# Fator de Resiliência para Aprimoramento Topológico em Redes Definidas por Software

**Pedro Montibeler[1], Fernando Farias[1], Antônio Abelém[1]**

[1]Grupo de Estudos em Redes de Computadores e Comunicação Multimídia
Instituto de Informática – Universidade Federal do Pará (UFPA)
pedro.salvador@itec.ufpa.br, {fernnf, abelem}@ufpa.br

***Abstract.*** *Software Defined Networks is a paradigm that flexibilizes the management of networking, which separates the control and forwarding planes. This separation introduces new concerns towards the resilience of the network, which now presents different vulnerabilities related to the interaction between these planes. A resilience factor for Software Defined Networks is proposed, using multiple metrics to analyze intrinsic features of its architecture, serving as an indication for its resilience. Beyond that, topological augmentation algorithms are employed to increase the resilience of test topologies, as indicated by the proposed factor. Tests results demonstrate an improvement of the topologies' resilience characteristics.*

***Resumo.*** *Redes Definidas por Software é um paradigma que flexibiliza a gerência de redes de computadores ao separar os planos de controle e de dados. Essa separação introduz novas preocupações quanto a resiliência da rede, que passa a apresentar diferentes vulnerabilidades relacionadas a interação entre os planos. É proposto um fator de resiliência para Redes Definidas por Software, utilizando múltiplas métricas para analisar características intrínsecas da arquitetura, servindo como indicativo de resiliência da rede. Além disso, algoritmos de aprimoramento topológico são empregados para aperfeiçoar a resiliência das topologias utilizadas. Os resultados demonstram melhoria nas características de resiliência.*

## 1. Introdução

Redes Definidas por *Software* (SDN) é um modelo de redes de computadores onde o plano de controle, tradicionalmente embutido nos comutadores, é separado do plano de encaminhamento, que agora abstrai suas funções de forma que possam ser programadas por *software* a partir do plano de controle [ONF 2012]. A programabilidade da rede a partir da visão centralizada do plano de controle flexibiliza e simplifica a gerência dos dispositivos de rede por parte dos administradores e desenvolvedores, facilitando a pesquisa e desenvolvimento de tecnologias na área [Farias et al. 2011].

A dependência do plano de controle centralizado, no entanto, traz novas

preocupações quanto à resiliência da rede. Falhas de dispositivos, que os tornem inoperantes ou incomunicáveis, estão sujeitas a acontecer não apenas no plano de encaminhamento, como também no plano de controle, sendo a conectividade entre esses planos outra vulnerabilidade. Falhas no plano de encaminhamento, tais como quedas de enlaces, devem ser detectadas e recuperadas pelo plano de controle, pois caso a falha prejudique a interação entre os controladores e os comutadores, os efeitos negativos na operação da rede podem ser agravados.

Por isso, uma rede que segue o modelo SDN deve ser capaz de tolerar falhas em entidades de seus diferentes planos [Ros e Ruiz 2014]. Logo, há a necessidade de se avaliar aspectos de resiliência durante o planejamento de uma SDN, considerando as características intrínsecas de sua arquitetura, buscando preservar o funcionamento de seus planos e sua correta interação.

Nesse contexto, trabalhos recentes tem estudado a otimização do posicionamento dos controladores para melhorar diferentes características da rede, como a resiliência. Comumente é utilizado apenas uma métrica para caracterizar a resiliência da rede [Ros e Ruiz 2014] [Müller et al. 2014], e mesmo quando são utilizadas múltiplas métricas, a otimização se limita ao plano de controle, embora o plano de dados influencie diretamente nas características da rede [Heller, Sherwood e McKeown 2012] [Hock et al. 2013].

O objetivo deste trabalho é contribuir com um fator de resiliência para o auxílio da tomada de decisões no planejamento de SDNs, onde são selecionadas e correlacionadas múltiplas métricas pertinentes às propriedades de uma SDN. Outra contribuição é a aplicação de algoritmos de aprimoramento topológico em SDNs buscando melhorar suas características de resiliência, em específico, algoritmos de Redistribuição de Arestas (*Edge Rewiring*). Na análise de resultados, observa-se que os algoritmos implementados melhoraram as características de resiliência das topologias testadas.

Além desta seção introdutória, este artigo está dividido da seguinte forma. Na Seção 2 são discutidos os trabalhos relacionados ao tema. A Seção 3 detalha o fator de resiliência proposto. A Seção 4 demonstra sua aplicação como um parâmetro de algoritmos de aprimoramento topológico. Por fim, a Seção 5 apresenta as conclusões gerais e trabalhos futuros.

## 2. Trabalhos Relacionados

Na análise de SDNs, trabalhos recentes têm estudado o Problema do Posicionamento do Controlador (*Controller Placement Problem*) [Heller, Sherwood e McKeown 2012], onde é evidenciado que o posicionamento dos controladores na rede afetam características de conectividade entre os planos e latência de comunicação. Nesse contexto, os trabalhos seguintes consideram características de resiliência em suas

análises.

Na proposta de Ros e Ruiz [2014] é investigado, especificamente, o impacto do posicionamento dos controladores na capacidade de sobrevivência da SDN. Em seu trabalho, buscam determinar a posição e quantidade de controladores em uma topologia de forma a garantir um valor mínimo na métrica de confiabilidade k-terminal (*k-terminal reliability*). No trabalho de Müller [2014] é proposto uma estratégia de posicionamento que esquematize o balanceamento de carga dos controladores, e otimize a resiliência da rede analisando os caminhos disjuntos entre os nós. Esses trabalhos caracterizam a resiliência somente com uma métrica relacionada a capacidade de sobrevivência da rede, que apesar de relevante, é insuficiente em SDN.

Nas propostas de Hock [2013] e Lange [2015], o problema do posicionamento do controlador é trabalhado utilizando diversas métricas, como latência entre dispositivos, balanceamento de carga entre os controladores, e a conectividade entre os planos. São consideradas múltiplas características pertinentes a resiliência em SDN, como a capacidade de sobrevivência e a latência de comunicação entre os dispositivos dos diferentes planos. No entanto, propõem otimizar unicamente o plano de controle, embora a estrutura topológica do plano de dados influencie diretamente na solução [Heller, Sherwood e McKeown 2012] [Hock et al. 2013] [Ros e Ruiz 2014].

Como exemplificado, os trabalhos em SDN comumente utilizam apenas uma métrica para caracterizar a rede quanto à sua resiliência, e mesmo quando investigam múltiplas métricas, as otimizações realizadas buscam somente alterar a posição e quantidade dos controladores na rede, sem interferir na estrutura topológica do plano de dados, o que influencia significativamente na solução, como observado pelos próprios autores.

Neste trabalho, múltiplas métricas pertinentes a resiliência de uma SDN são verificadas e consideradas simultaneamente, resultando em um fator para aferir a resiliência de uma topologia. O resultado pode ser utilizado para comparação objetiva entre topologias, ou aplicado como função objetivo em um algoritmo de posicionamento de controladores, ou ainda, como investigado neste trabalho, usado como parâmetro para algoritmos de aprimoramento topológico. Em nossa proposta utiliza-se algoritmos de redistribuição de arestas, investigados em trabalhos como de Beygelzimer [2005] e Bai Liang [2015], para realizar alterações topológicas em ambos os planos de uma SDN, buscando melhorar suas características de resiliência.

## 3. Proposta

Um fator de resiliência pode ser usado como uma ferramenta auxiliar durante a fase de planejamento de uma SDN, possibilitando a comparação objetiva de diferentes topologias, ou como função objetivo em um algoritmo de aprimoramento. Quanto mais características desejáveis forem consideradas na análise de um fator de resiliência, mais

informativos serão seus resultados. Portanto, o fator de resiliência para SDNs proposto deve retornar um valor que seja indicativo das propriedades da rede, correlacionando múltiplas métricas que analisem as características mais pertinentes da estrutura topológica da rede no que se refere a resiliência.

Para isso é verificado a seguir quais as características desejadas para uma SDN resiliente considerando as peculiaridades de sua arquitetura. Em seguida são escolhidas as métricas a serem empregadas como indicativos para essas características, por fim correlacionando-as em um fator de resiliência.

Definido um fator de resiliência, é possível empregá-lo como métrica em um algoritmo visando aprimorar as características de uma SDN. Com esse fim, são selecionados algoritmos de aprimoramento topológico que aplicarão transformações em ambos os planos da topologia SDN, buscando aumentar a resiliência da mesma.

### 3.1. Características de resiliência em SDN

Métricas de redes complexas e conceitos da teoria de grafos são, atualmente, uns dos principais elementos aplicados na análise de resiliência em redes de comunicação legadas. Comumente, são verificadas a conectividade da estrutura topológica da rede e a existência de caminhos alternativos entre os dispositivos, como indicativos para a capacidade de sobrevivência da rede [Habibi e Phung 2012]. Nas redes legadas, os planos de controle e encaminhamento estão juntos, distribuídos entre os comutadores. Nesse contexto, a análise é realizada trivialmente ao representar a topologia de rede como um grafo, onde os comutadores são os vértices e os enlaces as arestas, sem que haja a necessidade de discriminar os dispositivos, por estes exercerem papéis equivalentes na rede. Por outro lado, em SDN, os dispositivos de controle e encaminhamento não são necessariamente os mesmos. Logo, a análise deve ser diferenciada.

Assim como nas redes de comunicações legadas, é desejável que SDNs possuam uma estrutura topológica tolerantes a falhas, que permita a ocorrência de falhas de nós ou enlaces de forma que a rede não se torne desconexa. Isso se aplica intuitivamente em redes de computadores tradicionais, pois o seu propósito é a transmissão de dados e a comunicação entre todos os dispositivos da rede deve ser preservada para que essa transmissão possa acontecer.

Em uma SDN, mesmo com a separação de planos e a presença de controladores na rede, essa característica continua a ter a mesma importância. Sendo os controladores responsáveis pela lógica de encaminhamento da rede, o correto funcionamento do plano de encaminhamento depende das instruções transmitidas pelos controladores aos comutadores através do plano de controle. Não apenas a conectividade entre os comutadores deve ser tolerante a falhas, para que não se interrompa a transmissão de dados, como a conectividade entre os planos também deve ser tolerante a falhas, para que essa interação entre os planos não seja interrompida. Por último, é importante

lembrar que o plano de controle é logicamente centralizado, portanto mesmo quando múltiplos controladores são empregados, estes devem ser capazes de se comunicar para cooperar nas tomadas de decisão, e sua conectividade também deve ser tolerante a falhas. Conclui-se que, tal como em redes tradicionais, é interessante que a comunicação entre todos os dispositivos de uma SDN seja tolerante a falhas, independente de seu papel na arquitetura.

Relacionada a tolerância a falhas, há também a questão de redundância: apenas uma instância de controlador na rede pode ser suficiente para sua operação, mas a falha desse dispositivo deixará a rede sem plano de controle. Portanto, para aumentar a tolerância a falhas no plano de controle, é interessante que uma SDN possua múltiplos controladores em operação na rede.

Sendo o plano de controle responsável pela lógica de encaminhamento, a detecção de uma falha no plano de encaminhamento e a consequente atualização das regras é responsabilidade dos controladores. Com isso, a latência de comunicação entre os controladores e os comutadores, mais do que uma questão de desempenho, é uma questão de recuperação de falhas. A eficiência da comunicação entre os planos é determinante no tempo de recuperação de falhas da rede, afetando o tempo de resposta do plano de controles a cenários de falha. O plano de controle é logicamente centralizado e, portanto, a comunicação entre múltiplos controladores também deve ser eficiente para agilizar a sincronia entre suas diferentes instâncias. Conclui-se que é interessante para uma SDN que a eficiência de comunicação entre os múltiplos controladores e entre os controladores e os comutadores seja a maior possível.

### 3.2. Fator de Resiliência de Média de Múltiplas Métricas (FRM3)

A teoria das redes complexas é um tema interdisciplinar que abrange diversas áreas do conhecimento, como computação, matemática, sociologia, física e biologia. Uma rede é representada por um grafo, um conjunto de vértices conectados por arestas, modelando sistemas do mundo real, como a infraestrutura física de uma rede de computadores, para a resolução de problemas específicos [Metz et al. 2007]. Com o estudo de redes complexas, pode-se verificar propriedades de sistemas baseando-se nas relações entre seus componentes, aplicando conceitos e algoritmos da teoria matemática dos grafos. Em redes de computadores, utilizam-se métricas de grafos no planejamento de redes tradicionais, como na verificação de aspectos de resiliência em topologias de rede [Habibi e Phung 2012], controle de congestionamento, entre outros. Para a análise em SDN, as métricas selecionadas são métricas de grafos.

Na tolerância a falhas, uma métrica comumente utilizada é a k-conectividade [Habibi e Phung 2012]. A análise de k-conectividade retorna um valor inteiro que corresponde a quantidade mínima de vértices que precisam ser removidos do grafo para que o grafo induzido constituído dos vértices restantes seja desconexo. Com essa métrica se obtém um indicativo da capacidade de sobrevivência da rede a cenários de

falhas arbitrárias de dispositivos.

Quanto a eficiência de comunicação, a métrica de eficiência é um indicativo da eficiência da estrutura topológica da rede [Latora e Marchiori 2001]. Ela retorna um valor entre zero e um que é inversamente proporcional a média dos comprimentos dos menores caminhos entre os vértices do grafo. Essa métrica é um indicativo da proximidade geral dos dispositivos na topologia de rede.

Combinando as características de tolerância a falhas e eficiência, a métrica de vulnerabilidade indica o decaimento da eficiência com a remoção de um vértice arbitrário [Latora e Marchiori 2001]. O valor retornado é a maior alteração relativa do valor da métrica de eficiência com a remoção de um vértice do grafo. A métrica de vulnerabilidade indica o quanto a eficiência da comunicação entre os vértices de um grafo pode ser afetado pela remoção de um de seus nós.

Considerando as características de resiliência desejáveis especificamente para uma SDN e utilizando das métricas indicativas dessas características, é proposto um Fator de Resiliência de Média de Múltiplas Métricas (FRMMM ou FRM3). O fator proposto é constituído por cinco componentes, ou fatores, que analisam diferentes características da topologia. Cada fator retorna um valor entre zero e um, possibilitando que uma média possa facilmente ser calculada sem que um fator influencie o resultado mais do que os outros. Para as equações a seguir, define-se que um grafo simples $G=(V,E)$ é constituído de um conjunto $V$ de vértices, que representam os dispositivos da rede, e um conjunto $E$ de arestas que conectam dois vértices do grafo, representando os enlaces da rede. O primeiro fator é o Fator de Redundância, que considera o número de dispositivos controladores na rede $Nc$ :

$$FRed=1-\frac{1}{Nc},\ Nc \geqslant 1 \tag{1}$$

O Fator de Redundância retorna um valor proporcional ao número de controladores na rede, onde quanto maior a redundância, maior o valor. O número de controladores deve ser no mínimo um para que a rede possa ser considerada uma SDN. Esse fator avalia de forma simples a redundância no plano de controle, onde mais controladores significa melhor redundância.

O segundo é o Fator de Conectividade, que considera a k-conectividade da topologia. Sendo $Csdn$ um valor indicativo da capacidade de sobrevivência da topologia, onde $Kglobal$ é o valor de k-conectividade do grafo da topologia, no qual ambos os planos são considerados, e $Kpd$ o valor de k-conectividade somente do plano de dados, ou seja, do grafo induzido da topologia que contém apenas os comutadores:

$$Csdn=\frac{Kglobal+Kpd}{2} \tag{2}$$

O valor de $Csdn$ é a média simples de dois valores de k-conectividade da rede.

Dois valores são utilizados pois o número de falhas que deixem o plano de controle desconexo do plano de dados não é necessariamente o mesmo número de falhas que deixem o plano de dados desconexo. Portanto são analisados a k-conectividade do grafo, que testa a capacidade de sobrevivência entre todos os dispositivos, e do grafo induzido do plano de dados, constituído somente pelos dispositivos encaminhadores, tal como em uma rede tradicional. Com esse valor, se obtém o Fator de Conectividade:

$$FC = 1 - \frac{1}{Csdn} \tag{3}$$

O terceiro é o Fator de Eficiência de Rede, que considera o valor da métrica de eficiência. No entanto, como a eficiência de comunicação que se deseja investigar é a do plano de controle e entre os planos, são considerados apenas os caminhos que conectem um controlador ou a outro controlador ou a um comutador. Sendo $Vc$ o conjunto dos vértices que correspondem a controladores, $Nmc(Vc, V)$ o número de menores caminhos que conectem todo vértice controlador a todo outro vértice e $d(i, j)$ o comprimento do menor caminho entre quaisquer vértices $i$ e $j$ :

$$E(Vc) = \frac{1}{Nmc(Vc, V)} \sum_{i \neq j} \frac{1}{d(i, j)}, \ i \in Vc, \ j \in V \tag{4}$$

Essa fórmula restringe o cálculo de eficiência aos caminhos que conectem os controladores aos outros dispositivos da rede, sejam outros controladores ou comutadores. Dessa forma o valor retornado é um indicativo da eficiência de comunicação do plano de controle na rede, que é a característica desejável a se analisar. Com a Equação 4, o Fator de Eficiência de Rede é obtido simplesmente com:

$$FE = E(Vc) \tag{5}$$

O quarto é o Fator de Vulnerabilidade, que considera o valor da métrica de vulnerabilidade, com o diferencial de essa ser obtida usando a eficiência obtida na Equação 4. Dessa forma, o impacto analisado é na eficiência do plano de controle. A métrica de vulnerabilidade, ao contrário da eficiência, pode assumir valores positivos ou negativos, num cenário onde a remoção de um nó aumenta o valor da eficiência da rede, e pode assumir um valor absoluto maior do que um, num cenário onde o impacto foi maior de cem por cento. Considerando isso, para valores entre um positivo e um negativo, o valor é transformado para um valor proporcional entre zero e um. Para um valor absoluto maior do que um, o valor é limitado ao valor mínimo de zero e máximo de um. Dessa forma, valores de impacto de até cem por cento positivo ou negativo são considerados e transformados para obedecerem os limites estabelecidos, sem perda de informação. Sendo $V(Vc)$ o valor de vulnerabilidade do plano de controle, a vulnerabilidade transformada é obtida conforme a seguinte fórmula:

$$Vt = \begin{cases} \frac{V(Vc)+1}{2}, & |V(Vc)| \leqslant 1, \\ 1, & V(Vc) > 1, \\ 0, & V(Vc) < -1. \end{cases} \quad (6)$$

Com esse valor, o Fator de Vulnerabilidade é obtido por:

$$FV = 1 - Vt \quad (7)$$

Com essa fórmula, quanto maior o valor de vulnerabilidade, pior é o impacto de uma falha na eficiência do plano de controle, e menor o valor retornado pelo fator.

O quinto é o Fator de Eficiência de Domínio, que considera a eficiência de cada controlador aos comutadores sob seu controle direto. Em implementações do paradigma SDN, como na arquitetura *OpenFlow* [McKeown et al. 2008], cada dispositivo encaminhador é alocado a um controlador, que será responsável por trocar as mensagens de controle com esse dispositivo. É possível configurar múltiplos controladores em cada dispositivo, como sobressalentes para o controlador principal, com quem o dispositivo deve se comunicar (ONF, 2015). Nesse cenário, é interessante verificar a eficiência de comunicação de cada controlador com seus dispositivos alocados, que será referenciado a partir de agora como o domínio do controlador. Sendo $c$ um vértice correspondente a um controlador que tenha dispositivos em seu domínio, $Vd(c)$ o conjunto de vértices correspondentes a esses dispositivos e $Nmc(c, Vd(c))$ o número de menores caminhos que conectem o vértice controlador a todos os dispositivos de seu domínio, a eficiência desse domínio é obtido por:

$$E(c) = \frac{1}{Nmc(c, Vd(c))} \sum \frac{1}{d(c,i)}, \quad c \in Vc, \quad i \in Vd(c) \quad (8)$$

Calculando a eficiência de cada controlador com seu domínio, o Fator de Eficiência de Domínio é obtido como o mínimo dessas eficiências:

$$FEd = min(E(c)), \quad c \in Vc \quad (9)$$

O Fator de Eficiência de Rede e o Fator de Eficiência de Domínio fornecem indicativos de características diferentes da rede. Um valor alto no Fator de Eficiência de Domínio indica que os controladores estão distribuídos na topologia, cada um tendendo ao centro de seus respectivos domínios, o que é desejável, pois a proximidade de cada controlador aos seus dispositivos alocados tende a uma maior eficiência em sua comunicação. Um valor alto no Fator de Eficiência de Rede também é desejável, pois se todos os controladores estiverem numa posição central na topologia, na ocorrência de falha de um controlador, outro controlador sobressalente poderá absorver os dispositivos afetados em seu domínio com pouco impacto na eficiência de comunicação entre os planos. Um equilíbrio entre estes fatores é o cenário ideal: cada controlador tende ao

centro de seu domínio, assim como tende ao centro da rede.

Combinando esses cinco fatores, obtém-se o Fator de Resiliência de Média de Múltiplas Métricas:

$$FRM3 = \frac{PRed \times FRed + PC \times FC + PE \times FE + PV \times FV + PEd \times FEd}{PRed + PC + PE + PV + PEd} \quad (10)$$

Cada fator é multiplicado por um peso que pode ser definido arbitrariamente conforme as características mais prioritárias para uma determinada análise. A análise realizada na seção seguinte é realizada sem a atribuição de prioridades, sendo todos os pesos definidos com valor um, tornando a equação uma média simples entre os fatores.

### 3.3. Algoritmos de aprimoramento topológico

Um algoritmo de aprimoramento topológico por redistribuição de arestas se propõe a transformar uma topologia, usando de alguma estratégia para remanejar as arestas existentes [Beygelzimer et al. 2005]. No contexto de SDN, é possível utilizar estes algoritmos para alterar conjuntamente as conexões dos controladores e dos comutadores da rede, aprimorando toda a estrutura topológica em uma determinada função objetivo. Neste trabalho foram implementados três algoritmos:

- Redistribuição de Aresta Randômica: Uma aresta aleatória é removida, e uma aresta aleatória é adicionada, desde que não seja a mesma aresta [Beygelzimer et al. 2005].
- Redistribuição de Aresta Randômica Preferencial: Uma aresta aleatória é removida, e o vértice de menor grau conectado por esta aresta é conectado a outro vértice aleatório com uma nova aresta [Beygelzimer et al. 2005].
- *Smart Rewire*: Duas arestas aleatórias são removidas, e entre os vértices afetados, duas novas arestas são adicionadas, uma entre os dois vértices de maior grau, e outra entre os vértices de menor grau [Bai Liang et al. 2015].

O algoritmo de Redistribuição Randômica realiza uma redistribuição completamente randômica e é utilizado como base para comparação. O algoritmo de Redistribuição Preferencial busca preservar o grau dos vértices menos conectados durante a distribuição e apresentou melhores resultados no trabalho de referência. O algoritmo *Smart Rewire* emprega similarmente uma estratégia que busca preservar o grau dos vértices mais e menos conectados.

Esses algoritmos foram selecionados pela simplicidade e versatilidade, que permitem que o FRM3 fosse utilizado como função objetivo para um algoritmo de "subida de encosta" (*hill-climbing*). Os algoritmos realizam alterações na topologia até que ultrapassem um determinado número de tentativas sem que haja nenhum sucesso em aumentar o valor de FRM3. No experimento realizado, o valor escolhido é de dez tentativas, sendo que valores maiores não demonstraram ganhos significativos nos experimentos realizados. Transformações que desconectem o grafo não são permitidas, e

transformações que gerem efeitos negativos ao valor de FRM3 são revertidas.

## 4. Resultados

Para explorar a aplicação do fator de resiliência proposto, este foi empregado como métrica da função objetivo de algoritmos de aprimoramento topológico, para analisar e aprimorar as características de resiliência das topologias de teste. Para esse fim, foram utilizadas topologias disponibilizadas publicamente na *Internet Topology Zoo*[1], sob os quais experimentos foram conduzidos e resultados obtidos conforme descrito na subseção a seguir. Os valores retornados pelo FRM3 são então analisados, verificando como cada característica topológica influenciou nos resultados. Posteriormente são descritos como os algoritmos de aprimoramento topológico que foram aplicados nas topologias afetaram os valores retornados pelo FRM3.

### 4.1. Metodologia

Para os testes realizados foram utilizadas as topologias disponibilizadas na *Internet Topology Zoo* para o plano de dados. Como tais topologias são de redes tradicionais, fica faltando definir adequadamente o plano de controle. Neste contexto, para cada topologia foram adicionados vértices controladores posicionados aleatoriamente, ou seja, foram selecionados vértices aleatoriamente e conectados um vértice controlador a cada um. A quantidade de controladores a serem adicionados em uma topologia foi definido como uma porcentagem do número de nós da rede, especificamente 25%, 50% e 75%. Para definir os dispositivos alocados para cada controlador, ou seja, o domínio de cada controlador, cada dispositivo foi simplesmente alocado ao controlador mais próximo conforme o comprimento do menor caminho. Caso um dispositivo esteja a mesma distância de múltiplos controladores, este é alocado aleatoriamente a um desses controladores.

Como o posicionamento dos controladores na rede é feito aleatoriamente, e como é discutido neste trabalho e observado nos trabalhos relacionados que o posicionamento dos controladores na rede afetam os valores das métricas de resiliência, cada topologia possui o posicionamento dos controladores repetidos trinta vezes para se obter o caso médio da avaliação do FRM3, diminuindo a influência de melhores e piores casos nos valores observados. Foram utilizadas 39 topologias do *Internet Topology Zoo*, contendo desde 5 até 16 comutadores, os quais após a inserção dos controladores em diferentes proporções e em diferentes posições, resultaram em mais de 3500 diferentes topologias SDN.

Foi desenvolvido um programa em Java que gerou as topologias SDN a partir das topologias da *Internet Topology Zoo* como descrito anteriormente, obteve as métricas e calculou o FRM3 conforme detalhado na seção anterior, aplicando os algoritmos implementados de aprimoramento topológico nas topologias geradas,

1 Disponível em: http://www.topology-zoo.org/

retornando o novo FRM3 após o aprimoramento. Os gráficos gerados a seguir foram obtidos a partir desses testes, realizados em um servidor com as seguintes especificações: Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz, com 65 GB RAM, e sistema 64-bit. Sistema Operacional GNU/Linux Ubuntu, Kernel 3.13.0-48-generic.

### 4.2. Análise de resultados

Os valores dos fatores e do FRM3 antes e depois da aplicação dos algoritmos descritos na subseção 3.3 são ilustrados na Figura 1.

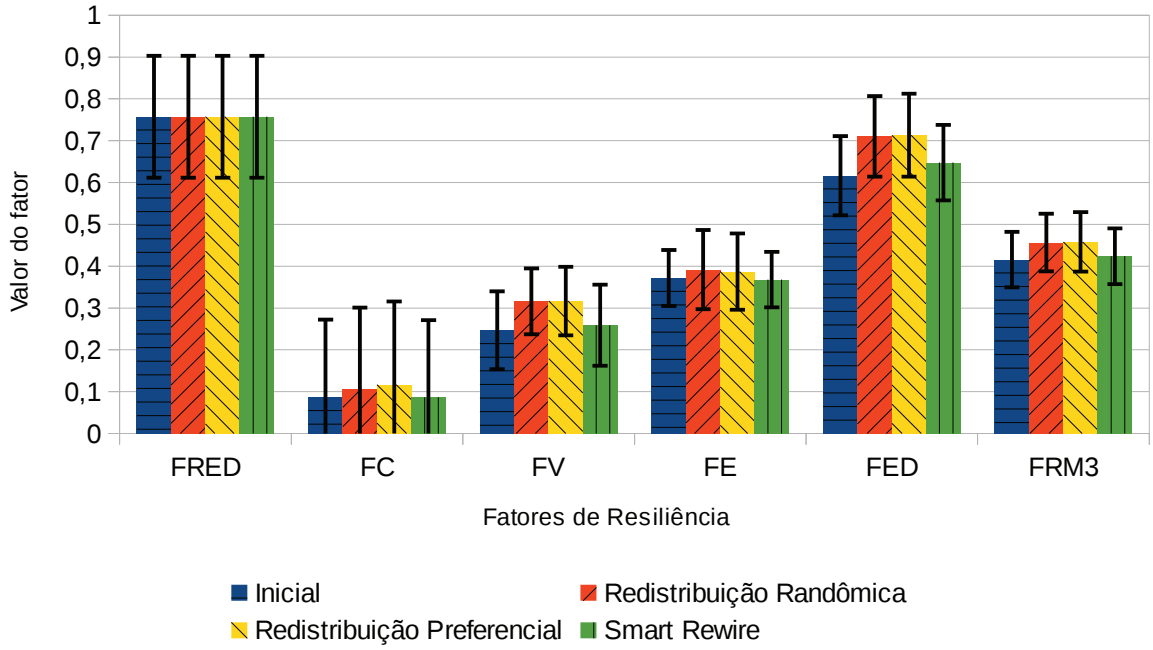


**Figura 1. Média e desvio padrão dos valores dos fatores de resiliência nas topologias de experimentação antes e após a aplicação dos algoritmos de aprimoramento.**

A maioria das topologias de teste possui múltiplos controladores, elevando o valor do Fator de Redundância, e essa redundância de controladores na rede naturalmente faz com que os comutadores tenham mais opções de alocação para um controlador, aumentando as chances de que tenha um controlador mais próximo, fazendo com que o Fator de Eficiência de Domínio também seja alto. No entanto, o posicionamento impensado dos controladores e a própria estrutura topológica do plano de dados resulta em Fatores de Conectividade, Eficiência de Rede e Vulnerabilidade mais baixos. Não há a preocupação em aproximar os controladores do centro da rede, e a fraca conectividade do plano de controle e de dados faz com que o valor final de FRM3 seja apenas mediano.

Com a aplicação dos algoritmos há um ganho em todos os fatores, com a exceção do Fator de Redundância, pois os algoritmos não alteram o número de controladores na rede. Os algoritmos de Redistribuição Randômica e Preferencial aumentaram a média do FRM3 em 9,7% e 10% respectivamente, apresentando ganhos em múltiplos fatores. O algoritmo de Redistribuição Randômica obteve melhorias em 89,6% das topologias, e o algoritmo de Redistribuição Preferencial aprimorou 91,8% das topologias. O algoritmo de *Smart Rewire* aumentou a média de FRM3 em 1,8%, obtendo resultados em 60,8% das topologias. A estratégia de redistribuição mais restritiva do *Smart Rewire* limitou a exploração por uma solução nas topologias testadas.

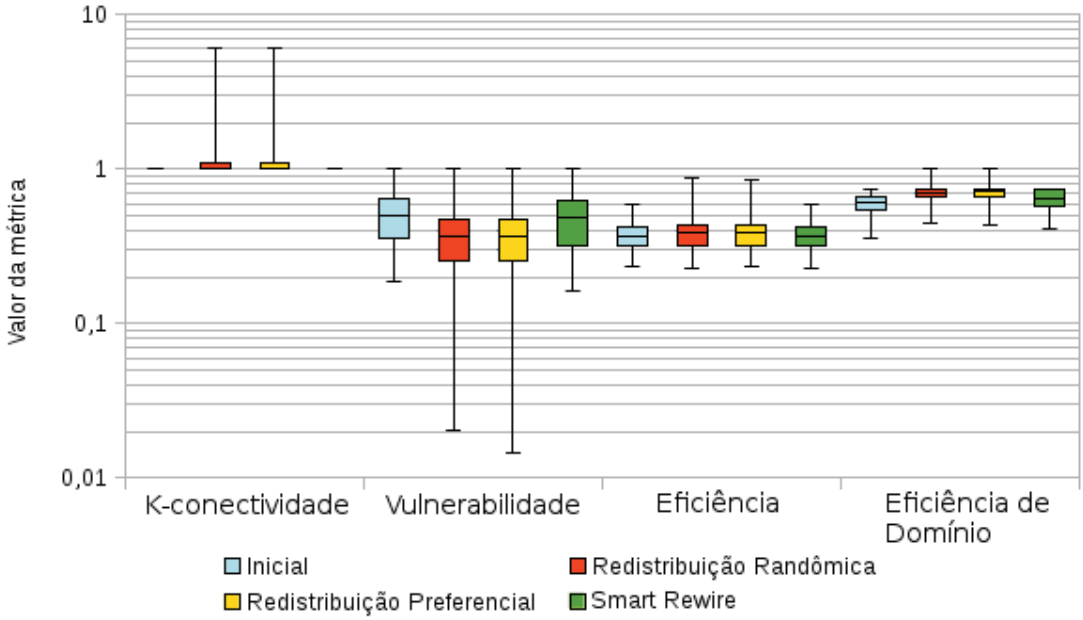


**Figura 2. Distribuição em *boxplot* dos valores das métricas de análise antes e após a aplicação dos algoritmos de aprimoramento.**

As formas que o ganho obtido no FRM3 reflete nas topologias pode ser visualizado na Figura 2. O impacto dos algoritmos de aprimoramento nas diferentes métricas reafirma os baixos ganhos do algoritmo de *Smart Rewire*, que não aprimorou a capacidade de sobrevivência das topologias, aumentou a média de eficiência da comunicação dos controladores para seus comutadores alocados em apenas 5% e diminuiu em apenas 4,7% em média a vulnerabilidade dessa comunicação. Os algoritmos de Redistribuição Randômica e Preferencial no entanto, aumentaram a k-conectividade da rede respectivamente em 6,4% e 6,9% das topologias, efetivamente aprimorando a capacidade de sobrevivência da rede à cenários de falha de dispositivo arbitrário. Também obtiveram aumento de 5,3% e 4% da média de eficiência de comunicação da rede, e aumento de 15,2% e 15,6% da média de eficiência de comunicação dos controladores para seus respectivos comutadores alocados, efetivamente diminuindo as distâncias dos menores caminhos da rede; adicionalmente

diminuindo em média 27,2% e 27,5% a vulnerabilidade dessa comunicação a falhas arbitrárias, através de caminhos disjuntos mais eficientes entre os dispositivos. O comportamento desses indicativos demonstra a eficácia do fator proposto como um indicativo informativo para a análise da rede, e para a aplicação como função objetivo.

Os algoritmos de Redistribuição Randômica e Preferencial apresentaram desempenho equivalente no aprimoramento das topologias testadas. O algoritmo *Smart Rewire* apresentou os menores ganhos devido a criteriosa estratégia de remanejamento de arestas aplicada, que limitou as transformações realizadas.

## 5. Conclusões e Trabalhos Futuros

É proposto um Fator de Resiliência de Múltiplas Métricas para Redes Definidas por *Software* que correlaciona múltiplas métricas de redes complexas, analisando diversas características de resiliência de uma topologia do paradigma SDN, levando em consideração os aspectos específicos a sua arquitetura. O fator proposto pode ser uma útil ferramenta na fase de planejamento de rede, permitindo uma análise objetiva e comparativa entre propostas de topologias e na aplicação computacional de algoritmos de aprimoramento topológico. Trabalhos relacionados demonstram pouca preocupação em correlacionar múltiplas métricas simultaneamente, e propõe soluções que otimizam apenas o posicionamento dos dispositivos no plano de controle, apesar de observarem que essa otimização é diretamente dependente da topologia formada por ambos os planos.

Topologias obtidas a partir de topologias disponibilizadas na *Internet Topology Zoo* foram analisadas e usadas como base para algoritmos de aprimoramento topológico de Redistribuição de Arestas, que obtiveram ganhos no fator proposto ao realizarem otimizações em características de resiliência de ambos os planos das topologias.

Como trabalhos futuros, pretende-se investigar de que forma o ajuste nos pesos dos componentes do fator proposto pode contribuir na aplicação dos algoritmos de aprimoramento topológico, além de comparar o desempenho de mais algoritmos, em mais topologias, para o aprimoramento topológico de Redes Definidas por *Software*.

## Referências

Bai Liang, Xiao Yan-Dong, Hou Lv-Lin et al. (2015) “Smart Rewiring: Improving Network Robustness Faster”, Chin. Phys. Lett., 32(07):078901.

Beygelzimer A., Grinstein G., Linsker R. e Rish I. (2005) “Improving network robustness by edge modification”, Physica A: Statistical Mechanics and its Applications, 357(3-4):593–612, Novembro.

Farias F. N. N., Júnior J. M. D., Salvatti J. J., Silva S., Abelém A. J. G., Salvador M.R., e Stanton M.A. (2011) “Pesquisa Experimental para a Internet do Futuro: Uma Proposta Utilizando Virtualização e o Framework Openflow”, Minicurso, Simpósio

Brasileiro de Redes de Computadores e Sistemas Distribuídos.

Habibi D. e Phung Q. V. (2012). "Graph Theory for Survivability Design in Communication Networks", New Frontiers in Graph Theory, Dr. Yagang Zhang (Ed.), ISBN: 978-953-51-0115-4, InTech, http://www.intechopen.com/books/new-frontiers-in-graph-theory/graph-theory-for-survivability-design-in-communication-networks

Heller B., Sherwood R., McKeown N. (2012) "The Controller Placement Problem", HotSDN'12, Helsinki, Finland, Agosto.

Hock D., Hartmann M., Gebert S., Jarschel M., Zinner T., Tran-Gia P. (2013) "Pareto-Optimal Resilient Controller Placement in SDN-based Core Networks", Proceedings of the 25th International Teletraffic Congress (ITC).

Lange S., Gebert S., Zinner, T., Tran-Gia P., Hock D., Jarschel M., Hoffman M. (2015) "Heuristic Approaches to the Controller Placement Problem in Large Scale SDN Networks", IEEE Transactions on Network and Service Management, Volume: 12, Issue 1, ISSN: 1932-4537, Março.

Latora V.; Marchiori M. (2001) "Efficient behavior of small-world networks", v. 87, n. 19, p. 198701. Disponível em: <http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.87.198701>.

McKeown N., Anderson T., Balakrishnan H., Parulkar G., Peterson L., Rexford J., Shenker S., e Turner J. (2008) "Openflow: enabling innovation in campus networks", SIGCOMM Comput. Commun. Rev., 38 (2):69–74, Março.

Metz J., Calvo R., Seno E. R. M., Romero R. A. F., Liang Z. (2007) "Redes Complexas: conceitos e aplicações", Relatórios Técnicos do Instituto de Ciências Matemáticas e de Computação, USP, Janeiro.

Müller L. F., Oliveira R. R., Luizelli M. C., Gaspary L. P., Barcellos M. P. (2014) "Survivor: An enhanced controller placement strategy for improving SDN survivability", Global Communications Conference (GLOBECOM) IEEE, ISBN: 978-1-4799-3512-3, Texas, Austin, USA, Dezembro.

ONF. (2015) "Openflow Switch Specification 1.5.1", https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.5.0.noipr.pdf, Março.

ONF. (2012) "Software-Defined Networking: The New Norm for Networks", Open Networking Foundation, Abril.

Ros F. J., Ruiz P. M. (2014) "Five Nines of Southbound Reliability in Software-Defined Networks", HotSDN'14, Chicago, IL, USA, Agosto.