

# Sistema Indicador de Resiliência na Conectividade de Redes Heterogêneas sem fio

Robson Melo, Michele Nogueira, Aldri Santos

<sup>1</sup>Núcleo de Redes Sem Fio e Redes Avançadas (NR2)  
Universidade Federal do Paraná – Curitiba – Brasil

{rgmelo, michele, aldri}@inf.ufpr.br

**Abstract.** *The dynamics and complexity of heterogeneous wireless networks difficult the development of adaptive security solutions to their conditions. The convergence of several communication technologies improves the connectivity, but they can also damage the availability of services on network. In this way, the network resilience is needed to tolerate the frequent disconnections, supporting the connectivity for several technologies. This paper presents an indicator system of security for heterogeneous wireless networks sensitive fragility and robustness of connectivity. The system evaluates the criticality of communication links and redundant routes between devices on the network to indicate the degree of security of the different access networks in an environment of overlapping heterogeneous networks. The results show that evaluation of availability of connectivity were accurate and that the proposal can be applied in different types of networks, supporting the creation of solutions focused on resilience and security in heterogeneous wireless networks.*

**Resumo.** *A dinamicidade e a complexidade das redes heterogêneas sem fio dificultam o desenvolvimento de soluções de segurança adaptativas às suas condições. A convergência de diferentes tecnologias de comunicação amplia as opções de conectividade, contudo, agregada aos problemas de segurança, podem afetar a disponibilidade dos serviços na rede. Soluções que garantam resiliência à rede são necessárias para tolerar as frequentes desconexões dos terminais móveis e ainda assim garantir a disponibilidade de conectividade por diferentes tecnologias de comunicação. Este trabalho apresenta um sistema indicador de resiliência, particularmente fragilidade e robustez, na conectividade de redes heterogêneas sem fio. O sistema avalia a criticidade dos enlaces de comunicação e a redundância de rotas entre os dispositivos na rede para indicar o grau de resiliência de diferentes redes de acesso em um ambiente de redes heterogêneas sobrepostas. Os resultados mostram a efetividade do sistema em avaliar a fragilidade e a robustez da conectividade e a aplicação do mesmo em diferentes tipos de redes, suportando a criação de soluções voltadas à resiliência e a segurança em redes heterogêneas sem fio.*

## 1. Introdução

A popularização dos dispositivos computacionais portáteis e o aumento da disponibilidade das redes de acesso têm intensificado o desejo dos usuários por conectividade em qualquer lugar e a todo instante [Melo et al. 2013]. As redes heterogêneas, formadas por diferentes redes com tipo de tecnologias de comunicação distintas, buscam atender a essa

demanda. Contudo, a convergência dessas diferentes tecnologias de comunicação traz consigo alguns problemas, principalmente sob o aspecto de segurança. As vulnerabilidades de segurança restritas a apenas um tipo de rede pode intensificar as vulnerabilidades de outras tecnologias além de se proliferar mais facilmente [Ghosh et al. 2012].

As soluções de segurança concebidas de forma individualizada para cada tipo de rede nem sempre são eficazes e necessitam ser repensadas quando aplicadas em redes heterogêneas [He et al. 2013]. A convergência de diferentes tecnologias de comunicação amplia as opções de conectividade, mas os problemas de segurança podem comprometer diretamente a disponibilidade dos serviços na rede e principalmente sua conectividade [Melo et al. 2013]. Em redes heterogêneas sem fio, o serviço de *handoff*, que corresponde à transição de conexão de uma rede para outra, pode sofrer interferências e ações de usuários maliciosos e acabar por indisponibilizar a comunicação [He et al. 2013]. Os dispositivos móveis conectados em uma rede *mesh* sem fio que migram suas conexões para redes *celulares 3G*, por exemplo, passam a ficar expostos aos problemas e vulnerabilidades inerentes a essas redes e podem sofrer interrupções em seus fluxos de dados.

Um outro agravante consiste na seleção da tecnologia e tipo de rede de acesso mais adequado em áreas com inúmeras redes sobrepostas. O *handoff* de uma rede para a outra sem uma avaliação prévia das condições da nova rede pode comprometer seriamente a transmissão de dados dos usuários, além de expô-los a riscos de segurança e à indisponibilidade de conectividade. A disponibilidade de conectividade em redes heterogêneas sem fio é afetada pela *criticidade* dos enlaces de comunicação. Os enlaces são considerados *críticos* a medida que sua interrupção indisponibiliza os serviços de comunicação, tais como o roteamento de pacotes e a comunicação fim-a-fim. Uma variedade de ameaças, como ataques, acidentes e falhas, pode causar degradações menores ou maiores independente do tipo de tecnologia utilizada. Contudo, as vulnerabilidades inicialmente restritas a um determinado cenário podem ser exploradas de modo mais amplo nesses ambientes heterogêneos convergentes.

A resiliência, decorrente da capacidade da rede de proporcionar e manter um nível aceitável do serviço em face a falhas e desafios para sua operação normal tem sido uma estratégia amplamente utilizada no combate às degradações na disponibilidade da conectividade [Heegaard and Trivedi 2009, Sterbenza et al. 2010]. O uso da tolerância a desafios, que consiste na capacidade de um sistema tolerar faltas tal que não ocorram falhas de serviço [Group 2004], também tem sido discutido. Contudo, essa abordagem depende de redundância como uma técnica para compensar falhas aleatórias e não correlacionadas. Logo, a tolerância a desafio não é suficiente diante de múltiplas falhas correlacionadas, portanto é necessária, mas não suficiente para prover resiliência e segurança à rede.

Deste modo, as soluções que garantam resiliência e segurança à rede são fundamentais para tolerar as frequentes desconexões dos dispositivos móveis e ainda assim garantir a disponibilidade de conectividade através de diferentes tecnologias de comunicação [Melo et al. 2013, Lima et al. 2009]. As estratégias que analisam tanto a *fragilidade* como a *robustez* da conectividade da rede são importantes para o desenvolvimento proativo de contramedidas que possam evitar interrupções, ou maiores degradações, nos serviços de comunicação. Além de auxiliarem na análise das condições da rede, permitindo um acesso seguro em redes heterogêneas sem fio sobrepostas.

Este trabalho apresenta um sistema indicador de resiliência na conectividade de redes heterogêneas sem fio. O objetivo do sistema consiste em indicar quais redes são momentaneamente mais resilientes sob o aspecto de disponibilidade de conectividade, o que possibilita uma escolha adequada do acesso em um ambiente sobreposto por inúmeras redes heterogêneas sem fio. Outra característica deste sistema consiste em avaliar e apontar os índices de fragilidade e robustez de conectividade para que estratégias e contramedidas possam ser utilizadas proativamente garantindo resiliência e segurança à rede.

A *fragilidade* da conectividade da rede é verificada pela criticidade dos enlaces de comunicação que correspondem aos links mais vulneráveis a falhas de operação e que podem desconectar a rede a medida que forem afetados. Em contrapartida, a *robustez* é analisada pela existência de rotas redundantes entre vizinhos de um dado dispositivo na rede, que se tornam alternativas as falhas de conectividade em uma dada comunicação. A aferição da fragilidade e da robustez permite determinar qual rede possui melhor condição de conectividade em um dado instante entre as diferentes redes disponíveis. Essa informação possibilita a escolha e a seleção da melhor rede de acesso no momento de transição por áreas com inúmeras redes heterogêneas sem fio sobrepostas.

A avaliação do sistema verifica a eficácia do indicador de resiliência no cálculo da fragilidade e da robustez das conectividades em redes heterogêneas sem fio. Foram utilizados traços de redes heterogêneas reais do projeto *MeshNet*. Os resultados mostraram que o sistema proposto conseguiu indicar com precisão o conjunto de enlaces críticos, bem como as rotas redundantes presentes na rede. Além de permitir seu uso com efetividade para a análise da fragilidade e da robustez de conectividade de redes heterogêneas sem fio, independente do tipo de tecnologia utilizada.

O restante deste trabalho está organizado da seguinte maneira: a Seção 2 apresenta os trabalhos relacionados. A Seção 3 descreve a modelagem do sistema. A Seção 4 detalha o sistema proposto, bem como o seu funcionamento. A Seção 5 apresenta a análise e avaliação do sistema e a Seção 6 conclui o trabalho.

## 2. Trabalhos relacionados

Trabalhos na literatura têm destacado a necessidade de tornar a conectividade das redes heterogêneas sem fio a fim de tolerar as frequentes desconexões de dispositivos móveis e os problemas de indisponibilidade, causados pela transição de terminais que migram suas conexões por redes de diferentes tecnologias de comunicação [Zhang et al. 2008, Ben Hadj Said et al. 2012, Ghosh et al. 2012, Lin et al. 2011]. O trabalho de [Sun et al. 2005] apresenta uma arquitetura para o gerenciamento de conectividade ciente de contexto para dispositivos móveis em redes heterogêneas sem fio. A plataforma fornece interfaces para os aplicativos consultarem a QoS de rede e as condições de disponibilidade da conectividade. Apesar da avaliação e análise da disponibilidade de conectividade, a proposta não considera aspectos de resiliência como estratégia de segurança.

O trabalho de [Gardner et al. 2013] descreve um algoritmo de *Self-Pruning* para a identificação de eventos raros e para a análise de resiliência da rede. O método de análise da resiliência utiliza características da própria rede com base no impacto dos eventos acontecidos. Os autores consideram eventos raros mais importantes na rede, como desastres naturais, rompimento de enlaces, catástrofes e outros, que não são identificados pelas abordagens tradicionais. Uma métrica para mensurar o impacto desses eventos em

uma rede heterogênea sem fio formada por cidades dos EUA foi apresentada. As medidas de conectividade e a capacidade da rede também foram utilizadas na análise. Os resultados mostraram que o impacto de um evento raro pode ser usado como uma métrica de avaliação da rede. Contudo, os próprios autores mencionam a necessidade de avaliação da resiliência da topologia da rede a fim de determinar os índices de fragilidade e robustez de sua conectividade.

O trabalho de [Zhang and Sundaram 2012] apresenta uma avaliação da robustez com base em teoria de redes complexas. Os autores consideram como métrica principal o grau mínimo dos vértices para medida de robustez. Os autores discutem a dificuldade de consenso entre os nós da rede com a presença de agentes mal intencionados difundindo informação. A modelagem analítica apresentada utilizou o modelo de redes complexas de Erdos-Rényi com grafos randômicos de larga escala. Os resultados mostram que o consenso pode ser alcançado de modo resiliente, e sem a necessidade de informação global, em grafos que são suficientemente robustos. No entanto, o uso desta métrica como método de determinar a robustez pode não ser suficiente para outros modelos de redes mais generalizadas como redes heterogêneas que possuem uma alta dinamicidade em sua infraestrutura devido às frequentes associações e dissociações dos dispositivos na rede.

### 3. Modelo de conectividade da rede

Esta seção descreve as premissas assumidas e prevê a definição dos enlaces críticos para redes heterogêneas sem fio. A conectividade da rede consiste na existência de uma conexão, direta ou através de enlaces intermediários, entre quaisquer dois dispositivos na rede, independente do tipo de tecnologia utilizada. A natureza dinâmica das redes heterogêneas sem fio é resultado da mobilidade dos dispositivos ou do uso de diferentes tecnologias de comunicação. Um *grafo dinâmico não direcionado*  $G = (V, E)$ , representa a rede heterogêneas sem fio, em que  $V$  corresponde a um conjunto finito de vértices que caracterizam os dispositivos (nós) da rede, e  $E$  é um conjunto finito de arestas indicando os enlaces (links) entre os pares de dispositivos. Os *grafos dinâmicos* são atualizados pela inserção ou remoção de vértices e arestas a qualquer momento. Assim, dada uma aresta  $e = \{u, v\} \in E$ , ela é dita incidente em  $u$  e  $v \in V$ . Logo, uma aresta entre  $u$  e  $v$  representa um enlace na rede com comunicação em ambos os sentidos.

O grafo  $G'$  obtido a partir de  $G$  representa um instante qualquer  $t$ , em que a rede está totalmente conectada. Assim, em cada instante  $t$ , existe um grafo completamente conexo para a topologia de conectividade da rede. Um grafo  $G'$  é totalmente conexo, se existe um *caminho*  $P_v^u$  para quaisquer  $u, v \in V$ . Logo, um caminho entre dois vértices  $u$  e  $v$  em  $G'$  significa uma sequência de arestas em  $E$  que liga uma sequência de vértices em  $V$ . Deste modo,  $G'$  é chamado *conexo*, se para cada  $u, v$  um  $P_v^u$  existe. Na rede, um *caminho* compreende uma conexão (rota) entre dois nós ligados diretamente ou através de nós intermediários, independente do tipo de tecnologia de transmissão utilizada. A *distância*  $d(u, v)$  entre os dois vértices  $u$  e  $v$  corresponde ao número de arestas que existe no caminho entre  $u$  e  $v$ . O *caminho mínimo*  $P_v^u$  indica um caminho de *distância mínima*  $d(u, v)$ . Na rede, a *distância* entre dois nós consiste no número de enlaces existentes na conexão, e o *caminho mínimo* corresponde a uma conexão com menor número de enlaces.

Um enlace crítico consiste em qualquer enlace que se quebrado, por algum evento inesperado, desconecta a rede gerando uma falha de conectividade. Sendo assim, dado

um grafo  $G'$  um *corte*  $C_{G'}$  representa uma partição dos vértices  $V$  em dois subconjuntos disjuntos  $\{X, Y\}$ , unidos por pelo menos uma aresta. Este corte  $C_{G'}$  indica os enlaces mais propícios a falhas de conectividade da rede, causando sua separação em pelo menos duas novas redes distintas. Na rede, as arestas de corte são consideradas enlaces críticos. Portanto, um  $cut_v^u$  de  $G'$  corresponde a uma divisão nos conjuntos  $\{X, Y\}$  em que  $u \in X$  e  $v \in Y$ . O tamanho de  $C_{G'}$  consiste no número de enlaces críticos que, se removidos, desconectam a rede. O *corte mínimo* (*mincut*) de um grafo  $G'$  compreende um  $C_{G'}$  com o menor número de arestas (caso não ponderada, ou a menor soma de pesos das arestas caso ponderadas), ou seja, o número mínimo de enlaces críticos, que se falhos resultam em uma interrupção da conectividade da rede. A identificação do *corte mínimo* ajuda a apontar enlaces vulneráveis em uma conexão de rede.

Uma *árvore de corte mínimo*  $T_C$  de  $G'$  corresponde a um grafo induzido pela remoção de arestas, de modo que exista apenas um único caminho, de menor distância, para qualquer dois vértices  $u$  e  $v$  de  $G'$ . Formalmente,  $T_C$  consiste em uma árvore tal que, para cada  $u, v \in V$ , um corte induzido pela remoção do conjunto de arestas mínimas de  $P_v^u$  em  $T_C$  é um  $mincut_v^u$  de  $G'$ . Para a rede,  $T_C$  significa uma nova rede formada com conexões de menor número de enlaces entre quaisquer dois dispositivos, sem a existência de rotas alternativas entre eles. A descoberta do *corte mínimo* em um caminho específico auxilia na identificação de pontos de vulnerabilidades de enlaces na rede dado um dispositivo origem e um destino.

#### 4. Sistema indicador de resiliência na conectividade de redes heterogêneas

O sistema indicador de resiliência na conectividade das redes heterogêneas sem fio calcula os índices de fragilidade e de robustez e indica quais redes são momentaneamente mais seguras em termos de disponibilidade de conectividade. Isso possibilita a escolha adequada do acesso em um ambiente sobreposto por inúmeras redes heterogêneas sem fio. Além disso, esses indicadores poderão auxiliar na definição de estratégias e contramedidas a serem desenvolvidas a fim de prover princípios de resiliência e segurança.

O sistema compreende três componentes: o *Verificador de Conectividade*, o *Medidor de Criticidade de Enlaces* e o *Medidor de Redundância de Rotas*, conforme ilustrado na Figura 1. O sistema recebe como entrada informações da topologia de cada rede de acesso detectada, extrai um grafo de conectividade, calcula a criticidade dos enlaces e a redundância de rotas em cada rede, e fornece um índice de fragilidade e robustez da conectividade de cada uma das redes disponíveis.

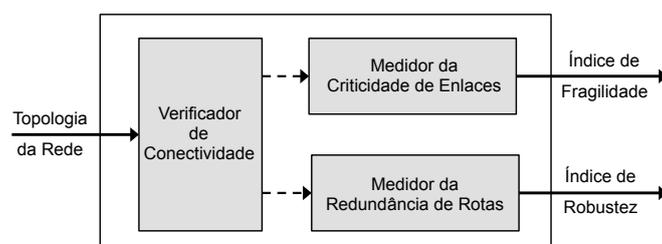


Figura 1. Arquitetura do sistema indicador de resiliência

O componente *Verificador de Conectividade* extrai um grafo de conectividade da rede a partir das informações de sua topologia. Na sequência, verifica a existência de

caminhos para todos os nós do grafo, constatando sua conectividade. Se nós isolados forem detectados classifica-se a rede como desconexa, caso contrário, sua conectividade será avaliada. O grafo de conectividade é encaminhado para os componentes medidor de criticidade de enlaces e medidor de redundância de rotas.

O componente *Medidor de Criticidade de Enlaces* recebe o grafo de conectividade e calcula os enlaces críticos, isto é, aqueles que se removidos são capazes de desconectá-lo. Esses enlaces são referência para o cálculo do índice de *Fragilidade de Conectividade da Rede* ou apenas *Fragilidade da Rede* (NF). O *Medidor de Redundância de Rotas* utiliza o grafo de conectividade da rede para verificar a existência de enlaces entres os vizinhos de um nó. Esse processo se repete até que a análise seja feita para todos os nós do grafo. O resultado desta análise é utilizado para caracterizar o índice de *Robustez de Conectividade da Rede* ou simplesmente *Robustez da Rede* (NR). As etapas para o cálculo destes dois índices são detalhadas a seguir.

#### 4.1. Medidor de criticidade de enlaces

A fragilidade da rede está diretamente relacionada com a vulnerabilidade a falha dos enlaces críticos. Desta forma, o cálculo da fragilidade tem como referência as *árvores de corte mínimo*, as quais indicam em um grafo a quantidade de enlaces necessários para desconectar a rede. As árvores de corte mínimo contém todos os vértices do grafo de topologia de conectividade da rede e um conjunto de arestas ponderadas. O peso de cada aresta na árvore corresponde ao número de enlaces necessários para a desconexão.

Dado um grafo  $G'$  que representa a topologia de conectividade da rede em um instante  $t$ , o algoritmo de árvores de corte mínimo retorna um novo grafo ponderado  $T_C$ . O  $w$  representa o peso de cada aresta e  $W_c$  o conjunto de todos os  $w$  do grafo. Os pesos  $W_c$  correspondem a todos os cortes mínimos  $mincut_v^u$  entre todos os pares de vértices  $u, v$ . O  $mincut_v^u$  representa o menor número de enlaces entre  $u, v$  que, se removidos, desconectam o grafo. Estes por sua vez são denominados enlaces críticos.

A *fragilidade da rede* é calculada a partir da árvore de corte mínimo  $T_C$  e do conjunto de pesos  $W_c$ . Com base nos resultados apresentados em [J. and M'Raïhi 1998] [Arce 2003], a fragilidade da rede é obtida por uma relação entre o menor e o maior número de enlaces expostos a perturbações na topologia de conectividade da rede. Logo, NF indica a relação entre o peso mínimo e o máximo de  $T_C$  para todos os pesos  $w$  pertencentes à  $W_c$ , como mostrado pela Equação 1. Uma topologia com *alta fragilidade* corresponde àquela que necessita de um menor número de enlaces removidos para desconectá-la, caso contrário, define-se como topologia de *baixa fragilidade*.

$$NF = \frac{\min\{w \mid \forall w \in W_c\}}{\max\{w \mid \forall w \in W_c\}} \quad (1)$$

#### 4.2. Medidor de redundância de rotas

A existência de rotas redundantes representa a robustez de conectividade da rede. Essas rotas se tornam alternativas às falhas de conectividade em uma dada comunicação, particularmente entre os vértices críticos (CV), que são conectados por enlaces críticos. A robustez é aferida por meio da técnica de agrupamento (clusterização), que verifica as conexões existente entre os vizinhos dos vértices no grafo. A partir desta medida, calcula-se

um índice local, para um único nó e um índice global para a rede como um todo, que serão usados na definição de NR.

Dado um grafo  $G'$ , o vértice  $v$  é dito vizinho de  $u$  se existe uma aresta direta entre ambos. O grau de  $v$  corresponde à soma de seus vizinhos, denotado por  $d_v$ . O coeficiente de agrupamento de  $v$  consiste na quantidade de arestas que os vizinhos de  $v$  têm entre eles, dividido pela quantidade total de arestas que  $v$  poderia ter. A partir de  $d_v$ , o maior número de arestas que  $v$  pode ter é dado por  $B = \binom{d_v}{2}$ . Seja  $E_v$  o número real de arestas que  $v$  possui, ou seja, o seu número atual de vizinhos, o coeficiente de agrupamento de  $v$  é definido pela Equação 2. O coeficiente de agrupamento  $C_v$  indica o nível de redundância que um nó tem em termos de conexões. Esta medida também indica o número de cliques, de tamanho 3, no grafo de conectividade da rede.

$$C_v = \frac{E_v}{B} = \frac{2 \cdot E_v}{d_v \cdot (d_v - 1)} \quad (2)$$

O coeficiente de agrupamento local  $C_v$  dos vértices possibilita calcular um valor global para a rede toda,  $C_{Global}$ . Neste caso, definido como o menor  $C_v$  entre todos os vértices de  $G'$ , como mostrado na Equação 3.

$$C_{Global} = \min\{C_v \mid \forall v \in V_G\} \quad (3)$$

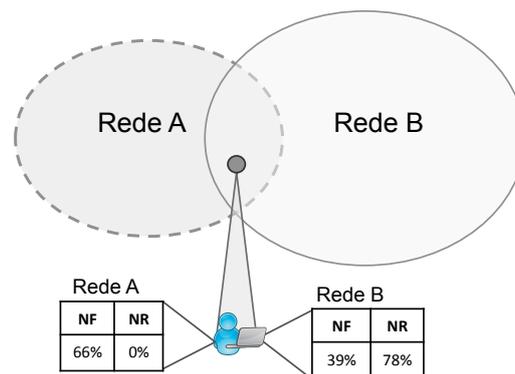
Os valores de  $C_{Global}$  e  $C_v$  permitem calcular o valor da NR, denotado pela Equação 4. Esta medida incide sobre os enlaces e os nós mais frágeis da rede. Logo, NR implica na relação entre o  $C_{Global}$  e o máximo  $C_v$  calculado para todos os vértices contidos no conjunto de vértices críticos (CV). Por sua vez, CV corresponde a todos os vértices presentes no caminho relacionado ao menor corte mínimo  $mincut_v^u$  de  $T_C$ .

$$NR = \frac{C_{Global}}{\max\{C_v \mid \forall v \in CV\}} \quad (4)$$

Com os índices de fragilidade e robustez fornecidos pelo sistema indicador de segurança cada dispositivo móvel em transição por diferentes redes de acesso consegue selecionar a rede mais segura em termos de disponibilidade de conectividade em ambientes sobrepostos por inúmeras redes heterogêneas sem fio. Além de uma avaliação momentânea das condições de conectividade da rede o sistema ajuda a evitar que os dispositivos móveis em transição se conectem em redes de acesso comprometidas e tenha suas comunicações interrompidas. Outra vantagem dos índices inferidos pelo sistema consiste em permitir que medidas proativas de prevenção possam ser desenvolvidas para evitar a indisponibilidade de conectividade da rede garantindo resiliência e segurança.

### 4.3. Funcionamento do sistema indicador de resiliência

Para exemplificar o funcionamento do sistema indicador de resiliência foi considerado um cenário em que um usuário portador de um dispositivo computacional móvel encontra-se em uma área de sobreposição de duas (ou mais) redes de acesso heterogêneas sem fio, como ilustrado na Figura 2. Antes de se conectar em qualquer uma das redes o sistema



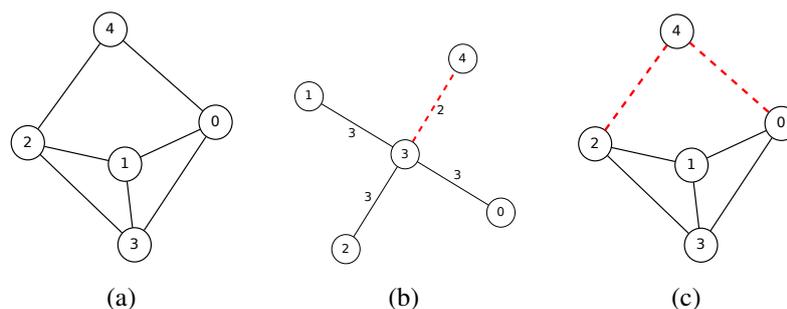
**Figura 2. Cenário de funcionamento do sistema indicador de resiliência**

avalia as condições de conectividade indicando os índices de fragilidade e robustez de ambas as rede. Com esses indicadores o usuário pode se conectar na rede mais resiliente.

O sistema indicador inicia sua operação a partir da obtenção de informações da topologia de todas as redes detectadas. Neste exemplo, as informações da topologia são representadas por uma *lista de adjacência* disponibilizada pelo provedor de acesso de cada rede. O componente *Verificador de Conectividade* realiza uma *busca em largura* nos dados da topologia da rede e retorna um grafo de conectividade da mesma. A Figura 3(a) ilustra o grafo de conectividade da “Rede A”.

O componente *Medidor de Criticidade de Enlaces* recebe o grafo de conectividade e identifica o conjunto de enlaces críticos através da árvore de corte mínimo. Neste trabalho, a árvore de corte mínimo foi obtida por meio do algoritmo de Gomory-Hu [Gomory and Hu 1961]. O algoritmo de Gomory-Hu tem como entrada um grafo da topologia de conectividade e retorna uma árvore de corte mínimo. A árvore de corte mínimo  $T_C$  e o conjunto de pesos  $W_c$ , obtidos com o algoritmo são construídos com a computação de  $|V| - 1$  corte mínimo.

A Figura 3(a) mostra um grafo  $G'$  que representa uma topologia de conectividade da “Rede A” em um instante  $t$ . A Figura 3(b) ilustra uma árvore de corte mínimo  $T_C$  extraído do grafo  $G'$  e seus pesos  $w$  representam a quantidade de arestas, que são necessárias para desconectar  $G'$ . Por exemplo, em  $T_C$  ilustrada pela Figura 3(b), a aresta tracejada em destaque entre os vértices 4 e 3 possui um peso  $w$  de valor 2, o que significa que se duas arestas que conectam os vértices 4 e 3 forem removidas, a rede será desconectada. De mesmo modo, diferentes arestas em  $T_C$  empregam essa mesma lógica.



**Figura 3. Análise de fragilidade**

Na Figura 3(b), entre todas as arestas de  $T_C$ , o peso  $w$  mínimo corresponde 2 e o máximo 3, para todo conjunto  $W_c$ . Assim, usando a Equação 1, o resultado é de aproximadamente 0,66, o que indica que o nível de fragilidade para esta rede corresponde a 66% (em relação aos seus enlaces). Com base neste exemplo, o corte mínimo envolve dois enlaces diferentes na topologia da conectividade da rede. Estes dois enlaces são chamados enlaces críticos e estão nas conexões entre os nós 4 e 3, como mostrado na Figura 3(c) pelas linhas tracejadas. Logo, os vértices conectados por enlaces críticos são denominados como vértices críticos. Na Figura 3(c), os vértices críticos são 4, 2 e 0.

Em paralelo à operação realizada pelo componente *Medidor de Criticidade de Enlaces*, o terceiro componente do sistema, o *Medidor de Redundância de Rotas* também é executado. Esse componente calcula o coeficiente de agrupamento dos vértices do grafo de conectividade. A Figura 4(a) mostra o coeficiente de agrupamento local  $C_v$  calculado para cada vértice e a Figura 4(b) mostra o valor do coeficiente de agrupamento global  $C_{Global}$  calculado para toda a rede. Dado que o valor de  $C_{global}$  implica no menor  $C_v$ , calculado para todo conjunto de vértice  $V$  do grafo  $G'$ , o valor de  $C_{global}$  para essa rede exemplificada pela Figura 4(a) corresponde a 0,0. Deste modo, utilizando a Equação 4, para esse exemplo, tem-se que  $C_{Global}$  corresponde a 0,0 e o maior  $C_v$  equivale a 0,66. Logo, o valor de NR implica em 0,0, e indica o índice de robustez da rede.

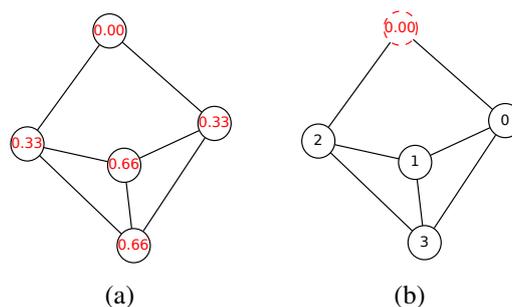


Figura 4. Análise de robustez

Esse procedimento realizado para a análise das condições de conectividade da “Rede A” também é realizado para a “Rede B”. Assim, a partir dos resultados dos índices de fragilidade e robustez de cada rede o dispositivo móvel em transição poderá se conectar na rede de acesso mais segura em termos de disponibilidade de conectividade.

## 5. Análise e avaliação do sistema indicador de resiliência

Esta seção apresenta a análise do sistema indicador de resiliência na conectividade de redes heterogêneas sem fio, cujo o objetivo consiste em identificar os índices de fragilidade e robustez da conectividade dessas redes.

### 5.1. Metodologia

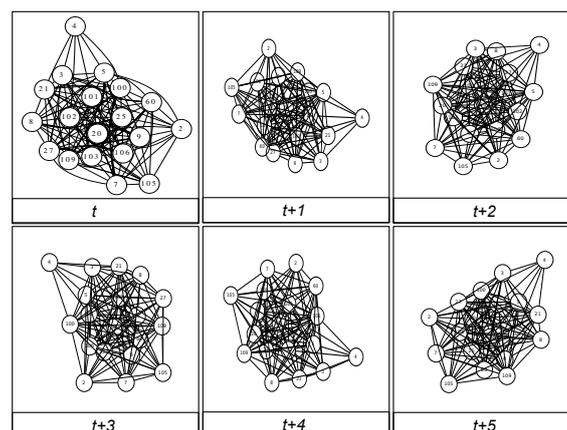
A análise do sistema indicador de resiliência foi realizada utilizando traços reais da rede *mesh* do projeto *UCSB MeshNet* da Universidade da Califórnia em Santa Barbara, nos Estados Unidos. A rede representa um ambiente de um campus universitário, composta por 19 nós que operam nos padrões *802.11a/b*, criando uma rede heterogênea em termos de seus padrões de comunicação [Meshnet 2013]. Os dispositivos móveis conectados na

rede fazem transições de suas conexões durante a sua mobilidade, mudando constantemente a topologia de conectividade da rede. Os dados utilizados correspondem a testes realizados em 2007 e estão disponíveis no repositório web CRAWDAD<sup>1</sup>.

A base de dados é formada por 900 arquivos contendo as listas de adjacências da topologia da rede. Cada arquivo representa um instante de tempo com as condições de conectividade da rede. Com o objetivo de avaliar apenas os instantes em que a rede era conexa, um script subtrai os arquivos que continham instantes em que a rede era desconexa, resultando em 577 arquivos. Cada linha dos arquivos determina as conexões entre os nós. O primeiro elemento da linha consiste no endereço IP de um nó específico, seguido de uma lista que contém o endereço IP com quem o primeiro nó tem conexão. Um exemplo pode ser visualizado no quadro a seguir.

10.1.1.2	10.1.1.60	10.1.1.9	10.1.1.100	10.1.1.103	10.1.1.5
----------	-----------	----------	------------	------------	----------

Essa linha representa as conexões do nó 10.1.1.2. Nesse instante de tempo, ele possui conexões com os nós 10.1.1.60, 10.1.1.9, 10.1.1.100, 10.1.1.103 e 10.1.1.5. Para a representação da conectividade da rede a Figura 5 ilustra seis topologias da mesma rede em diferentes instantes de tempo  $t$ .



**Figura 5. Exemplos de grafos de conectividade da rede em diferentes instantes**

A partir do grafo foi possível definir uma estrutura de dados para a execução do algoritmo de árvores de corte mínimos de *Gomory-Hu* e para o cálculo do coeficiente de agrupamento. A biblioteca LEMON fornece diversos algoritmos e estruturas de dados próprias para a manipulação de dados relacionados a teoria de grafos [Lemon 2013]. Neste trabalho, a biblioteca LEMON foi utilizada para extrair a árvore de corte mínimo de cada topologia utilizada. Um script Python foi implementado para automatizar todo o processo de análise dos vários arquivos e grafos. O script faz a leitura e o tratamento dos dados, depois com o grafo estruturado é gerada uma segunda estrutura específica da biblioteca LEMON e nessa etapa as informações necessárias são coletadas para o cálculo do coeficiente de agrupamento individual. Na etapa seguinte o algoritmo de *Gomory-Hu* é executado e o coeficiente de agrupamento é calculado, a partir do algoritmo, os  $mincut_v^u$  de cada vértice são calculados. Na última etapa o script organiza esses dados em uma tabela para análise futura.

<sup>1</sup><http://crawdad.cs.dartmouth.edu/meta.php?name=ucsb/meshnet>

## 5.2. Avaliação da fragilidade

A *fragilidade alta* consiste na menor quantidade de enlaces necessária para a desconexão da rede. Já a *fragilidade baixa* consiste na maior quantidade de enlaces críticos para a desconexão. Assim, quanto menos enlaces necessários para desconectar a rede maior sua fragilidade, quanto mais enlaces necessários para sua desconexão menor é a fragilidade da rede. O algoritmo de árvore de corte mínimo de *Gomory-Hu* foi utilizado para quantificar o conjunto de enlaces necessários para a desconexão da rede, bem como, identificar a localização desses enlaces, considerados críticos.

A Figura 6(a) ilustra um grafo  $G'$  representando um determinado instante  $t$  de conectividade da rede *MeshNet*, ao aplicar o algoritmo de *Gomory-Hu* obtemos a árvore de corte mínimo, Figura 6(b), e partir desta árvore, podemos identificar que a quantidade mínima de arestas necessárias para a desconexão do grafo é seis (indicada pelo peso da linha pontilhada), as quais conectam o nó 4 ao restante da rede. A partir da quantidade de arestas descobertas que desconectam a rede, realizamos a identificação e a localização destas arestas no grafo original, indicadas pelas linhas tracejadas na Figura 6(c). Como visto na Figura 6(c), as arestas que conectam o nó 4 aos nós 3, 5, 21, 100, 101 e 102 são os enlaces críticos da rede no instante  $t$ . Deste modo, ao remover apenas esse conjunto mínimo de enlaces, desconecta-se a rede.

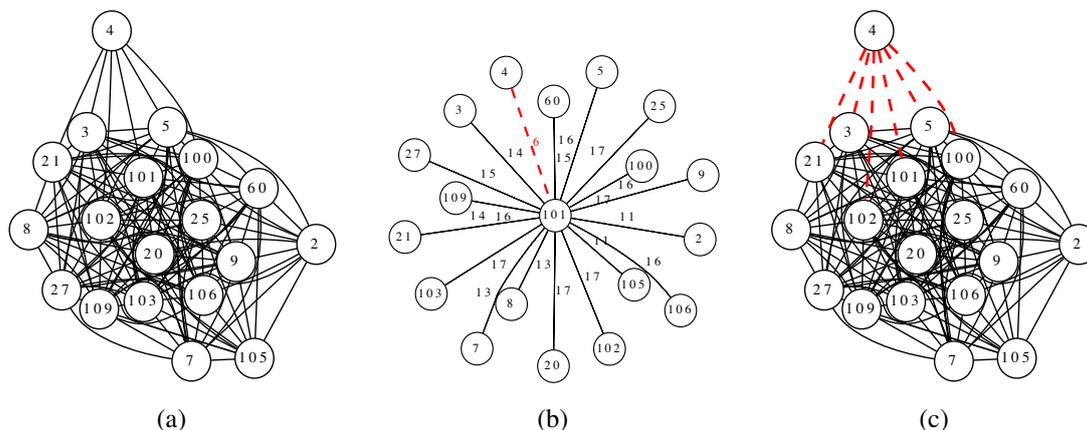


Figura 6. Análise do grafos de conectividade no instante  $t$

Posterior à análise de um instante específico, foi realizado o processamento de todos os arquivos representando as condições global da rede para todo seu período de funcionamento. A Figura 7(a) ilustra a variação da quantidade de vizinhos de cada nó em todos os instantes da rede, o que mostra a dinamicidade durante seu funcionamento. A Figura 7(b) apresenta a variação do número de arestas críticas da rede.

Apesar da dificuldade em garantir a conectividade a todo instante, observa-se certa estabilidade entre os valores de enlaces críticos, variando entre seis e oito arestas do grafo de conectividade. Outro comportamento observado é a existência de repetições de alguns enlaces específicos, que aparecem no grupo de arestas de fragilidade alta. Isso indica que esses enlaces constantemente estão entre os mais frágeis, como ilustrado na Figura 7(c).

A Tabela 1 ilustra as arestas pertencentes a cada conjunto de enlaces críticos. A Figura 7(c) mostra que as arestas pertencentes ao conjunto  $A$  aparecem constantemente

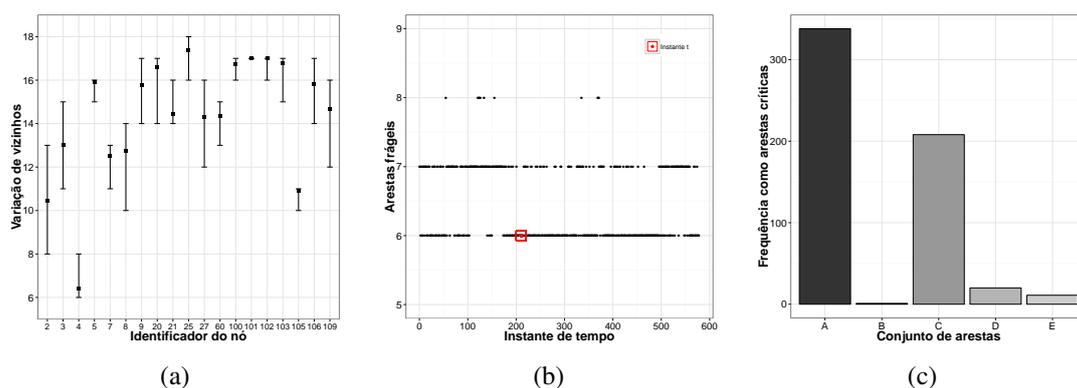


Figura 7. Avaliação da fragilidade

entre as arestas de fragilidade alta. Deste modo, é possível afirmar que as arestas do conjunto *A* são os enlaces mais frágeis da rede.

Conjuntos	Arestas							
A	4, 101	3, 4	4, 100	4, 5	4, 21	4, 102	-	-
B	4, 101	3, 4	4, 100	4, 5	4, 21	4, 25	-	-
C	4, 101	3, 4	4, 100	4, 5	4, 21	4, 25	4, 102	-
D	4, 101	4, 8	3, 4	4, 100	4, 5	4, 21	4, 102	-
E	4, 101	4, 8	3, 4	4, 100	4, 5	4, 21	4, 25	4, 102

Tabela 1. Descrição do conjunto de arestas da Figura7(c).

### 5.3. Avaliação da robustez

A robustez foi mensurada de forma local pelo número de conexões entre os vizinhos de um nó, e de forma global para toda a rede. Assim, a robustez da conectividade da rede é determinada pela relação entre o índice global e o índice local, deste modo, nenhum nó frágil será ocultado pela média do coeficiente de agrupamento. Dado um determinado instante  $t$  de conectividade da rede ilustrado pela Figura 6(a), foi aplicada a técnica de clusterização para encontrar os valores dos coeficientes de agrupamento locais, como observado na Figura 8(a), em que os valores de cada nó representam seu índice de robustez. Como o agrupamento global da rede é representada pelo menor índice local, a Figura 8(b) ilustra o grafo do instante  $t$  com o nó que determina o valor do coeficiente de agrupamento global da rede. Como visto na Figura 8(b), três nós possuem os mesmos valores, correspondentes ao menor índice da rede. Logo, qualquer um deles pode ser utilizado para o cálculo do índice de robustez da rede.

Após a análise individual do instante  $t$ , foram realizadas as análises para todo o período de funcionamento da rede a fim de encontrar a variação dos valores de clusterização local de cada nó e os valores para a clusterização global. A Figura 9(a) mostra os gráficos de variação da clusterização local de cada nó durante todos os 577 instantes em que a rede esteve totalmente conectada. A Figura 9(b) ilustra a variação da clusterização global durante todo tempo de atividade da rede.

Com base nos resultados é possível identificar qual o nó que por maior período determina o valor de agrupamento global da rede, e define o valor de robustez da mesma, por ser o nó de menor índice de clusterização. A Figura 9(c) ilustra o número de vezes que um nó determina o valor da clusterização global da rede. Logo, a partir dos resultados é possível afirmar que o nó 101 corresponde ao nó que por maior período determinou o

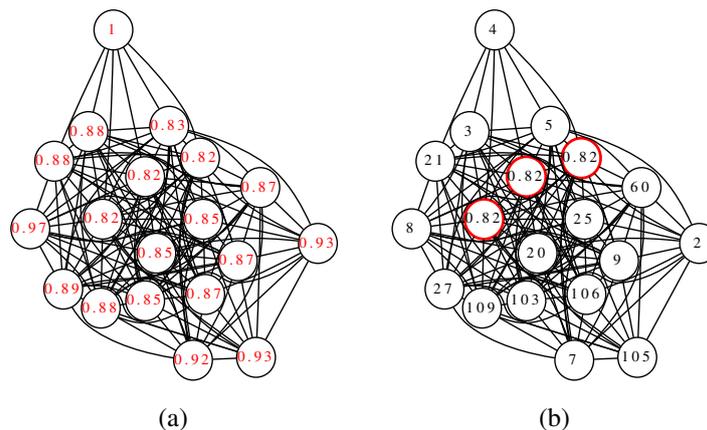


Figura 8. Análise de agrupamento da rede

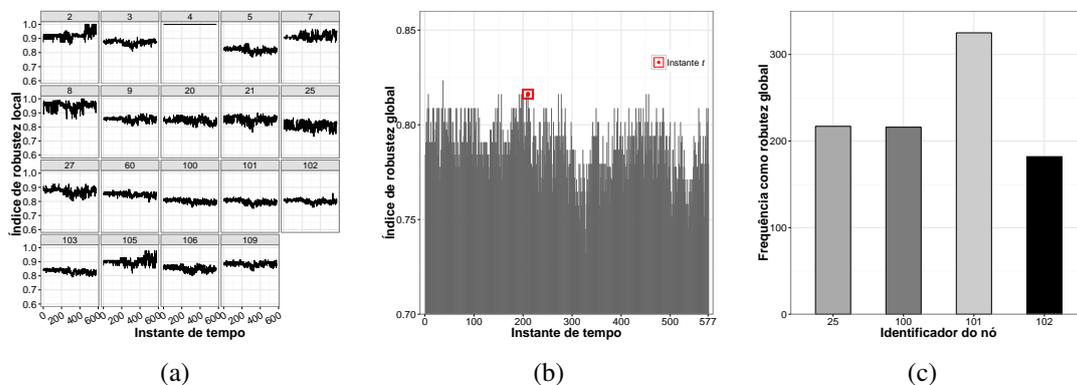


Figura 9. Avaliação da robustez

valor de clusterização global. Deste modo, esse mesmo nó foi usado por mais vezes para o cálculo do valor de robustez da rede.

## 6. Conclusão

O trabalho apresentou um sistema que mede a resiliência de redes heterogêneas sem fio no momento da tomada de decisão de transição de acesso entre redes. Este sistema indica quais redes são momentaneamente mais seguras sob o aspecto de disponibilidade de conectividade, possibilitando aos dispositivos móveis em transição uma escolha adequada do acesso em um ambiente sobreposto por inúmeras redes heterogêneas sem fio. O sistema avalia e aponta os índices de fragilidade e robustez de conectividade de modo que estratégias e contramedidas possam ser aplicadas para garantir a resiliência e segurança à rede. A avaliação do sistema considera traços reais de uma rede heterogênea sem fio. Os resultados mostraram a eficácia do sistema na identificação dos índices de fragilidade e de robustez da conectividade da rede em diferentes momentos de avaliação. Como trabalho futuro, pretende-se usar esse sistema para apoiar o desenvolvimento de soluções voltadas à resiliência e a segurança de redes heterogêneas sem fio.

## Referências

Arce, I. (2003). The weakest link revisited. *IEEE Security Privacy*, 1(2):72–76.

- Ben Hadj Said, S., Guillooard, K., and Bonnin, J. (2012). On the need for adaptive connectivity management in multi-access architectures. In *IEEE NOF*, páginas 1–5.
- Gardner, M., Beard, C., and Medhi, D. (2013). Using network measure to reduce state space enumeration in resilient networks. In *IEEE DRCN*, páginas 250–257.
- Ghosh, A., Mangalvedhe, N., Ratasuk, R., Mondal, B., Cudak, M., Visotsky, E., Thomas, T. A., Andrews, J. G., Xia, P., Jo, H. S., Dhillon, H. S., and Novlan, T. D. (2012). Heterogeneous cellular networks: From theory to practice. *IEEE Communications Magazine*, 50(6):54–64.
- Gomory, R. E. and Hu, T. C. (1961). Multi-Terminal Network Flows. *Journal of the Society for Industrial and Applied Mathematics*, 9(4):551–570.
- Group, T. W. (2004). Reliability-related metrics and terminology for network elements in evolving communications networks. *Alliance for Telecommunications Industry Solutions (ATIS)*.
- He, D., Bu, J., and Zhang, Y. (2013). Security and efficiency in roaming services for wireless networks: challenges, approaches, and prospects. *IEEE Communications Magazine*.
- Heegaard, P. E. and Trivedi, K. S. (2009). Network survivability modeling. *Computer Networks*, 53(8):1215–1234.
- J., M. and M’Raïhi, D. (1998). Mix-based electronic payments. In *Proc. of the Selected Areas in Cryptography*, páginas 157–173.
- Lemon (2013). Library for efficient modeling and optimization in networks. <http://lemon.cs.elte.hu/trac/lemon>. Último acesso: junho 2014.
- Lima, M., dos Santos, A. L., and Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks. *IEEE Communications Surveys & Tutorials*, 11(1):66–77.
- Lin, P., Zhang, J., Chen, Y., and Zhang, Q. (2011). Macro-femto heterogeneous network deployment and management: from business models to technical solutions. *IEEE Wireless Communications*, páginas 64–70.
- Melo, R., Santos, A., Nogueira, M., and Medhi, D. (2013). *Anais / 31º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, chapter Modelagem e projeto de redes sem fio heterogêneas, resilientes e sobreviventes, páginas 1–50. SBC.
- Meshnet (2013). Mesh testbed is an experimental wireless mesh network. <http://moment.cs.ucsb.edu/meshnet/>. Último acesso: Junho 2014.
- Sterbenza, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Scholler, M., and Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 58(1):1245–1265.
- Sun, J.-Z., Riekkki, J., Jurmu, M., and Sauvola, J. (2005). Adaptive connectivity management middleware for heterogeneous wireless networks. *IEEE Wireless Communications*, 12(6).
- Zhang, C., Song, Y., and Fang, Y. (2008). Modeling secure connectivity of self-organized wireless ad hoc networks. In *IEEE INFOCOM - The 27th Conference on Computer Communications*.
- Zhang, H. and Sundaram, S. (2012). Robustness of complex networks with implications for consensus and contagion. In *IEEE CDC*, páginas 3426–3432.