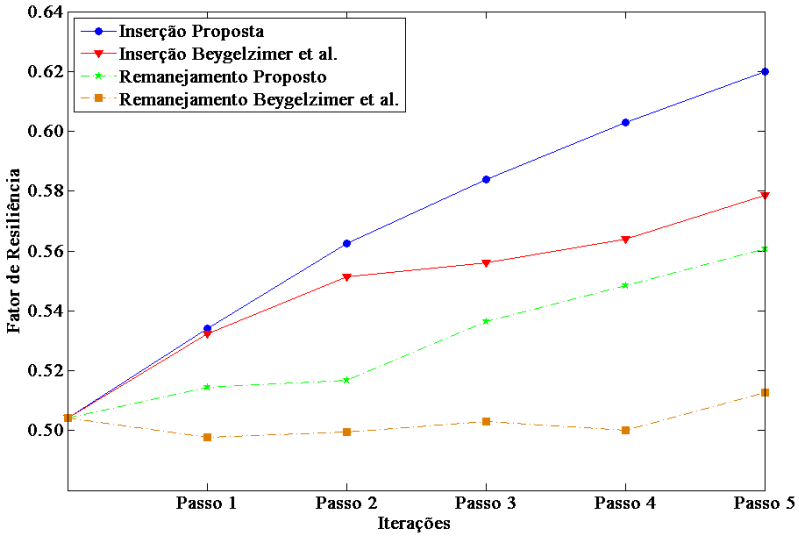


FIG. 4.1: Comparação de estratégias de alteração para a topologia Cost-239

4.3.2 TESTES COM A TOPOLOGIA TELCORDIA

Os testes realizados com as estratégias de Remanejamento e Inserção Beygelzimer et al. seguiram todas as orientações dos autores, como no teste da topologia Cost-239. O único fato que merece comentário aconteceu no primeiro passo do Remanejamento Beygelzimer et al., em que o FR teve um decréscimo, causado provavelmente pela "aleatoriedade" da estatégia. Na adição de enlaces houve melhoria na resiliência em todas as iterações.

Nos testes utilizando a estratégia de Remanejamento Proposto, em todos

os passos foram necessárias várias combinações de testes devido a nós com medidas de centralidade similares. Como realizados no teste anterior, foram utilizados os melhores resultados aferidos.

De acordo com a Fig. 4.2 as estratégias propostas foram superiores às propostas pelo trabalho referenciado. A estratégia de Inserção Proposta permitiu um aumento do FR em 38%, sendo que, comparado com a outra estratégia, foi superior em 5%. Na estratégia de Remanejamento Proposto, houve um aumento do FR em 18%, 9% superior à estratégia do trabalho referenciado.

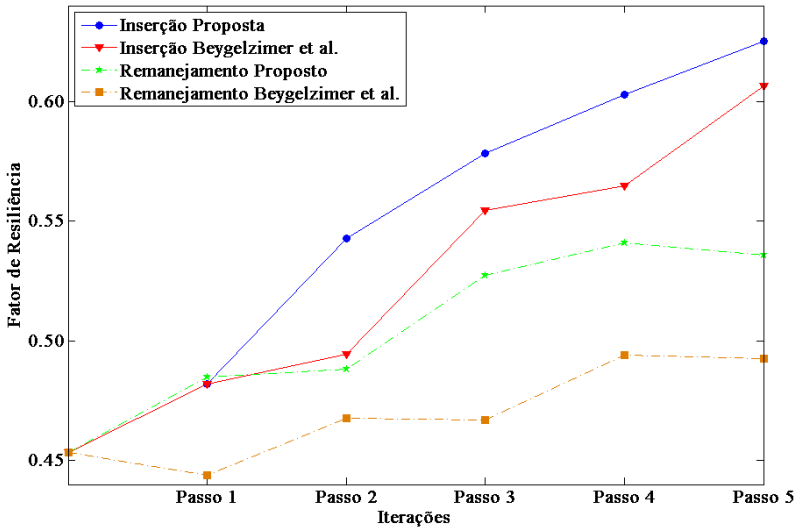


FIG. 4.2: Comparação de estratégias de alteração para a topologia Telcordia

4.3.3 TESTES COM A TOPOLOGIA RNP

Os testes realizados com a topologia RNP apresentaram alguns resultados peculiares, devido ao seu arranjo topológico. A RNP possui uma grande quantidade de subgrafos acíclicos, 17 em um total de 27 nós, e o seu núcleo é

formado por um anel central com os nós Rio de Janeiro, São Paulo, Brasília e Belo Horizonte, e dois anéis adjacentes. Um destes anéis adjacentes é composto pelos nós Salvador, Natal e Fortaleza (ligados ao Rio de Janeiro e Belo Horizonte) e o outro é composto pelos nós Porto Alegre, Florianópolis e Curitiba (ligados a São Paulo e Brasília).

Na estratégia de remanejamento, qualquer alteração nos 3 anéis do núcleo da topologia causou um decréscimo no Fator de Resiliência, tanto para a estratégia do trabalho referenciado como para a estratégia proposta nesta dissertação. Isto se deve provavelmente ao fato mencionado anteriormente, quando foi discutida a alteração de redes com topologia em anel. Uma possível alternativa para estes casos seria a tentativa de todos os remanejamentos possíveis para a topologia em questão, estudo que pode ser objeto de trabalhos futuros.

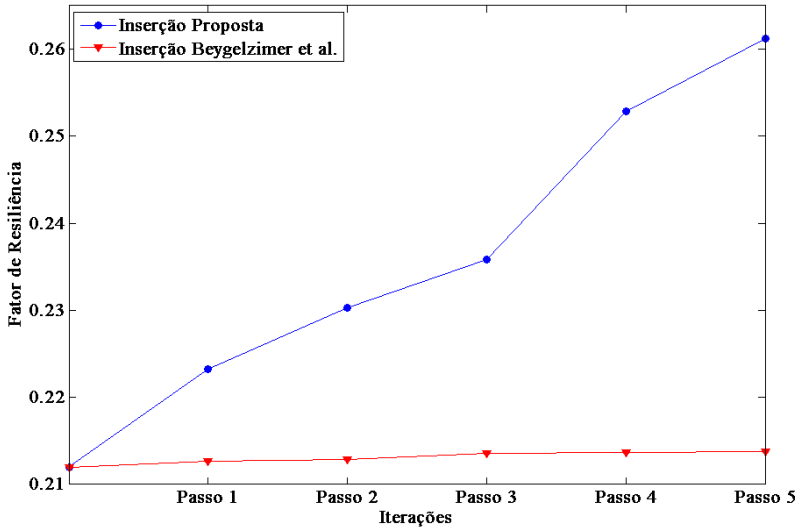


FIG. 4.3: Comparação de estratégias de alteração para a topologia da RNP

Nos testes com as estratégias de inserção de enlaces, a estratégia proposta obteve melhores resultados que a do trabalho referenciado. Nos cinco passos

do teste de inserção de enlaces, a estratégia de Inserção Proposta aumentou o FR em 23% em apenas cinco iterações, superior em 22% ao resultado da estratégia de Inserção Beygelzimer et al. A Fig. 4.3 apresenta gráfico comparativo que contempla os resultados das estratégias de inserção de enlaces. Os resultados dos testes remanejamento foram suprimidos por ser estratégia não indicada para esta topologia.

5 CONSIDERAÇÕES FINAIS

5.1 CONCLUSÕES DO TRABALHO

Este trabalho apresentou o Fator de Resiliência como a medida de robustez de uma rede. Utilizando topologias reais, a resiliência destas topologias foi testada em simulações de ataque aos nós de maior importância da rede, usando como base medidas de centralidade utilizadas em redes sociais. Para validar a métrica proposta, o Fator de Resiliência foi comparado com as três métricas usadas no artigo de (BEYGELZIMER, 2005). Os resultados gerados pelas simulações de ataques, utilizando as métricas AISPL, LCC e diâmetro, foram comparados com os resultados gerados pelo Fator de Resiliência.

Em todas as situações, o Fator de Resiliência seguiu a tendência das métricas do artigo referenciado. Além disto, o Fator de Resiliência se mostrou mais consistente do que as outras métricas, sob os mais variados aspectos. As métricas AISPL e diâmetro não se mostraram consistentes em topologias que se tornaram desconexas após os ataques e o LCC não se mostrou boa escolha para topologias conexas. O Fator de Resiliência foi consistente tanto em testes de redes que se mantiveram conexas como em redes que ficaram desconexas após os ataques ou falhas em nós importantes da rede. Demonstrou uma melhor variação no seu valor, tanto nas simulações de ataques como na comparação direta entre redes no seu estado original.

Os resultados apresentados indicam que o fator proposto pode ser usado para quantificar o grau de tolerância a falhas e ataques de uma rede, permitindo a análise do impacto de alterações na topologia ou auxiliando no

projeto de novas redes.

Como segunda contribuição deste trabalho, duas estratégias de modificação de topologias foram propostas, uma inserindo novos enlaces e outra remanejando enlaces já instalados. Foram realizados testes em topologias reais e os resultados das estratégias propostas comparados com os resultados das estratégias apresentadas por (BEYGELZIMER, 2005). Em todos os testes foi utilizado o Fator de Resiliência proposto neste trabalho como métrica de avaliação da robustez das topologias. As estratégias apresentadas neste trabalho obtiveram os melhores resultados, tanto na inserção como no remanejamento de enlaces.

Durante a pesquisa e escrita desta dissertação foi submetido e aceito trabalho na IADIS International Conference WWW/Internet 2009, a ser realizado na Universidad de Alcalá, Madrid, Espanha, em outubro de 2009. O trabalho "Medindo a Robustez de Uma Rede com o Fator de Resiliência" apresenta o Fator de Resiliência proposto nesta dissertação.

5.2 TRABALHOS FUTUROS

Como trabalhos futuros, a busca de novos algoritmos ou heurísticas para o cálculo da k-conectividade parcial é desejável, devido o alto custo computacional necessário para o cálculo do fator em grandes redes. O número de combinações necessárias para a realização do teste da k-conectividade parcial é exponencial, reforçando a necessidade de uma outra forma de cálculo do fator proposto.

A utilização do custo e do tráfego médio dos enlaces não está no escopo deste trabalho, sendo uma sugestão para a continuidade desta pesquisa. A estratégia de remanejamento de enlaces proposta neste trabalho obteria me-

lhores resultados com a introdução do custo/tráfego dos enlaces na escolha de qual enlace deve ser alterado.

Novas estratégias de alteração de topologias, utilizando outras medidas relacionadas ao estudo das redes sociais, é mais uma sugestão de trabalhos futuros. A identificação de nós com mais de uma característica de centralidade pode nos auxiliar na elaboração de novas estratégias. Métricas como a distância física entre os nós e outras de cunho prático também podem ser avaliadas nos cálculos de alteração de topologia.

Por fim e até aqui, um estudo sobre o projeto de novas redes é mais uma possibilidade de pesquisa futura.

6 REFERÊNCIAS BIBLIOGRÁFICAS

AGGELOU, G. ***Wireless Mesh Networking***. McGraw-Hill Professional, 2008. ISBN 0071482563.

ALVES, R. A. e MURTA, C. D. Topologia dos Sistemas Autônomos : Evolução e Predição. Em *Anais do 26 Simpósio Brasileiro de Redes de Computadores, SBRC2008*, Rio de Janeiro, Brasil, maio 2008.

ALVES JR., N. ***Caracterização de Redes Complexas - Aplicação à Modelagem Relacional entre Sistemas Autônomos da Internet***. Tese de Doutorado, Universidade do Estado do Rio de Janeiro, março 2007.

BARABASI, A.-L., ALBERT, R. e JEONG, H. **Scale-free characteristics of random networks: the topology of the world-wide web**. *Physica A: Statistical Mechanics and its Applications*, 281(1-4):69–77, June 2000.

BERTSEKAS, D. e GALLAGER, R. ***Data networks***. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1987. ISBN 0-13-196825-4.

BEYGELZIMER, A., GRINSTEIN, G., LINSKER, R. e RISH, I. **Improving network robustness by edge modification**. *Physica A: Statistical Mechanics and its Applications*, 357(3-4):593–612, novembro 2005.

BEZERRA, R. L. Análise da conectividade em redes móveis utilizando dados obtidos da mobilidade humana. Dissertação de Mestrado, Universidade Federal do Rio de Janeiro/COPPE, março 2009.

BREDIN, J. L., DEMAINE, E. D., HAJIAGHAYI, M. e RUS, D. Deploying sensor networks with guaranteed capacity and fault tolerance. Em *MobiHoc '05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, págs. 309–319, New York, NY, USA, 2005. ACM. ISBN 1-59593-004-3.

CASTELUCIO, A. O., SALLES, R. M. e ZIVIANI, A. Uma rede sobreposta no nível dos sistemas autônomos para rastreamento de tráfego em redes ip. Dissertação de Mestrado, Instituto Militar de Engenharia, abril 2008.

CRUCITTI, P., LATORA, V., MARCHIORI, M. e RAPISARDA, A. **Error and attack tolerance of complex networks**. *Physica A: Statistical Mechanics and its Applications*, 340(1-3):388–394, setembro 2004.

DEAL, R. ***Cisco Router Firewall Security***. Cisco Press, 2004. ISBN 1587051753.

DEKKER, A. H. e COLBERT, B. Scale-free networks and robustness of critical infrastructure networks. Em *Proceedings of the 7th Asia-Pacific Conference on Complex Systems, Complex 2004*, Cairns, Australia, December 2004a.

DEKKER, A. H. e COLBERT, B. D. Network robustness and graph topology. Em ESTIVILL-CASTRO, V., editor, *ACSC*, volume 26 of *CRPIT*, págs. 359–368. Australian Computer Society, 2004b.

DIESTEL, R. ***Graph Theory***. Springer, 2005. ISBN 3540261826.

FALOUTSOS, M., FALOUTSOS, P. e FALOUTSOS, C. **On power-law relationships of the internet topology**. *SIGCOMM Comput. Commun. Rev.*, 29(4):251–262, October 1999. ISSN 0146-4833.

FORD, L. R. e FULKERSON, D. R. ***Flows in Networks***. Princeton University Press, 1962.

FRANTZ, T. e CARLEY, K. M. Relating network topology to the robustness of centrality measures. Technical Report CMU-ISRI-05-117, School of Computer Science, Carnegie Mellon University, 2005.

FREEMAN, L. C. **Centrality in social networks: Conceptual clarification**. *Social Networks*, 1(3):215–239, 1979.

GIBBONS, A. ***Algorithmic Graph Theory***. Cambridge University Press, Cambridge, New York, 1985.

GROSS, J. e YELLEN, J. ***Handbook of Graph Theory (Discrete Mathematics and Its Applications)***. CRC, 1 edition, December 2003. ISBN 1584880902.

HOLME, P., BEOM, J. K., CHANG, N. Y. e SEUNG, K. H. **Attack vulnerability of complex networks**. *Physical Review E*, 65(056109), 2002.

JIA, X., KIM, D., MAKKI, S., WAN, P. e YI, C. **Power assignment for k-connectivity in wireless ad hoc networks**. *Journal of Combinatorial Optimization*, 9(2):213–222, March 2005. ISSN 1382-6905.

KAMMER, F. e TÄUBIG, H. Graph connectivity. Technical Report TUM-INFO-12-I0422-0, Institut für Informatik, Technischen Universität München, 2004.

KLEITMAN, D. **Methods for investigating connectivity of large graphs**. *IEEE Transactions on Circuit Theory*, CT-16(2):232–233, May 1969.

LEE, H. e KIM, J. Attack resiliency of network topologies. Em *PDCAT*, págs. 638–641, 2004.

LEE, H., KIM, J. e LEE, W. Y. **Resiliency of network topologies under path-based attacks**. *IEICE Transactions*, 89-B(10):2878–2884, 2006.

LIU, G. e JI, C. **Scalability of network-failure resilience: analysis using multi-layer probabilistic graphical models.** *IEEE/ACM Trans. Netw.*, 17(1):319–331, 2009.

LUIS, BARAHONA, G. e ROBLES, G. Applying social network analysis to the information in cvs repositories. Em *Proceedings of the Mining Software Repositories Workshop. 26th International Conference on Software Engineering*, 2004.

MAHADEVAN, P., KRIOUKOV, D. V., FOMENKOV, M., HUFFAKER, B., DIMITROPOULOS, X. A., CLAFFY, K. C. e VAHDAT, A. **The internet as-level topology: Three data sources and one definitive metric**. *CoRR*, abs/cs/0512095, 2005. informal publication.

MENGER, K. **Zur allgemeinen kurventheorie**. *Fundamenta Mathematicae*, 10:96–115, 1927.

MORENO, J. L. **Sociogram and sociomatrix**. *Sociometry*, 9:348–349, 1946.

NAJJAR, W. e GAUDIOT, J.-L. **Network resilience: A measure of network fault tolerance**. *IEEE Transactions on Computers*, 39(2):174–181, 1990.

SAM, S. B., SUJATHA, S., KANNAN, A. e VIVEKANANDAN, P. **Network topology against distributed denial of service attacks**. *Information Technology Journal*, 2006.

SKIENA, S. S. ***The Algorithm Design Manual***. Springer, 2nd edition, August 2008.

TANGMUNARUNKIT, H., GOVINDAN, R., JAMIN, S., SHENKER, S. e WILLINGER, W. **Network topology generators: degree-based vs. structural**. *SIGCOMM Comput. Commun. Rev.*, 32(4):147–159, 2002. ISSN 0146-4833.

WASSERMAN, S., FAUST, K. e IACOBUCCI, D. ***Social Network Analysis : Methods and Applications (Structural Analysis in the Social Sciences)***. Cambridge University Press, November 1994. ISBN 0521387078.

YANG, L. **Building k-connected neighborhood graphs for isometric data embedding**. *IEEE Trans. Pattern Anal. Mach. Intell.*, 28(5):827–831, 2006. ISSN 0162-8828.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo