ROBSON GOMES DE MELO

GERENCIAMENTO DE CONECTIVIDADE SEGURA E CONTÍNUA EM REDES DE ACESSO HETEROGÊNEAS

Tese apresentada como requisito parcial à obtenção do grau de Doutor. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.

Orientador: Prof. Dr. Aldri Luiz dos Santos
Coorientadora: Profa. Dr. Michele Nogueira

CURITIBA

2014

Melo, Robson Gomes de
Gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas / Robson Gomes de Melo . – Curitiba, 2014
155 f. : il.; tabs.

Tese (doutorado) – Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Informática.
Orientador: Aldri Luiz dos Santos
Coorientadora: Michele Nogueira
Bibliografia: p.144-155

1. Redes de computadores - Administração. 2. Conectividade. 3. Mobilidade. I. Santos, Aldri Luiz dos. II. Nogueira, Michele. III. Título

CDD 004.6

AGRADECIMENTOS

Agradesço primeiramente a Deus por ter me dado força nessa luta árdua e diária. Agradeço minha familia pelo apoio incondicional. Agradesço os professores Aldri e Michele pela orientação e condução durante a pesquisa. Agradesço a todos os colegas do Laboratório NR2 que foram fundamental durante esse período do doutorado. Agradesço também a nova família construída em curitiba durante minha estadia nesta cidade.

RESUMO

A popularização dos dispositivos computacionais portáteis com suporte à conexão de diferentes tecnologias de comunicação e a proliferação das redes de acesso heterogêneas aumentam as demandas por conexão ubíqua. Logo, a conectividade em redes heterogêneas, definida como o acesso e a manutenção da conexão de forma contínua durante a transição por diferentes redes, é essencial para a convergência entre tecnologias. Contudo, a mobilidade, mesmo com manutenção de conectividade, expõe os usuários móveis a diversas vulnerabilidades de segurança. Ao transitar de uma rede para outra os usuários estão vulneráveis a ameaças inerentes às redes e acabam colocando seus dados e serviços em risco. Esta tese apresenta uma arquitetura para o gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas. A abordagem proposta evita a exposição dos usuários móveis às redes de acesso inseguras, assim como previne as redes de intervenção de usuários nômades mal intencionados, infectados ou propagadores de ameaças. A tese apresenta um estratégia de avaliação de segurança e conectividade da rede a partir de indicadores quantificáveis de suas condições. Esses indicadores auxiliam a tomada de decisão de acesso em ambientes de redes heterogêneas sobrepostas. Um esquema de decisão com ênfase nas condições de segurança da rede foi elaborado para escolha de melhor conexão e garantia de conectividade segura. A gerência autonômica do serviço de endereçamento dinâmico em redes heterogêneas também foi abordado como uma forma de garantia da continuidade da conectividade dos dispositivos em transito de uma rede para outra. Os resultados obtidos a partir da análise e avaliação do indicador das condições de segurança da rede, da estratégia de decisão de seleção de acesso e da gerência autonômica do endereçamento de dispositivos em trânsito, mostram a eficácia da arquitetura de gerenciamento de conectividade contínua e segura em redes de acesso heterogênea e abre possibilidades de pesquisas promissoras na área.

Palavras-chave: redes heterogêneas, gerenciamento, conectividade, mobilidade, segurança.

ABSTRACT

The popularity of portable computing devices with the support of different communication technologies, and the proliferation of heterogeneous access networks increase the demands for ubiquitous connection. Hence, connectivity in heterogeneous networks, defined as the continuous access operation and maintenance of the connection during the handoff through different networks, is essential to guarantee convergence among these networks. However, devices mobility, even when connectivity is kept, exposes users to different security vulnerabilities. When moving from one network to another users can experience threats inherent in networks and end up putting their data and services in risk. In this context, this thesis proposal presents an architecture for the management of secure connectivity and continuous heterogeneous access networks. The proposal avoids the exposure of mobile users to access insecure networks, and prevents access networks from intervention of nomads, malicious, infected or threats propagator users. The thesis presents a strategy for evaluation of safety and network connectivity from quantifiable indicators of their conditions. These indicators assist the decision making of overlapping heterogeneous access network environments. A decision scheme with emphasis on the security situation of network is designed to choose the best connection and ensuring secure connectivity. The autonomic management of dynamic addressing service in heterogeneous networks was also discussed as a way of ensuring the continuity of the connectivity of devices in transit from one network to another. The results obtained from the analysis and evaluation of the condition indicator of network security, the access selection decision and autonomic management of devices addressing transit, show the effectiveness of the management architecture of seamless and secure connectivity heterogeneous access networks and opens possibilities for promising research in the area.

Keywords: heterogeneous networks, management, connectivity, mobility, security.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

3G	Three Generation
3GPP	3rd Generation Partnership Project
4G	Fourth Generation
AAA	Authentication, Authorization and Accounting
ABC	Always Best Connected
AHP	Analytic Hierarchy Process
ANDSF	Access Network Discovery and Selection Function
APAV	Access Point Acceptance Value
BD_ADDR	Bluetooth Device Address
BER	Bit Error Rate
CA	Connectivity Antifragility
CIDR	Classless Inter-Domain Routing
CIR	Carrier-to-Interferences Ratio
DSL	Digital Subscriber Line
ELECTRE	Elimination and Choice Expressing Reality
GRA	Grey Relational Analysis
GSM	Groupe Special Mobile
HetNet	Heterogeneous Network
HIP	Host Identity Protocol
HMD	Heterogeneous Multi Domain
HostID	Host Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equip- ment Identity
IP	Internet Protocol
KPI	Key Performance Indicators
LTE	Long Term Evolution

LISTA DE ABREVIATURAS E SIGLAS

MAHO Mobile-Assisted HandOver

MANET Mobile Ad Hoc Networks

MCHO Mobile-Controlled HandOver

MDP Markov Decision Process

MEW Multiplicative Exponential Weighting Method

MICS Media Independent Command Services

MIES Media Independent Event Services

MIH Media independent handover

MIHF Media Independent Handover Function

MIIS Media Independent Information Services

MIP Moblie IP

NAHO Network-Assisted HandOver

NCHO Network-Controlled HandOver

NEMO Network Moblity

NetID Network Identification

NF Network Fragility

NIST National Institute of Standards and Technology

NR Network robustness

OLSR Optimized Link State Routing Protocol

PDA Personal Digital Assistant

PSV Access Point Satisfaction Value

QoE Quality of Experience

QoS Quality of Service

RSS Received Signal Strength

LISTA DE ABREVIATURAS E SIGLAS

SAE	System Architecture Evolution
SAP	Service Access Points
SAW	Simple Additive Weighting Method
SHAWK	Secure Heterogeneous Advanced Wireless networK
SIP	Session Initiation Protocol
SIP-NEMO	Session Initiation Protocol Network Moblity
SIR	Signal-to-Interferences Ratio
TOPSIS	Technique for Order Preference by Similarity to Ideal Solution
UHO	AUtonomic HandOver
VANET	Vehicular Ad hoc Network
WAN	Wide area network
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WMN	Wireless Mesh Networks
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

NOTAÇÃO

CA	índice de antfragilidade de conectividade da rede
C_i	Coeficiente de clusterização do vértice i
C_G	Um corte do grafo G
C_{Global}	Coeficiente de clusterização global
C_p	Conjunto de pesos de importância
Cr	Conjunto de redes
Cro	Conjunto de redes ordenadas
CV	vértices críticos
d_i	Grau do vértice i
$d(u, v)$	Distancia ente os vértices i, v
E_G	Conjunto de arestas do grafo G
e	Aresta grafo G
G	Grafo
G'	Grafo induzido de G
$mincut_v^u$	Corte mínimo entre os vértices u, v
NC_i	Normalização do critério i
NF	índice de fragilidade da rede
P_v^u	Um caminho no grafo G entre os vértices u, v
QoR	Qualidade da rede
u	Vértice grafo G
T_C	Árvore de corte
u	Vértice grafo G
v	Vértice grafo G
V_G	Conjunto de vértices do grafo G
X	Uma componente conexa
W_c	Conjunto de pesos
Y	Uma componente conexa

CAPÍTULO 1

INTRODUÇÃO

As redes de acesso evoluíram de modo significativo nos últimos anos em razão do surgimento de novos paradigmas e oportunidades de conexão. As infraestruturas de redes têm progredido da conexão fixa e cabeada para um modelo móvel estruturado e muitas vezes não estruturado e auto organizável. Influenciados por essas evoluções, os atuais modelos de redes de acesso exigem outros serviços, como o suporte a mobilidade com conectividade contínua e segura, para romper suas limitações. Soluções que atendam a essas questões motivam as pesquisas e o desenvolvimento do modelo de rede denominado *Redes do Futuro* [1].

O conceito *Redes do Futuro* compreende uma nova abordagem ainda sem consenso sobre uma definição formal de sua concepção [2]. A comunidade científica tem apresentado de forma consolidada propostas sobre questões e requisitos que esse novo modelo deve atender, de modo a oferecer serviços ubíquos aos usuários. Esses requisitos são decorrentes das experiências vivenciadas com os atuais modelos de redes de acesso, que passam por transformações para suportar as demandas cada vez mais exigentes dos usuários, tais como a qualidade de serviços, a garantia de mobilidade, segurança das informações.

As experiências vivenciadas nos últimos anos possibilitam a identificação de lacunas nas abordagens correntes e que devem ser atendidas nas concepções futuras. Embora as demandas por conectividade, roteamento, transporte e aplicação, sustentadas pelo ambiente tradicional sejam atendidas de certa forma, outros requisitos relevantes como o suporte a mobilidade com manutenção de conectividade e a segurança necessitam de estratégias mais completas. As pesquisas demonstram que a evolução nas redes de comunicação não é maior devido à herança deixada pelos ambientes tradicionais, classificados como engessados e individualizados [3, 4, 5]. Esses modelos não permitem o desenvolvimento de esquemas considerados triviais, quando comparados aos avanços de outras áreas.

Logo, as estratégias atualmente desenvolvidas atuam apenas como medidas paliativas para as questões emergenciais.

As redes heterogêneas estabelecem um novo ambiente de rede de acesso, integrando os serviços de dados, voz e recursos multimídias com qualidade, segurança, alta largura de banda e disponibilidade em um ambiente altamente convergente [6, 7]. As redes heterogêneas sem fio, (ou apenas "redes heterogêneas) compreendem vários tipos de redes utilizando diferentes e independentes tecnologias de comunicação sem fio. O objetivo dessas redes consiste em oferecer uma plataforma de conexão e transporte comum, reunindo variadas estruturas de redes com e sem fio em cenários de tecnologias integradas, diferentemente das atuais abordagens independentes de comunicação, como redes telefônica, Internet, rede de transmissão de TV, etc.

Essa plataforma de comunicação oferecerá serviços em ambientes de computação e conexão pervasiva, permitindo aos usuários diversos modos de acesso à informação. A popularização de dispositivos computacionais móveis como *smartphones, tablets* estimulam o modo de conectividade ubíqua dos usuários, oferecendo acesso a qualquer momento e em qualquer lugar. Esse cenário coloca em destaque o paradigma das conexões móveis no contexto das redes de acesso. As situações em que usuários utilizam celulares para verificar seus *e-mails*, redes sociais, realizar compras online durante o trânsito de uma área para outra corresponde um cenário gradativamente mais comum nos ambientes convergentes.

As conexões destes dispositivos móveis nas redes celulares e na Internet têm mudado o modo como essas redes passaram a ser estudadas e planejadas [8]. Algumas pesquisas apresentam resultados iniciais do processo de integração, demonstrando sistematicamente a tendência natural de convergência de diferentes tecnologias de comunicação [8, 9]. Cenários como esses são inerentes as redes heterogêneas que devem oferecer aos usuários a possibilidade de manutenção da conectividade de seus dispositivos, mesmo durante sua mobilidade por áreas geograficamente distintas.

Uma variada gama de serviços e aplicações se beneficiam com a infraestrutura oferecida pela convergência de redes heterogêneas. Os serviços da *TV Digital* por exemplo, poderão ser mais explorados pela integração das redes de transmissão de TV convencional com

a Internet, melhorando a qualidade deste serviço e alcançando regiões geograficamente distantes. A *Computação em Nuvem* é outro exemplo de serviço amplamente favorecido com a integração de diferentes redes de acesso. Com o aumento da disponibilidade de conexão por redes heterogêneas, os usuários poderão se manter mais tempo conectados usufruindo dos serviços em nuvem que demandam de alta conectividade. O *Big Data* que tem como base os *5V*, velocidade, volume, variedade, veracidade e valor [10], consiste de outro serviço também favorecido com a infraestrutura convergente das redes heterogêneas. Essas redes permitirão o acesso aos dados por diferentes redes de comunicação com maior velocidade e facilidade. Além desses exemplos de serviços, outros se beneficiarão pelo gerenciamento e manutenção da conectividade contínua e segura por redes de acesso heterogêneas.

A segurança ainda representa uma questão desafiadora, apesar dos benefícios proporcionados pela convergência das redes de acesso heterogêneas. A integração de diferentes tecnologias de comunicação também reúne ameaças e vulnerabilidades, que podem ser proliferadas pelos dispositivos móveis que transitam de uma rede para outra. Proteger as redes de diferentes tecnologias exige estratégias de segurança mais integradas e que não atuem de forma individualizada, como atualmente. As soluções específicas para cada tipo de rede deverão ser repensadas com uma visão mais ampla e até modularizada para serem eficazes neste novo ambiente dinâmico e convergente de redes heterogêneas.

1.1 Motivação

Os atuais modelos de redes, existentes de forma individualizada, têm sofrido impactos significativos no oferecimento de seus serviços que passaram a convergir [3]. Essa convergência é fundamental para garantir a integração de aplicações que atuam sob determinada tecnologia de acesso e demandam por modelos de comunicação mais interligados e altamente disponíveis. O processo de convergência requer suporte às características como conectividade, mobilidade, localização e acesso ubíquo dos dispositivos em transição, exigindo uma estrutura robusta e confiável das redes de acesso. Garantir a conectividade contínua e a segurança desses dispositivos e da rede ainda representam desafios significa-

tivos de pesquisa [11].

O suporte à mobilidade com conectividade contínua dos dispositivos móveis em redes heterogêneas permitirá a transição dos usuários por diferentes redes de acesso sem a interrupção das transmissões nas comunicações *fim-a-fim*. Um ambiente favorável para a criação deste modelo de conectividade requer esforços em vários níveis das camadas de protocolos de comunicação. Uma infraestrutura básica de conectividade deve ser garantida para sustentar todos os novos requisitos desse modelo de redes do futuro. Contudo, o uso de aplicações altamente interativas apoiadas por protocolos de transporte seguros, de baixa latência, sustentados por roteamento redundante e de alto desempenho na escolha das rotas, sem uma estrutura mínima de conexão de nada adianta.

Outra adversidade que surge com a proliferação das redes de acesso e o crescimento das áreas de cobertura de conectividade, trata-se das questões de segurança em redes heterogêneas. As vulnerabilidades e ataques restritos a cada modelo de comunicação passam a ser passíveis de execução em todo ambiente convergente, devido à integração de diferentes redes. Um ataque específico para uma dada rede pode ser realizado em outras redes. Além dos ataques, a proliferação de *worms, spywares, malwares, vírus, etc.* que contaminam os dispositivos móveis representa outro desafio. O perfil nômade dos usuários os expõem à contaminação em determinada rede de acesso, que pode ser propagada quando o mesmo dispositivo transitar por redes diferentes. Esses agravantes causam impacto tanto na segurança da rede quanto nos dispositivos em transição.

Neste aspecto, o gerenciamento da seleção adequada da rede de acesso representa um tópico de pesquisa a ser explorado. A escolha da melhor rede em ambientes com múltiplas redes sobrepostas garantirá aos usuários maiores níveis de qualidade de serviços, segurança e confiabilidade nas transmissões de seus dados. A seleção equivocada da rede de acesso poderá expor os usuários a diversos problemas como a falta de conectividade, comprometimento da integridade e privacidade de suas informações entre outros ataques [2]. Ao selecionar uma rede de acesso com objetivo de manter a conectividade, os usuários estão sujeitos a todas as vulnerabilidades inerentes àquela rede. Os atacantes podem induzir o acesso às redes boicotadas a fim de prejudicar as transmissões dos usuários e até

mesmo roubar informações confidenciais para futuras personificações. As redes de acesso também podem ser comprometidas com a ação dos usuários maliciosos que transitam de uma rede para outra. Ao oferecer acesso para os dispositivos móveis a rede se expõe às ações maliciosas e às vulnerabilidades pertinentes aos dispositivos, que podem prejudicar o oferecimento de seus serviços ou até mesmo indisponibilizá-los.

1.2 Descrição dos problemas

O caráter individual das soluções de segurança em redes de acesso, que necessitam de abordagens mais amplas e completas para atuarem de forma mais eficaz nas redes heterogêneas, destaca-se entre os problemas abordados nesta tese. Embora existam muitos mecanismos de segurança para as redes de acesso, eles usam diferentes abordagens separadamente, sem fornecer a integração e cooperação necessárias às redes heterogêneas. Além disso, essas soluções de segurança não levam em conta as particularidades da rede, tais como as suas necessidades e características.

A exposição e a insegurança dos usuários móveis durante a transição por redes de acesso heterogêneas consiste de outro agravante. O trânsito dos usuários por diferentes redes os expõem às vulnerabilidades do processo de transição, momento oportuno para os atacantes obterem informações confidenciais. A interrupção de conectividade causada pela troca de rede representa outro desafio a ser superado. A transição entre redes homogêneas ou heterogêneas pode causar falhas na conectividade dos usuários móveis que devem ser minimizadas, a fim de oferecer serviços de maior qualidade, disponibilidade e confiabilidade.

A dificuldade de supervisão e controle de modo autônomo e auto-organizável da seleção da rede de acesso adequada e segura para estabelecimento de conexão, e as vulnerabilidades e ataques que podem ser explorados pela seleção equivocada da rede são as maiores adversidades para a proteção dos dispositivos móveis e das redes de acesso. Os atacantes podem induzir os usuários móveis a se conectarem em determinadas redes com a premissa de oferecer alta conectividade e se valerem de inúmeros artifícios para sabotá-los. As redes de acesso que oferecem seus serviços a qualquer dispositivo móvel também estão

sujeitas a ataques e a propagação de *worms, spywares, malwares, vírus* pela rede e isso pode comprometer o oferecimento dos seus serviços ou indisponibilizá-los. Deste modo, é fundamental um mecanismo de gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas, que possa realizar uma análise mútua das condições da rede e dos dispositivos em transição e selecionar as redes de acesso mais adequadas.

1.3 Objetivo

O objetivo desta tese consiste em tratar as vulnerabilidades e indisponibilidade de conectividade de dispositivos móveis em transição por redes de acesso heterogêneas, de modo a garantir conexões seguras e contínuas. Para isso a tese detalha um arcabouço para o gerenciamento da conectividade integrada e adaptativa de modo autonômico, que permite acesso seguro as redes heterogêneas com suporte a mobilidade com conectividade contínua. Esse arcabouço garante a manutenção da segurança e da qualidade da conectividade e seus serviços durante a mobilidade por ambientes de redes heterogêneas. O arcabouço utiliza informações de contexto a fim de realizar uma avaliação mútua das condições da rede e dos dispositivos móveis em transição. A análise realizada tem como base os valores de *fragilidade, robustez e antifragilidade* da conectividade como indicadores de segurança da rede e dos dispositivos candidatos à conexão, garantindo um acesso e migração seguro dos dispositivos móveis em trânsito por redes de acesso heterogêneas.

Diferente das concepções tradicionais, que utilizam somente critérios de desempenho como forma de avaliação, a estratégia proposta consiste em definir e utilizar métricas de segurança, de forma dinâmica, para estimar as condições da rede e dos dispositivos móveis. O uso de coeficientes como *fragilidade, robustez, antifragilidade,* entre outros, permitem aos dispositivos a tomada de decisão de conexão por redes heterogêneas mais robustas, seguras e confiáveis. De mesmo modo, os indicadores dos dispositivos também possibilitam às redes conceder ou não o acesso e recursos à determinados dispositivos em transição, mantendo alto seus níveis de proteção e segurança.

1.4 Contribuições

As contribuições da tese são sumarizadas a seguir:

- **Um estudo das iniciativas relacionadas à seleção da melhor rede de acesso para dispositivos móveis em transição por redes heterogêneas**. O estudo fornece uma visão geral dos conceitos de transição de acesso em redes heterogêneas com manutenção de conectividade. Estratégias de seleção de melhor rede e abordagens de segurança são discutidas. Os resultados permitiram identificar as questões em aberto e a oportunidade de desenvolvimento de um arcabouço de gerenciamento de conectividade segura e contínua para redes heterogêneas.

- **Uma arquitetura para o gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas**. Avaliando as iniciativas de seleção de melhor rede de acesso, manutenção de conectividade e segurança para diferentes tipos de redes foi projetada uma arquitetura de gerenciamento de conectividade em redes heterogêneas. Essa arquitetura possui planos de atuação em *Segurança, Conectividade e Gerência*, para garantir a decisão e seleção adequada da melhor rede de acesso.

- **Indicadores de resiliência de conectividade de redes de acesso heterogêneas**. Os índices de segurança que indicam as condições das diferentes redes de acesso detectadas pelos dispositivos em transição apontam a melhor rede disponível. Diferentemente das abordagens tradicionais, que se baseiam apenas em critérios e métricas de desempenho, esse serviço também utiliza como base as condições relacionadas a segurança para indicar a melhor rede de acesso disponível.

- **Uma estratégia de decisão sobre o acesso seguro e confiável em redes heterogêneas**. O serviço de tomada de decisão utiliza os valores dos indicadores das condições da rede, combinado com diferentes critérios e métricas utilizadas nas abordagens tradicionais, para a realização de uma decisão multicritério de melhor rede, que corresponde à rede mais segura. O serviço de decisão analisa, calcula e

classifica as melhores redes para uma seleção e transição segura de conexão contínua por redes heterogêneas sobrepostas.

- **Gerência autonômica do serviço de endereçamento em redes heterogêneas**. Esse serviço controla a negociação e troca de endereços dos dispositivos em transição por redes heterogêneas, para garantir a manutenção da conectividade e continuidade dos fluxos de dados nas comunicações fim-a-fim. O serviço de gerência utiliza princípios da computação autonômica para reduzir a necessidade de intervenção humana no gerenciamento da conectividade da rede e evitar o surgimento de vulnerabilidades de segurança.

1.5 Organização da Tese

Esta tese está organizada em oito capítulos. O Capítulo 2 apresenta os conceitos e fundamentos relacionados à tese, descrevendo as características gerais das redes heterogêneas, os aspectos relacionados à mobilidade com manutenção da conectividade, e a segurança. O Capitulo 3 discute o estado da arte do processo de seleção de rede de acesso e as estratégias de segurança existentes na literatura. O Capítulo 4 detalha uma arquitetura de gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas, descrevendo seus objetivos e os requisitos levantados durante o estudo bibliográfico. O Capítulo 5 descreve um indicador de resiliência de conectividade em redes heterogêneas, utilizado para calcular as condições das redes de acesso e axilar o processo de escolha de melhor rede. O Capítulo 6 apresenta um serviço de tomada de decisão de melhor acesso em redes heterogêneas, que escolhe a rede mais adequada para a conexão a partir de um conjunto de redes detectadas pelo dispositivo móvel. O Capítulo 7 detalha a gerência do serviço de endereçamento em redes heterogêneas, desenvolvido a partir de princípios autonômicos para evitar à necessidade de intervenção humana no processo de gerência dos serviços relacionados a conectividade em redes heterogêneas. Por fim, o Capítulo 8 conclui a tese e aponta possibilidades de trabalhos futuros.

CAPÍTULO 2

REDES HETEROGÊNEAS, MOBILIDADE E SEGURANÇA

Esse capítulo apresenta os fundamentos relacionados ao tema de pesquisa desta tese. A Seção 2.1 aborda os conceitos e definições sobre redes heterogêneas. A Seção 2.2 apresenta os modelos de mobilidade em rede de acesso sem fio. A Seção 2.3 descreve os princípios de mobilidade com manutenção de conectividade. A Seção 2.4 define os aspectos de segurança e vulnerabilidades na transição em redes heterogêneas, e a Seção 2.5 apresenta um resumo do capítulo.

2.1 Redes heterogêneas

O recente desenvolvimento das novas tecnologias de transmissões de dados têm revolucionado o modo das comunicações. Várias tecnologias estão evoluindo simultaneamente no sentido de oferecer aos usuários serviços de alta qualidade e acesso às redes de banda larga. As redes de transmissão sem fio desempenham um papel importante neste processo. As redes sem fio de longa distância *(WWAN)* e as redes de áreas metropolitanas *(WMAN)* estão evoluindo para oferecer ampla cobertura e boa capacidade de mobilidade. Por outro lado, uma série de padrões como *IEEE 802.11a, b, g, n* e recentemente o *ac* foram estabelecidos para as redes sem fio locais *(WLAN)* com o objetivo de oferecer alta velocidade e baixo custo. As redes sem fio pessoais *(WPAN)* evoluem para proporcionar a transmissão de dados de pequeno alcance entre os dispositivos e seus periféricos [12]. Contudo, o estabelecimento de conexão e a permanência de acesso em um único tipo de rede não é suficiente para atender aos novos requisitos dos usuários e as suas aplicações, como a conectividade contínua e segura durante a mobilidade.

As redes heterogêneas sem fio, ou apenas redes heterogêneas, compreendem a integração de vários tipos de redes utilizando diferentes e independentes tecnologias de acesso sem fio. As redes de telefonia celular, as rede de transmissão de TV e a Internet re-

presentam redes heterogêneas que oferecem serviços específicos sob tecnologias distintas. As redes de comunicação de dados *WWAN* e *WMAN* são consideradas heterogêneas por utilizarem diversas tecnologias de redes de acesso, como *3G, 4G/LTE, WiMax*, etc. Por sua vez, a heterogeneidade das *WLAN* estão nos diferentes padrões de comunicação, tais como os *IEEE 802.11a, b, g* e *n* [13].

Deste modo, é possível definir redes heterogêneas como redes de comunicação de dados de diferentes tecnologias, padrões, áreas de cobertura ou infraestrutura de comunicação. Uma rede heterogênea suporta a interoperabilidade entre as redes e tecnologias, sendo capaz de prover serviços através de qualquer tipo de rede mantendo sua disponibilidade de forma transparente para o usuário final [14, 15, 16]. Em geral, mudanças no tipo de rede ou de tecnologia são provenientes da mobilidade dos usuários finais e seus dispositivos ou pela degradação do sinal recebido na área de cobertura, a qual altera as condições da rede e dos serviços. Mudanças de tecnologia de rede de acesso também podem ocorrer em redes fixas, tais como na infraestrutura das redes em malha *(MESH)* e nas redes veiculares *(VANETs)* que sofrem constantemente com mudanças em suas topologias físicas.

A Figura 2.1 ilustra um conjunto de redes heterogêneas formadas por diferentes tecnologias de comunicação. Na ilustração, as redes coexistem na mesma área de cobertura mas com tecnologias diferentes operando com frequências, padrões e protocolos distintos.

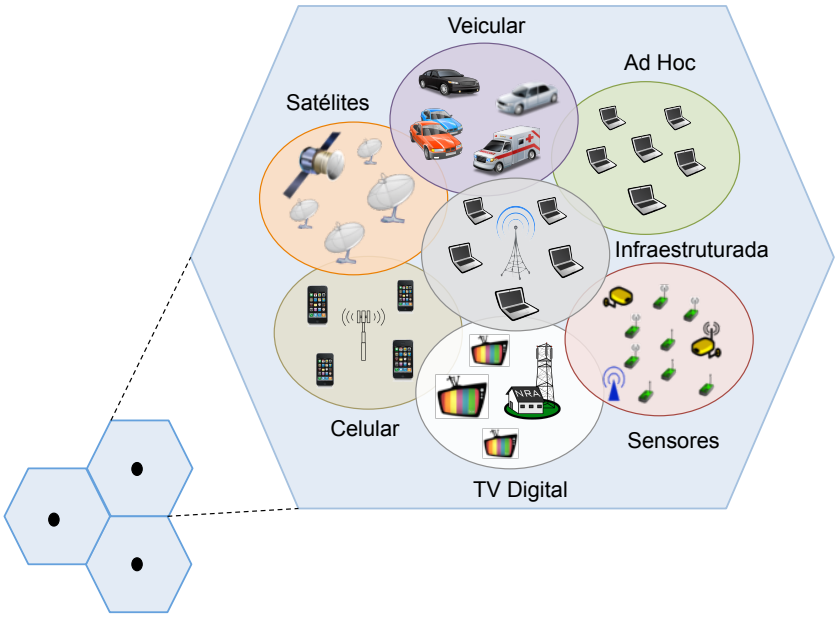


Figura 2.1: Redes heterogenêas

2.1.1 HetNet

A *HetNet (Heterogeneous Networks)*, consiste de outra denominação de redes heterogêneas, em que o foco são as diferentes tecnologias de áreas de cobertura. Essas áreas variam de ambientes externos, prédio comercial, residências até áreas subterrâneas [17, 18]. A *HetNet* é uma rede composta por pontos de infraestrutura (estações de acesso) com várias tecnologias de comunicação sem fio, cada um desses pontos possui diferentes capacidades, restrições e funcionalidades operacionais [19, 20]. Estas estações de acesso sobrepostas de baixa potência podem coexistir na mesma área geográfica, compartilhando o mesmo espectro de frequência [18]. As *HetNets* são formadas por áreas de cobertura com diferentes características como descritas por Lopez [18].

- **Macro-células** consiste de uma ampla área de cobertura de transmissão, tipicamente na ordem de alguns quilômetros (aproximadamente 2 a 6 Km).

- **Micro-células** oferecem o mesmo tipo de acesso das *macro-células* porém com coberturas inferiores, em torno de 1 a 2 km.

- **Pico-células** são torres de operadora de baixo consumo de energia instaladas com acesso à recursos das *macro-células*. São geralmente utilizadas de forma centralizada, servindo algumas dezenas de usuários. As *pico-células* são utilizadas principalmente para preenchimento e cobertura exterior ou interior como por exemplo em edifícios de escritórios.

- **Femto-células** são redes de baixo custo, baixo consumo de energia implantadas pelo usuário como pontos de acesso. Elas transferem o tráfego de dados através de uma ligação de banda larga *Backhaul* [21, 22] (normalmente *DSL - digital subscriber line*, cabo ou fibra), e servem uma de dúzia usuários ativos em residências ou empresas. Tipicamente, as *femto-células* operam em grupo de assinante aberto ou de acesso restrito.

- **Relays** consistem de pontos de acesso, cuja finalidade consiste em encaminhar os dados a partir das macro-células aos usuários e vice-versa. Eles são posicionados

de modo a aumentar a intensidade do sinal e desta forma melhorar a recepção nas áreas de fraca cobertura nas redes existentes. Uma descrição mais detalhada sobre a composição, funcionamento e características das *HetNets* é encontrada em [23, 13, 24].

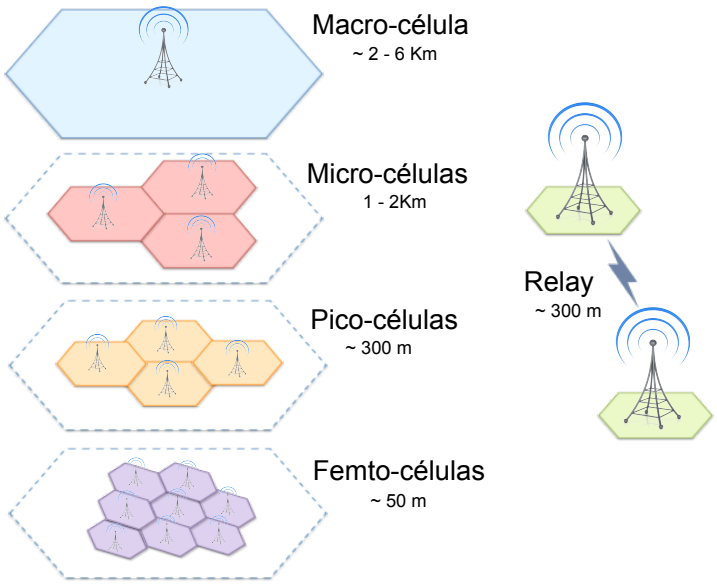


Figura 2.2: HetNet *(Heterogeneous networks)*

A Figura 2.2 ilustra as diferentes áreas de cobertura das *HetNet*, bem como seus respectivos alcances de transmissões e recepções. As Macro-células possuem uma área de alcance de poucos quilômetros (aproximadamente cinco km). As Micro-células de um a dois km de área de cobertura, as Pico-células de aproximadamente 300 metros, as Femto-células de aproximadamente 50 metros e as redes Ralay com aproximadamente 300 metros de alcance, semelhante às Pico-células.

2.1.2 Redes de acesso heterogêneas

Além das definições de redes de acesso heterogêneas mencionadas anteriormente, outras formas de heterogeneidade de rede são encontradas na literatura, como as redes de aplicações, de sistemas operacionais e de dispositivos heterogêneos que compõem os elementos e agentes da rede. Contudo, as redes de acesso tem sido o grande foco de pesquisas sobre heterogeneidade. Os trabalhos recentes na área têm investigado principalmente técnicas de sobreposição de cobertura para o descarregamento de trafego de dados para as

células menores [18, 24]. Embora os ganhos com esta abordagem são promissores, eles ainda representam apenas um ponto de partida. A previsão é de que as redes heterogêneas desempenharão um papel central na evolução da redes de acesso de banda larga móvel sem fio, e servirão como uma plataforma facilitadora para inovações tecnológicas disruptivas [16].

Impulsionados pelo uso crescente de dispositivos portáteis, os quais aumentam as requisições pelos serviços de rede, a indústria e a academia têm investido no desenvolvimento de redes de acesso heterogêneas sem fio, por serem extremamente flexíveis e proporcionar conectividade em diferentes tecnologias de comunicação [25, 26, 27]. Essas redes operam de forma complementar para suportar as necessidades dos usuários finais, diminuir os problemas causados pelo crescimento da infraestrutura de rede e oferecer um ambiente de computação ubíquo. Deste modo, essas redes possuem uma ampla variedade de aplicações, tais como as redes domésticas, militares, de emergência [26]. Assim, o emprego de redes heterogêneas nas mais variadas áreas de comunicação é apropriado devido ao suporte a uma diversidade de tecnologias de transmissão de dados.

A Figura 2.3 apresenta algumas possibilidades de utilização de redes de acesso heterogêneas para estabelecer conexões. As redes de acesso utilizam diferentes tecnologias de transmissão para oferecer serviços e recursos a seus usuários, como as redes celulares, que evoluíram suas tecnologias de primeira à quinta geração para garantir melhor QoS.

Garantir a conexão, a identificação e a segurança nestas redes e em seus dispositivos ainda representam desafios [11]. O processo de convergência requer suporte às características de conectividade, mobilidade, localização, acesso ubíquo e segurança dos elementos em transição de uma rede para outra, exigindo uma estrutura robusta das redes de acesso. As transições entre diferentes redes são caracterizadas pela conexão na rede de destino e desconexão da rede de origem dos dispositivos em trânsito de modo que a troca de mensagens seja realizada.

Os desafios das redes de acesso passam pela convergência de diferentes tecnologias de comunicação em uma única rede onipresente. Para alcançar a agregação de enlaces de redes sem fio heterogêneas, três grandes etapas devem ser abordadas: *i)* heterogeneidade

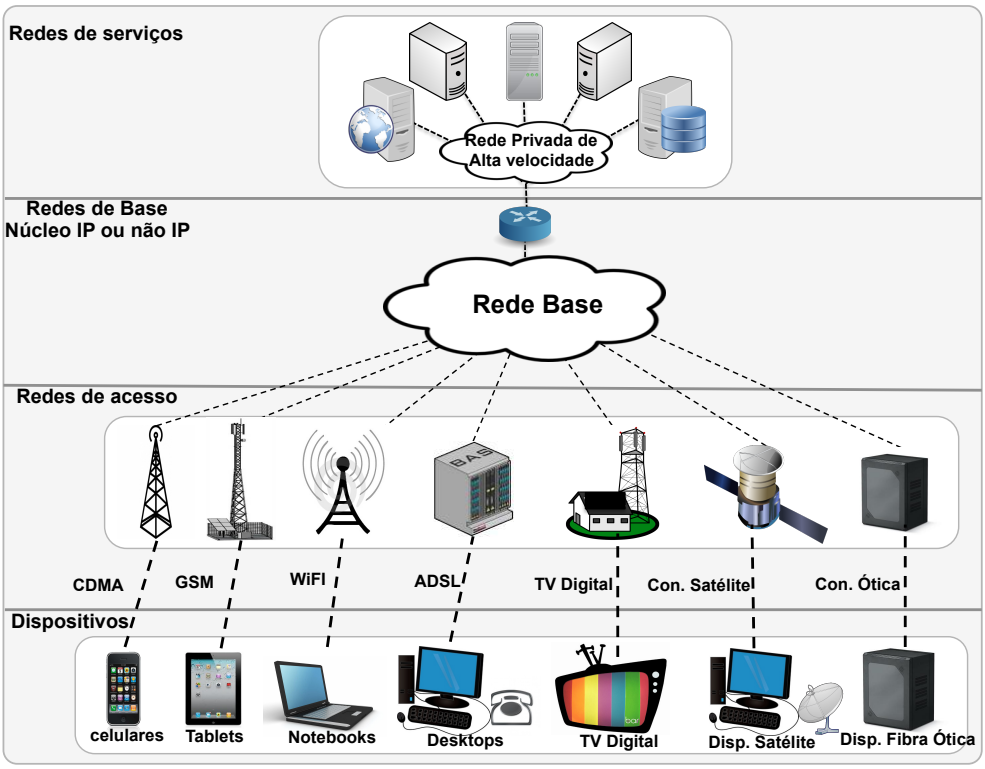


Figura 2.3: Redes de acesso heterogêneas

na interface do enlace - os usuários finais precisam acessar diferentes tipos de ligações; *ii)* interrupção do enlace de comunicação - devido à mobilidade dos usuários finais, sinais de rádios são instáveis e a cobertura é limitada; e *iii)* vulnerabilidade do enlace de acesso - as ligações móveis são altamente vulneráveis a ataques e incidentes de segurança [16].

2.2 Modelos de mobilidade

O suporte à mobilidade é um dos principais requisitos que impulsiona o desenvolvimento das redes do futuro. A proliferação dos dispositivos computacionais com capacidade de conexão às redes sem fio e a evolução das redes de acesso, proporcionando conectividade à internet, fazem aumentar o desejo dos usuários por conectividade com suporte à mobilidade. O anseio pelo acesso à informação em qualquer lugar e a qualquer momento torna a conectividade com suporte à mobilidade imprescindível na vida das pessoas. Contudo, as iniciativas existentes para o gerenciamento de mobilidade, principalmente em redes heterogêneas ainda não são eficazes a ponto de estarem consolidadas como soluções concretas.

A mobilidade consiste na capacidade e na vontade de se mover mudando do local em que se esteja [28]. Essa mudança pode ser medida por associações com base em uma escala que varia de Forte para Fraco. As associações "Fortes" acontecem quando os padrões de ligações são estáticos e fixos, e as associações "Fracas" quando as ligações/conexões são dinâmicas e variáveis [28]. Em razão dessas características o processo de mobilidade para as redes heterogêneas deve suportar três modos de operação: mobilidade de aplicações, mobilidade de rede e mobilidade dos dispositivos.

2.2.1 Migração de aplicação

A mobilidade de aplicações significa migrar programas em tempo real de um dispositivo para outro, que possua recursos computacionais iguais ou superiores [28, 29] . A partir do aumento do poder computacional dos dispositivos e das otimizações das tecnologias de programação tornou-se possível a programas antes considerados pesados serem executados com facilidades em dispositivos portáteis. Os navegadores de internet que antes eram restritos aos *desktops*, mas que atualmente estão presentes em quase todos *smartphones* são exemplos destas aplicações. Com o suporte à mobilidade de aplicações, casos como o de *Bob* que está assistindo um filme em seu *desktop* em casa, mas quando percebe que está na hora de ir para seu escritório trabalhar e mesmo assim deseja continuar assistindo o filme, seriam suportados. Nesta situação, como ilustrado na Figura 2.4, o *player* de vídeo poderia ser migrado para o *smartphone* ou outro dispositivo móvel e *Bob* permaneceria assistindo o filme do ponto em que parou em seu dispositivo portátil.

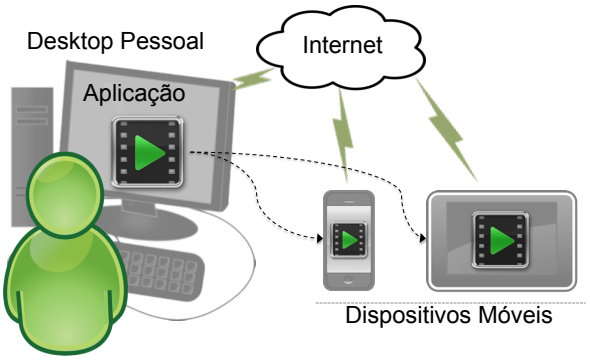


Figura 2.4: Mobilidade de aplicação

Entre as estratégias de mobilidade de aplicação mais utilizadas estão os *desktops* remotos, sistemas de máquinas virtuais ou estação de trabalho virtual, abordagens com base em *middlewares e cloud services*. Entretanto, existem inúmeros desafios nesta área, principalmente relacionados a inteligência envolvida na mobilidade da aplicação e questões de segurança e privacidade [28, 30].

2.2.2 Mobilidade de rede

A mobilidade de rede implica na capacidade da rede toda se mover sem prejudicar a conexão entre seus dispositivos *(nós)* [31]. Neste cenário, a mobilidade está presente na infraestrutura e na topologia de comunicação. As redes de comunicação sem fio possuem duas formas de organização de sua topologia de comunicação, o modo infraestruturado com um ponto centralizador da comunicação, e o modo *ad hoc* sem um ponto centralizador e auto organizável. A mobilidade pode acontecer nessas duas formas de topologia.

As redes Intraveiculares são exemplos de mobilidade da rede em ambientes infraestruturados. As redes intraveiculares, normalmente formadas por um ponto de acesso oferecendo conexão para outros dispositivos no interior dos veículos como ônibus, trens, aviões, etc. que se movimentam em um trajeto específico. Dentro desses veículos o modo de comunicação é infraestruturado, e assim, o ponto de acesso se torna um *gateway* da rede intraveicular para as redes externas como a Internet. Neste aspecto, à medida que o veículo se movimenta o ponto de acesso passa a se conectar em outras diferentes redes pelo caminho, garantindo a conexão dos dispositivos no interior do veículo com as redes externas. Com a movimentação do veículo a rede toda em seu interior também está em movimento.

Na ilustração da Figura 2.5 o *Ônibus B* possui uma rede intraveicular formada pelos seus passageiros, contudo, o veículo se conecta com a internet por intermédio de um *ponto de acesso* no modo infraestruturado e a medida que se distancia da área de cobertura do ponto de acesso, passa a se conectar com os outro veículos (*Automóvel C e Ônibus A*) durante seu trajeto no modo *ad hoc* para continuar a oferecer seus serviços e garantir a conectividade.

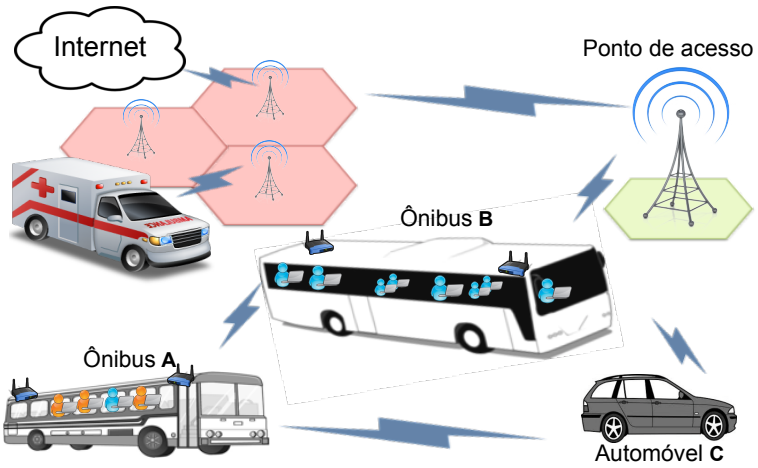


Figura 2.5: Mobilidade de rede

Diferentemente das redes infraestruturadas, a mobilidade da rede é uma característica inerente às redes *ad hoc* sem fio, como as *MANETs (Mobile Ad Hoc Networks)* e as *VANETs*. Essas redes não possuem uma infraestrutura física e são formadas por topologia dinâmica de comunicação. Como não há uma infraestrutura pré-definida, cada nó atua como roteador, encaminhando os pacotes do remetente ao destinatário através de nós intermediários. Deste modo, a rede toda pode se mover dentro dos limites de cobertura, que os pacotes de dados serão entregues ao seu destino.

2.2.3 Mobilidade de dispositivo

A mobilidade do nó consiste na mudança de ponto de conexão ao longo do tempo. O nó móvel permanece conectado quando se movimenta dentro da área de cobertura da rede ou se desvincula dela e se conecta em outra rede a medida em que se movimenta durante um trajeto. Esse cenário é cada vez mais comum com a proliferação dos novos dispositivos computacionais com suporte às múltiplas interfaces de comunicação *(multihoming)*.

A evolução dos dispositivos computacionais portáteis como os *PDAs (Personal digital assistant), Notebooks, Tablets, Smartphones*, etc. popularizou a mobilidade do nó na rede. Os usuários portadores destes dispositivos transitam livremente pela área de cobertura da rede ou até mesmo estabelecendo novas conexões com outras redes a todo momento. Os dispositivos móveis passam a suportar *multihoming* para o estabelecimento de conexão

sem fio em diferentes tipos de redes, e a sua autonomia energética está cada vez maior. Essas características favorecem um ambiente de mobilidade irrestrita de seus usuários não limitada a baixa mobilidade mas com suporte às velocidades mais elevadas como no caso das *VANETs* [32]. A Figura 2.6 ilustra um cenário de mobilidade de dispositivos de uma rede para outra ao longo de um trajeto.

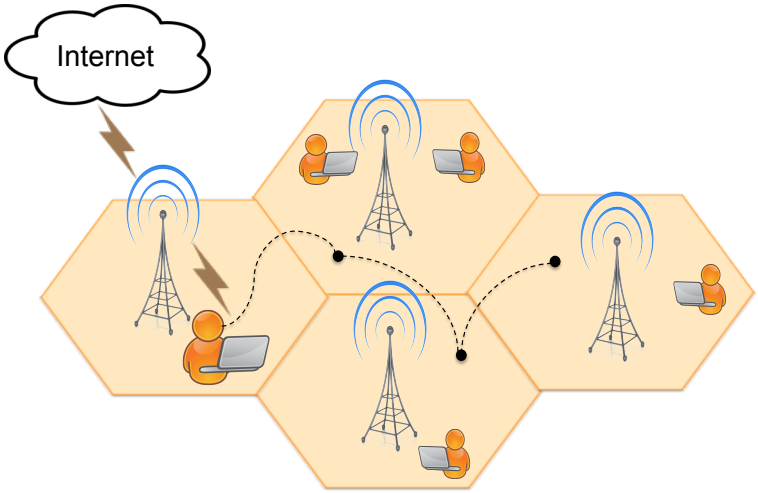


Figura 2.6: Mobilidade irrestrita de dispositivos

2.3 Mobilidade em redes de acesso heterogêneas

Muitos trabalhos já foram realizados para apoiar à mobilidade em ambiente de rede sem fio, contudo, ainda não há uma estrutura sistemática para identificar e resolver os problemas no desenvolvimento eficaz e eficiente de suporte à mobilidade no contexto de redes sem fio heterogêneas [30]. Inúmeras propostas foram apresentadas pela comunidade científica tentando encontrar a solução mais adequada. As estratégias de suporte à mobilidade em redes heterogêneas são as mais variadas, abordando a mobilidade da aplicação, da rede e do dispositivo.

O trabalho de Ping [33] utiliza uma estratégia de mobilidade em redes heterogêneas baseada em política. Os autores argumentam que a sobrecarga do endereço *IP*, que representa a identidade do nó e o endereço de rede ao mesmo tempo, é um grande obstáculo para a mobilidade. Deste modo, eles propõem o uso dos os protocolos *MIP (Moblie IP)* e *HIP (Host Identity Protocol)* como formas de suporte à mobilidade dos nós. A solução

é construída por um esquema de identificador lógico hierárquico que define um perfil dos usuários formado por duas partes: *i)* parte formada por informações invariantes como *Id* do usuário com informações da rede, subrede e do nó, informações de autenticação, informações de contatos etc. *ii)* parte formada por informações variantes como informações de localização e status corrente. O resultado é uma extensão do *HMD (Heterogeneous Multi Domain)* que controla o processo de mobilidade com base nas políticas de cada domínio de rede.

Kumudu *et al.* [31] apresentam uma proposta de mobilidade em grupo para redes heterogêneas. O grupo forma uma rede móvel composta por dispositivos computacionais portáteis no interior de veículos de transporte público. Os autores propõem a adaptação e a utilização do protocolo *NEMO (Network Moblity)* de redes homogêneas como forma de suporte à mobilidade de grupos entre redes heterogêneas. A principal estratégia é melhorar o *SIP-NEMO (Session Initiation Protocol - Network Moblity)* como mecanismo de gerenciamento de mobilidade. Segundo os autores, a introdução de *SIP-NEMO* para facilitar o suporte à mobilidade em grupo baseada em sessão e optimização de rotas, introduz uma redução significativa na sobrecarga de sinalização, daí um aumento substancial da QoS para os usuários finais.

A estratégia em [34] prevê o uso de *multihoming* em dispositivos móveis como forma de suporte à mobilidade em redes heterogêneas. Neste trabalho os autores propõem o uso do protocolo *SIP (Session Initiation Protocol)* com as funções *pre-call* e *mid-call* para o gerenciamento da mobilidade. Um usuário de um cliente SIP recebe um identificador exclusivo que é registrado no servidor *SIP*, juntamente com seus múltiplos endereços de rede *(IPs)*. Assim, o *SIP* associa os identificadores aos endereços para facilitar a localização do nó nas diferentes redes. A função *pre-call* preserva a acessibilidade de um dispositivo para as solicitações de chamadas recebidas quando ele se move entre as redes *IP*. A *mid-call* mantém sessões em curso quando um dispositivo muda de endereço. Deste modo, o nó abre uma nova sessão com seu novo endereço *IP* e finaliza a seção anterior. Os resultados mostram que a estratégia reduz a perda de pacotes do nó em transição.

Seguindo a estratégia de dispositivos *multihoming*, Shin [35] apresenta uma solução

para a mobilidade em redes heterogêneas com base na seleção de múltiplos caminhos. Nesta abordagem o dispositivo móvel mantém a conexão com várias redes pelas suas diferentes interfaces e a medida em que ele avalia os diferentes caminhos vai se desconectando das redes com os piores caminhos.

O trabalho de Yannan [36] apresenta uma solução com base em mecanismo de predição de mobilidade. A predição de mobilidade desempenha um papel importante em rede de acesso heterogênea, pois pode prestar o serviço de gerenciamento de mobilidade, controle e admissão de chamadas, reserva de recursos, entre outros. O trabalho trata da questão de como prever a localização de um usuário móvel em redes heterogêneas. Como solução os autores propõem o *MPMboLC*, um mecanismo de predição de mobilidade baseado em logística de célula. Os resultados alcançados mostram que a predição com base em células logísticas são precisas e auxiliaram na entrega dos dados para os usuários móveis em trânsito.

Um estudo minucioso sobre o processo de mobilidade e os métodos de integração em redes heterogêneas foi apresentado por Sivakami [37]. O trabalho discute as soluções de gerenciamento de mobilidade com base em: *Micromobilidade*, processo pelo qual os nós móveis mudam entre subredes de mesmo domínio, normalmente para redução de carga; e *Macromobilidade*, quando os nós se movem por redes de diferentes domínios, normalmente em busca de QoS. O trabalho também apresenta uma taxonomia para a classificação das soluções de gerenciamento de mobilidade, além de uma sucinta comparação entre o protocolos encontrados na literatura.

O número de trabalhos que abordam assuntos relacionados à mobilidade é significativo e vem crescendo nos últimos anos. A mobilidade dos usuários em redes heterogêneas é assistida pelas técnicas de transições de conexões de uma rede para outra. Contudo, a mudança de conexão de um ponto da rede para outro, ou de uma rede para outra, ainda apresenta desafios, principalmente quando a manutenção da conectividade é uma exigência.

2.3.1 Manutenção de conectividade

O principal objetivo dos usuários móveis durante um trajeto com redes de acesso disponíveis é a manutenção da conectividade. A mobilidade sem a conectividade contínua, provendo o acesso a informação de modo oportuno, não é tolerada pelas aplicações, que cada vez mais necessitam de conexão para seu funcionamento. Os recentes serviços e aplicações, como é o caso dos serviços em nuvem, estão mais dependentes da internet. Deste modo, a demanda dos usuários pela conectividade contínua durante a mobilidade é muito exigida nos cenários atuais.

Trabalhos como [38, 39] têm apresentado estratégias para garantir a conectividade aos usuários. Estes trabalhos apresentam a ideia de região de conectividade para os usuários que se movimentam dentro de uma área restrita de mobilidade. Assim, se o dispositivo estiver fora de uma área definida ele estará desconexo, mesmo existindo outras redes de acesso na região. Diante da proliferação das redes de acesso de igual ou diferentes tecnologias de comunicação proporcionando uma ampla área de cobertura nos ambientes urbanos, assim como a evolução dos dispositivos móveis com o suporte de conexão a diversificadas redes de transmissão, soluções de conectividade com suporte à mobilidade restrita do usuários não correspondem às demandas mais urgentes.

O desejo pelo suporte à mobilidade com manutenção de conectividade não se restringe a apenas uma área pré-definida de cobertura. Os usuários portadores de dispositivos móveis anseiam por conectividade irrestrita de mobilidade. As demandas são por acesso em toda a região urbana, intermunicipal e até um possível acesso global, tendo em vista a evolução das redes de acesso. Neste tipo de ambiente, o gerenciamento da mobilidade é a questão essencial que suporta o *roaming* de usuários de uma rede para outra. O processo responsável por sustentar a transição dos dispositivos móveis de uma rede para outra garantindo a mobilidade irrestrita com manutenção da conectividade é o *handoff* [40, 41].

2.3.2 *Handoff*

O *Handoff* (transição) também conhecido como *Handover* é o processo pelo qual o nó se desconecta de um ponto e se conecta em outro durante sua mobilidade [41]. É por meio

do processo de *handoff* que as transições de uma rede para outra são executadas pelos dispositivos móveis. De modo geral, cada dispositivo móvel permanece conectado a um ponto da rede também conhecido como estação base. A área de cobertura de cada estação de base é identificada como célula, a dimensão e as características da célula dependem do tipo da rede. A transição de uma célula para outra com a manutenção da conectividade implica na finalidade do *handoff*.

Tipos e classificação de *handoff*

Segundo [40, 42], o *handoff* pode ser classificado por vários fatores, tais como o tipo de rede, frequências de propagação envolvidas, número de conexões ativas, tipo de tráfego suportado. O modo mais comum de classificação do *handoff* é pelo tipo de rede, que pode ser caracterizado como *handoff horizontal* ou *vertical*.

- ***Handoff Horizontal*** consiste no processo de transição de um dispositivo móvel entre pontos de acesso de redes com mesma tecnologia de transmissão. Por exemplo, um dispositivo móvel transitando com conectividade entre pontos de acesso de uma rede *Wifi 802.11n*. O *handoff horizontal* permite a transição de conexão por redes de acesso homogêneas.

- ***Handoff Vertical*** implica no processo de transição do dispositivo móvel entre pontos de acesso de redes com diferentes tecnologias de comunicação. Por exemplo, a transição de conexão a partir de uma estação de base *Wifi 802.11n* para uma rede celular sobreposta é considerada um processo de *handoff vertical*. O *handoff vertical* permite a transição de conexão por redes de acesso heterogêneas.

Existem dois tipos de handoffs verticais: para cima *(upward)* e para baixo *(downward)*. Um *handoff vertical* para cima compreende a mudança para uma rede com um tamanho maior de células e menor largura de banda, tais como as *WANs (redes celulares)*, e um *handoff vertical* para baixo consiste na mudança para uma rede com célula de tamanho menor mas com largura de banda maior, como as *WLANs (redes 802.11)*.

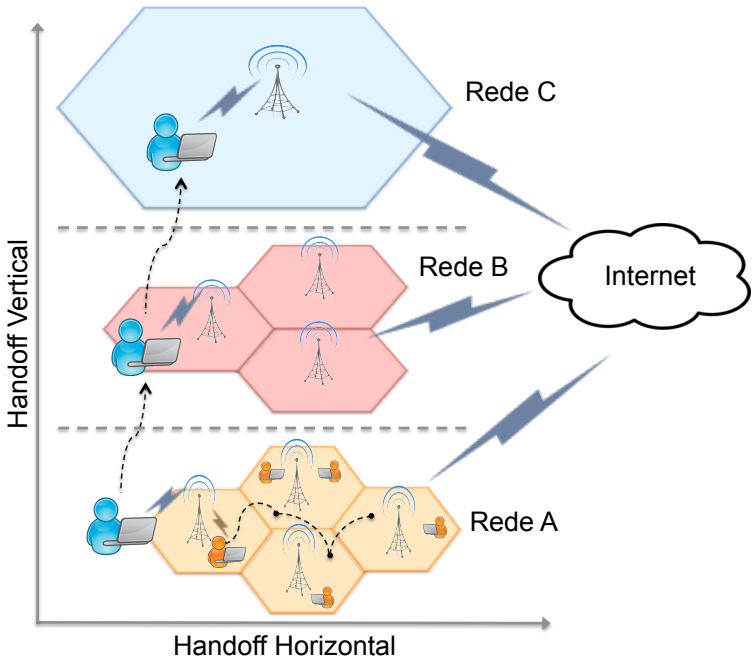


Figura 2.7: *Handoff* vertical e horizontal

Outra classificação do *handoff* trata da conectividade envolvida na transição. Neste caso o modo consiste de *Hard e Soft Handoff*.

- ***Hard handoff*** acontece quando o nó móvel finaliza uma conexão com a estação base de origem para posteriormente estabelecer um nova conexão com a estação base de destino. Nesse processo a conectividade é afetada no momento da transição de uma célula para outra, fazendo com que o nó fique sem conexão por alguns instantes.

- ***Soft handoff*** mantém a conexão com a estação base de origem enquanto a nova conexão com a estação destino não for estabelecida. Neste caso, a conectividade do nó móvel não é afetada, pois ele continuará a receber dados pelo ponto de acesso de origem até sua completa transição para o ponto de acesso de destino.

Outros modos de classificação do *handoff*, além dos apresentados são encontrados na literatura [40, 42]. Uma taxonomia com uma lista mais exaustiva da classificação do *handoff* pode ser vista na Figura 2.8, extraída de [42]

Diante dos tipos e das classificações apresentadas é possível identificar que o processo de *handoff* configura a possibilidade de transições entre redes de acesso homogêneas ou heterogêneas. O *soft handoff* unido ao *handoff horizontal* garante a mobilidade com suporte

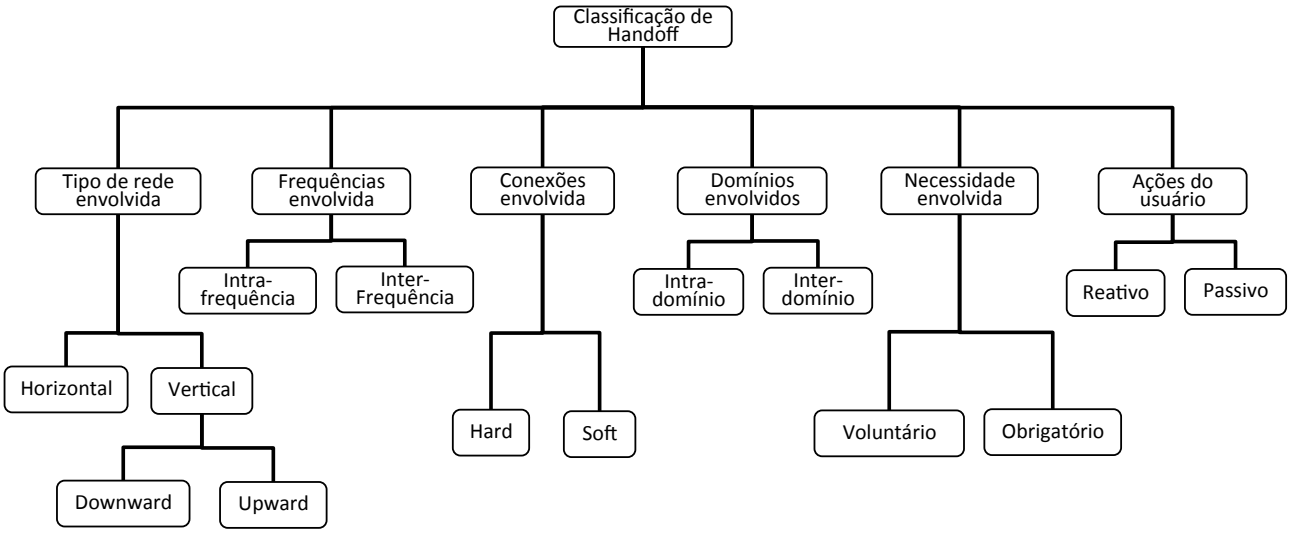


Figura 2.8: Taxonomia da classificação de *handoff*

a conectividade contínua em redes de mesma tecnologia. Já a união do *handoff vertical* e do *soft handoff* proporcionam a mobilidade irrestrita dos dispositivos móveis diante de redes de acesso heterogêneas com suporte à conectividade. Deste modo, a integração de diferentes tecnologias de rede de acesso sem fio é necessária para proporcionar uma "perfeita" interoperabilidade e convergência entre as tecnologias heterogêneas. Logo, o uso de técnicas de *handoff verticais* torna-se obrigatórias para assegurar o acesso onipresente aos usuários [37].

Fases do processo de *handoff* vertical

De acordo com [40, 14, 43, 44], o processo de *handoff vertical*, garante a conectividade em redes heterogêneas, é dividido em três fases: *Descoberta, Decisão* e *Execução.*

- **Descoberta de Rede**. Nesta fase um dispositivo móvel procura por redes sem fio disponíveis. O dispositivo móvel deve ativar suas interfaces para receber anúncios dos serviços que são transmitidos por diferentes tecnologias de redes sem fio. Durante esta fase, o dispositivo móvel determina quais redes podem ser usadas e os serviços disponíveis em cada rede. As redes também podem anunciar algumas de suas características como parâmetros de QoS e desempenho.

- **Decisão de *handoff***. Durante a fase de decisão de *handoff*, o dispositivo móvel

em transição define qual é a rede a qual tentará se conectar. A decisão considera os parâmetros obtidos na etapa anterior e pode depender de várias questões relacionadas com a rede de origem e a rede de destino. Por exemplo, a decisão de realizar o *handoff* pode ser feita com base em critérios como a largura de banda de rede, área cobertura, custo por acesso, QoS e preferências do usuário. Maiores detalhes sobre esse assunto são tratados posteriormente dado a importância dessa fase no processo de seleção de redes de acesso.

- **Execução do *handoff***. Essa fase realiza a transição efetiva de uma rede para outra. Durante a fase de execução, as conexões devem ser encaminhadas a partir da rede de origem para a nova rede de uma forma contínua. A fase deve garantir um processo de transição suave sem interrupção de conexão e permitir que o nó móvel transite por diferentes redes mantendo os seus fluxos de dados, o que também inclui a transferência de informações de contexto do usuário.

Inúmeros desafios ainda não foram superados em todas as fases do processo de *handoff*. A coleta de informações adequadas das redes disponíveis representam adversidades a serem superadas. A escolha e a decisão da melhor rede de acesso compreende um tópico muito discutido, devido às diferentes técnicas, parâmetros e critérios de escolha. Garantir a execução das transições entre tecnologias de comunicação diferentes sem a perda da continuidade dos fluxos de dados, envolve problemas em nível de conectividade, encaminhamento e entrega confiável dos dados. Essas questões são apenas algumas dentre as inúmeras que ainda necessitam de maiores investigações, como é o caso da seleção da melhor rede de acesso.

2.4 Segurança em redes heterogêneas

As redes heterogêneas formadas por diferentes redes de acesso com tipo de tecnologias de comunicação distintas são redes concebidas para atender as demandas dos usuários por conectividade em todo local e a toda instante. Contudo, as redes heterogêneas além de necessidade de convergência e conectividade com suporte a mobilidade possuem ou-

tras premissas consideradas fundamentais para sua consolidação. Requisitos como QoS e principalmente segurança compreendem tópicos fundamentais.

Os aspectos de QoS e segurança não foram planejados durante a concepção dos modelos correntes de redes em virtude de outras demandas mais importantes para a época. Nos modelos de comunicação atuais esses requisitos são implementados em nível de aplicação não fazendo parte da estrutura da rede. Logo, quando oferecidos são realizados de forma não planejada, apenas para satisfação das necessidades emergenciais. Tratando-se de segurança, tal medida está fadada ao fracasso, pois as soluções paliativas não garantem a estrutura adequada para sustentação de redes seguras [4]. Deste modo, nas redes heterogêneas os mecanismos de segurança deverão coexistir de maneira integrada à própria arquitetura da rede.

A convergência de diferentes tecnologias de comunicação traz consigo alguns problemas, principalmente relacionados as questões de segurança. Vulnerabilidades de segurança que são restritas a apenas um tipo de rede poderão se proliferar para todas as outras tecnologias de comunicação com a integração proporcionada pelos ambientes heterogêneos [16]. Portanto, os mecanismos de segurança deverão ser implantados como parte integrante da arquitetura da rede, ao invés de serem sobrepostos à estrutura básica por meio de serviços e aplicações como é feito atualmente.

Nos modelos clássicos de redes de acesso os requisitos de segurança se concentram nas camadas mais altas da pilha de protocolos. Isso acontece porque as concepções anteriores não exigiam certas preocupações como as redes heterogêneas exigem. Aspirações para um paradigma de comunicação sem limites para as redes heterogêneas mudaram a maneira convencional de atentar para a segurança da rede, com essa visão, os esquemas de segurança devem não só ser garantidas aos usuários finais locais, mas também proteger as redes inteiras de indivíduos maliciosos [45]. Os resultados de pesquisas e projetos apresentados ao longo de vários anos demonstram que segurança não recai em uma função singular que deve ser implantada isoladamente em uma única camada da rede [1]. Essas soluções exigem a combinação de responsabilidades sobre toda a pilha de protocolos, principalmente sobre as práticas dos processos de comunicação.

As abordagens de segurança concebidas de forma individualizada para cada tipo de rede não são eficazes e necessitam ser repensadas. Estratégias funcionais de proteção, reação e tolerância que sejam rigorosamente específicas para um determinado contexto, não atendem os propósitos de escalabilidade e portabilidade inerente às redes heterogêneas. A proposição de soluções genéricas demais podem comprometer sua eficácia e eficiência. Deste modo as exigências do novo modelo de rede determinam que as novas soluções de segurança devem ser abertas e extensíveis o suficiente para atender futuras estruturas.

A convergência de diferentes tecnologias de comunicação amplia as opções de conectividade com suporte à mobilidade, mas os problemas de segurança podem afetar diretamente a confidencialidade, integridade e disponibilidade dos serviços e aplicações de rede. Devido a uma infraestrutura convergente, as ameaças à segurança de um único ambiente não pressupõe o confinamento ao seu domínio de origem e podem facilmente ser propagadas para todas as outras redes [46]. Assim, um ataque limitado a um único modelo de rede poderá ser explorado de modo generalizado em todo ambiente convergente. Deste modo, estratégias de segurança que garantam a proteção, reação e tolerância a rede contra vulnerabilidades e ataques maliciosos ou egoísta são fundamentais.

A diversidade de problemas relacionados a segurança implica em outro desafio que requer soluções amplas que atendam ao maior número possível de requisitos. As estratégias atuais têm sido concentradas inicialmente nas abordagens proativas e reativas; no entanto, a necessidade de mecanismos tolerantes tem levantado muito interesse da comunidade científica e profissionais de segurança. As novas condições das redes requerem garantias à continuidade e disponibilidade dos serviços e aplicações mesmo na presença de ataques, intrusões, falhas e acidentes. Esta abordagem impulsiona as linhas de pesquisa sobre proteção, resiliência e sobrevivência de rede. Embora a junção das abordagens proativas, reativas e tolerantes sejam fundamentais, a maioria dos projetos de pesquisa, mesmo aqueles colaborativos, tendem a dedicar maior ênfase a um atributo ou a um conjunto de problemas específico. No contexto das redes heterogêneas essa tendência deve ser mudada para uma visão mais abrangente, buscando alternativas mais completas.

Além dos problemas de segurança causados pela convergência de redes heterogêneas, a

constante conexão e desconexão de diferentes dispositivos infectados por vírus ou software maliciosos *(malware)* devem ser evitadas para minimizar as chances de ataques e manter a qualidade dos serviços oferecidos pela rede. O perfil nômade dos usuários que utilizam essas redes de forma aleatória dificulta a criação de soluções de segurança eficazes. As redes heterogêneas devem garantir e manter o mesmo nível de segurança para os usuários quando eles estiverem em transição entre diferentes ambientes [4].

Oferecer segurança a um ambiente de redes heterogêneas implica uma perspectiva desafiadora e demanda por soluções robustas que considerem ações em diversos níveis de atuação, indo desde o meio físico até as aplicações [24, 8]. Nestas circunstâncias, muito ainda pode ser explorado quando se trata de segurança, principalmente no contexto de *Disponibilidade, Privacidade e Integridade.*

A *disponibilidade* de conectividade, serviços e aplicações diante de ameaças como ataques, intrusões, falhas, acidentes, entre outros, principalmente em ambientes em que a mobilidade predomina, implica em complexidade e desafios [5]. Essa complexidade aumenta consideravelmente em ambiente com redes heterogêneas que herdam todos os problemas existentes em cada modelo de rede.

A *privacidade* de serviços e conteúdo torna-se importante para os usuários, a fim de anonimizar sua movimentação, conexões no ambiente, localização, serviços utilizados e também dados coletados por sensores ou outros dispositivos, nem sequer conhecidos [47]. Os mecanismos de criptografia receberão maior atenção nestes cenários por oferecerem alternativas de ocultação.

A *integridade* garante que o estado das informações, programas e redes não foram alteradas indevidamente, permitindo determinar a confiabilidade. A confiabilidade implica em um dos atributos críticos em redes heterogêneas, pois pode influenciar diretamente na escolha de serviços, aplicações e conectividade em redes de acesso. Devido a necessidade de manutenção da conectividade durante a mobilidade em ambientes de redes heterogêneas de modo seguro, um problema em especial merece ser destacado, trata-se da confiabilidade e segurança no processo de transição por redes de acesso

2.4.1 Segurança na transição por redes

A segurança dos dispositivos móveis durante a mobilidade entre diferentes áreas de cobertura demanda soluções dinâmicas e autônomas que sejam tão eficientes quanto as ameaças de usuários maliciosos ou mal intencionados. A fase de transferência de conexão durante a mobilidade dos usuários compreende o momento mais crítico e propício a ataques. A transição do nó móvel com desejo de conexão contínua a qualquer custo expõe os usuários aos ataques e as vulnerabilidades ignorando as premissas básicas de um acesso seguro e confiável [15].

Para uma transição em redes homogêneas em que a mobilidade do nó ocorre por diferentes áreas de coberturas mas apoiados por mesma tecnologia de comunicação, existem soluções de segurança maduras e consistentes. O controle de acesso, por exemplo, implica em uma dessas soluções herdadas do modelo de autenticação utilizado na telefonia celular. Esta abordagem funciona com uma estação gestora da célula que autentica o usuário com base nas informações obtidas de uma central de autenticação mantida pela operadora, que armazena todas as credenciais dos usuários os quais oferece seus serviços [48, 49]. Como a tecnologia utilizada para a conexão é a mesma em toda área de cobertura, a autenticação de usuário acontece com a consulta em um único tipo de base de dados, centralizado ou distribuído pela rede. As soluções de segurança para este modo de mobilidade atuam na proteção e recuperação dessas bases de dados com as credencias dos usuários [48, 49]. Outra abordagem trata da garantia de privacidade das conexões, apoiado pela utilização de técnicas de *cifragem* e *decifragem* de dados trocados na rede.

Embora isoladamente as redes já estejam mais confiáveis e proporcionando conectividade com determinados níveis de qualidade e segurança, ainda há muito a ser feito no contexto de redes heterogêneas. Em relação à segurança, inúmeros obstáculos necessitam ser vencidos para uma conjuntura de ambientes convergentes. Ao contrário da suposição de conexões estáveis sobre a qual incide o desenvolvimento dos protocolos de comunicação, o principal desafio em redes heterogêneas está no descarte da conectividade contínua *fim-a-fim (end-to-end)*, devido à "flutuação" dos usuários em diversos pontos de acesso [5]. A conectividade intermitente advém das interrupções (planejadas ou não) de conexão

dos usuários, que migram de uma rede para outra constantemente. Este cenário dificulta o desenvolvimento soluções de segurança triviais, exigindo arcabouços complexos para garantir o oferecimento dos serviços de rede diante de variadas vulnerabilidades.

2.4.2 Vulnerabilidades da mobilidade em redes

Para suportar a mobilidade com conectividade contínua por redes heterogêneas, as estratégias de segurança implicam em maior complexidade devido a três principais fatores: *i)* A integração de diferentes tecnologias de rede de acesso; *ii)* O perfil nômade dos usuários móveis; *iii)* A escolha inadequada da rede de acesso.

- **Integração de diferentes tecnologias de rede de acesso**

  A convergência de redes heterogêneas faz com que os problemas de segurança de determinada rede se propaguem para todas as outras redes integradas. A convergência de tecnologias expõe as redes de comunicação aos mais diversos tipos de vulnerabilidades que antes eram restritos a cada rede. Os ataques, antes direcionados a uma determinada tecnologia serão passíveis de uso em toda a infraestrutura convergente, podendo não só contaminar como tornar indisponível toda a rede.

- **Perfil nômade dos usuários móveis**

  Os dispositivos móveis que se conectam em diferentes redes estão sujeitos aos seus problemas de segurança, e quando infectados se tornam fontes propagadoras de vírus, *Malware, Spyware,* etc. de uma rede para outra. A constante associação e dissociação dos dispositivos móveis em diferentes redes não afastam a possibilidade de infecção por códigos maliciosos que abram brechas para futuros ataques. Assim, ao se conectarem em outras redes esses códigos, oriundos dos dispositivos em transição, podem ser proliferados proporcionando portas de entradas *(Backdoors)* para atacantes maliciosos ou egoístas na rede.

- **Escolha inadequada da rede de acesso**

  A escolha inadequada da rede de acesso pode causar sérios problemas ao usuário

como a perda dos serviços utilizados ou até mesmo a indução de conexão à redes boicotadas por atacantes maliciosos. A seleção errada pode induzir usuários a se conectarem em redes totalmente contaminadas por códigos maliciosos, resultando em roubo de informações confidenciais, quebra do sigilo de dados e até aquisições de credenciais para possíveis futuras personificações.

Esses três pontos de vulnerabilidade representam os principais problemas de segurança que podem ser explorados em redes heterogêneas. Evitar a perda de conectividade durante o trânsito de um dispositivo em diferentes redes satisfaz uma das premissas básicas para um ambiente de rede heterogêneas. No entanto, determinar os níveis de segurança e confiabilidade dessas redes para serem usados como um critério de decisão de seleção da rede de acesso compreende um dos principais problemas a ser tratado.

2.5 Resumo

Neste capítulo foram abordados os conceitos e fundamentos relacionados ao tema de pesquisa desta tese. Foram discutidos os conceitos relacionados às redes de acesso heterogêneas e seus modos de heterogeneidade. Também foram descritos os modelos e princípios de mobilidade nessas redes com a manutenção de conectividade. Por fim, os aspectos de segurança e as vulnerabilidades associados a essas redes foram descritos.

CAPÍTULO 3

SELEÇÃO DE ACESSO E ESTRATÉGIAS DE SEGURANÇA

Esse capítulo discute as técnicas de seleção de acesso e estratégias de segurança existentes na literatura. A Seção 3.1 detalha os desafios da interoperabilidade e complexidade de integração de conectividade em redes heterogêneas. A Seção 3.2 apresenta os padrões e normas relacionados à conectividade durante a transição por diferentes redes de acesso. A Seção 3.3 descreve o princípio *sempre melhor conectado*, método mais empregado no processo de seleção de redes. A Seção 3.4 apresenta os algoritmos, métodos, critérios e métricas utilizados na seleção. A Seção 3.5 descreve as estratégias de segurança existentes em rede de acesso, e a Seção 3.6 apresenta o resumo do capítulo.

3.1 Interoperabilidade e complexidade de integração

Os sistemas de comunicação do futuro serão cada vez mais complexos, envolvendo várias tecnologias de redes com diversos recursos e diferentes capacidades [14]. Proporcionar a interoperabilidade e acesso a essas redes heterogêneas, com objetivo de fornecer aos usuários conexão ubíqua a serviços avançados de alta qualidade de uma forma segura, eficiente, a qualquer momento e em qualquer lugar, é um dos grandes desafios para pesquisadores da área. Com a proliferação das diferentes redes de acesso e a evolução dos dispositivos computacionais móveis com suporte a diferentes tecnologias de comunicação, a seleção adequada da melhor rede de acesso entre as disponíveis se torna uma questão crítica, ainda sem solução concreta.

A evolução do desenvolvimento de dispositivos computacionais móveis e a proliferação das tecnologias de redes de acesso possibilitarão a manutenção da conectividade contínua. Logo, o acesso as redes de transmissão de dados não é e nem será o principal problema de conexão. O aumento das áreas de cobertura dessas redes de acesso heterogêneas existentes já garantiram a abrangência de quase todas as áreas urbanas, permitindo uma

conectividade globalizada, mesmo a usuários mais remotos aos grandes centros.

Nestes sentido, além da ampla área de cobertura, um elevado número de região de sobreposição de diferentes tecnologias de redes de acesso coexistem, permitindo a escolha da rede mais adequada para os serviços e aplicações dos usuários. Contudo, a seleção da rede de acesso mais adequada em um ambiente com múltiplas redes de diferentes características não é uma tarefa trivial. A escolha equivocada da rede pode causar sérias consequências aos usuários, como a perda de conectividade, falha intermitentes nos serviços utilizados e principalmente ameaças e vulnerabilidades de segurança [50]. Deste modo, a seleção da rede pode ser considerada um problema complexo, envolvendo um processo de diversas etapas.

3.2 Padrões e normas em redes heterogêneas

Uma forma de garantir a transição e a interoperabilidade entre várias tecnologias de acesso é a criação de várias extensões específicas de mídia de acesso. Por exemplo, o acesso à determinada tecnologia *T1* pode ser estendido para interoperar com o acesso à uma tecnologia *T2*, enquanto que seria necessário uma outra extensão para garantir a interoperabilidade com uma tecnologia *T3*. Da mesma forma, as tecnologias de acesso *T2 e T3* exigiriam suas próprias extensões. Assim, seriam necessários $N \times (N-1)$ extensões específicas de mídia para garantir que todas as N tecnologias de acesso interajam umas com as outras. A complexidade deste tipo de abordagem aumenta na ordem de N^2 e não se adapta bem quando mais tecnologias de acesso são consideradas [51].

Com o desenvolvimento acelerado das redes de acesso heterogêneas, a comunidade científica e a indústria têm direcionado esforços para garantir a interoperabilidade entre as redes e a uniformidade dos modos de transição. Assim, iniciativas de padronização têm sido propostas para definir um modelo comum de acesso em diferentes redes. As iniciativas propõem o desenvolvimento de normas, padrões e protocolos que sustentem o funcionamento dessas tecnologias de redes de comunicação heterogêneas.

3.2.1 IEEE 802.21

O padrão *IEEE 802.2*1 para redes locais e metropolitanas define os mecanismos de acesso a mídia independente, que facilita as transições entre redes heterogêneas. O *IEEE 802.21* permite a conexão em diferentes redes de acesso a partir de informações obtidas através da exploração dos serviços da função de mídia independente de *handover MIHF (media independent handover function)*, que consiste de um mecanismo para a troca de informações através da mídia independente *handover MIH (media independent handover)* entre terminais móveis e pontos de acesso fixos da rede [14, 51, 52]. O objetivo do *IEEE 802.21* é melhorar a experiência do usuário, fornecendo a funcionalidade MIH, que facilita os *handoffs* iniciados pelo dispositivo móvel ou pela rede. De acordo com [51], a especificação do padrão é constituída pelos seguintes componentes:

- **MIHF**. Consiste da Função MIH composta por três serviços específicos: o *MIES, MICS e MIIS*. O *MIES* - serviço de evento de mídia independente, detecta as alterações de propriedades na camada de enlace e os relata para as interfaces locais ou remotas. Deterioração ou indisponibilidade do link são exemplos de alterações detectadas. Este tipo de serviço é fornecido a partir de camadas mais baixas para as camadas superiores. O *MICS* - serviço de comando de mídia independente, fornece um conjunto de comandos para o *MIH* de usuários para controlar o estado do link. O *MICS* oferece comandos para as camadas superiores controlar as camadas inferiores em relação *handoff*. Os comandos seguem uma direção de cima para baixo, em oposição aos eventos. Os comandos típicos são o escaneamento de redes disponíveis e a configuração de dispositivos. O *MIIS* - serviço de informação de mídia independente, fornece informações sobre as redes vizinhas, incluindo a sua localização, propriedades e serviços relacionados. O *MIIS* oferece o mecanismo para a recuperação de informações para auxiliar a decisão de *handoff*.

- **SAPs**. Os Serviços de Ponto de Acesso definem as interfaces específicas de mídia independentes. Em particular, os *SAPs* incluem:

  - *MIH_SAP*, uma mídia independente SAP que fornece uma interface uniforme

para camadas superiores para controlar e monitorar diferentes ligações, independentemente da tecnologia de acesso.

  - *MIH_LINK_SAP*, uma mídia específica SAP que fornece uma interface para o MIHF para controlar e monitorar um enlace de mídia específica. Para o MIHF fornecer o MIES e o MICS de um determinado enlace, ele deve implementar um MIH_LINK_SAP para essa camada de enlace.
  - *MIH_NET_SAP*, uma mídia independente SAP que fornece serviços de transporte sobre o plano de dados no nó local, apoiando a troca de informações e mensagens MIH com o MIHF remoto.

- **MIH user**. Representam as entidades funcionais que empregam os serviços *MIH*. Um usuário típico de serviços MIH pode ser o gestor de aplicações de mobilidade que usam esses serviços para otimizar as transições. Por exemplo, os usuários MIH podem se inscrever com as MIES para serem notificados quando eventos específicos e importantes para a decisão e o processo de transferência ocorrerem [51]. A Figura 3.1 ilustra a estrutura de alto nível do protocolo 802.21 com o relacionamento entre seus componentes.

Segundo [14] a gestão, as políticas e os algoritmos de *handoff* envolvidos na tomada de decisão devem ser manipulados por uma entidade externa da seleção de rede e não se enquadram no âmbito desta norma. São necessárias alterações nos padrões existentes de diferentes tecnologias de mídia específicas (por exemplo, *IEEE 802.3, IEEE 802.11, IEEE 802.16*, e sistemas *3GPP/3GPP2*) para satisfazer as necessidades identificadas pelo padrão IEEE 802.21 [53].

3.2.2 3GPP TS 23.402 e TS 24.312

As especificações *3GPP TS 23.402 e TS 24.312, release 11*, apresentam um novo elemento de rede chamado de descoberta de rede de acesso e função de seleção -*ANDSF (access network discovery and selection function)* que é definido como um sistema de evolução de arquitetura - *SAE (System Architecture Evolution)* para apoiar a descoberta e seleção

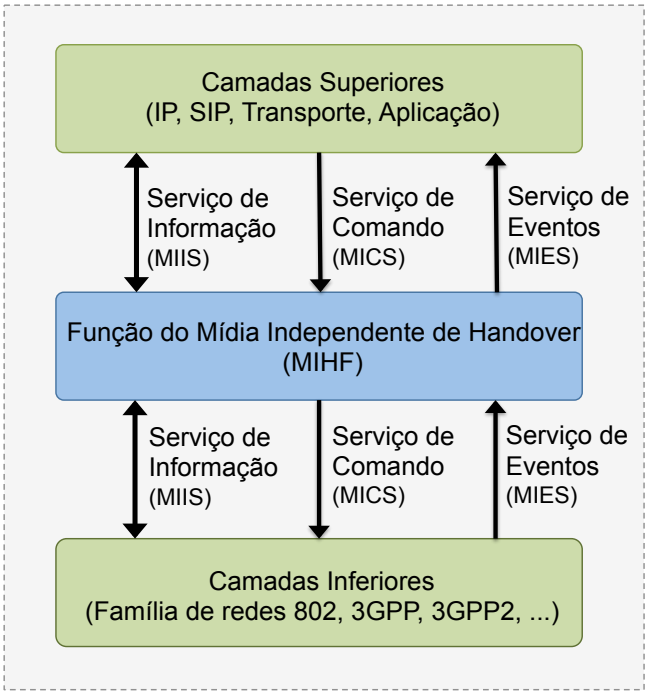


Figura 3.1: Estrutura em alto nível do padrão 802.21

de rede de acesso. O ANDSF é implantado na infraestrutura da rede e contém o gerenciamento de dados e a funcionalidade de controle para auxiliar os dispositivos móveis no processo de seleção através do provisionamento de políticas relacionadas à mobilidade dos dispositivos. A pedido de um nó móvel, o ANDSF pode fornecer uma lista de redes de acesso disponíveis em suas imediações, incluindo informações sobre identificador e tipo de tecnologia da rede de acesso. As políticas de mobilidade implicam nas regras de operação definidas e nas preferências que afetam as decisões de mobilidade realizada pelo dispositivo móvel. Elas podem indicar se um tipo de tecnologia específica ou um identificador de rede de acesso é preferível em relação a outro, as condições em que a mobilidade é restrita a partir de um tipo de rede para outro, e em que condições as políticas a serem aplicadas são válidas [14, 54, 55].

3.2.3 IEEE 1900.4

O padrão *IEEE 1900.4* define a construção de arquiteturas de tomada de decisão distribuída, permitindo aos dispositivos fazer uso otimizado dos recursos de rádio em redes de acesso sem fio heterogêneas. Especificamente, o padrão tem como objetivo melhorar a

qualidade de serviço de redes sem fio em ambientes de vários rádios, através da definição de arquitetura e protocolos adequados para facilitar a otimização de recursos, incluindo controle de acesso dinâmico de espectro. A reconfiguração adequada de redes e de terminais são empregados com base em informações trocadas entre os dispositivos móveis e a rede [14, 56].

Outros padrões não tão conhecidos ou em fase de desenvolvimento abordam a questão de seleção e acesso de redes heterogêneas. Essas soluções ainda necessitam de muitos testes e investigações para se tornarem consolidadas, alguns ainda encontram-se em fases de definições e projeto, sem uma expectativa de utilização em cenários reais. Apesar das iniciativas de padronizações a comunidade científica vêm constantemente apresentando trabalhos relacionados a esse assunto. Novas abordagens considerando as iniciativas de padronização são anunciadas a todo momento como é o caso do princípio *ABC*.

3.3 Sempre Melhor Conectado

O princípio *Always Best Connected* ABC implica na capacidade dos usuários se conectarem a rede de acesso mais adequada aos serviços solicitados, entre um conjunto de redes de mesma ou diferente tecnologia de comunicação disponíveis [14]. A seleção da rede de acesso mais eficiente e adequada para satisfazer os requisitos de QoS de aplicações específicas tornou-se um tópico importante, cujo foco real é a maximização da *QoE (qualidade de experiência)* do usuário. O ABC se enquadra no âmbito da transferência de procedimentos de uma rede para outra, que deve ser flexível e eficiente, envolve complexas considerações multicritérios como preferências do usuário, requisitos e restrições dos serviços e aplicações, condições e recursos da rede e dos dispositivos móveis. Ao mesmo tempo, os usuários devem permanecer isentos da heterogeneidade da infraestrutura de comunicação, bem como das potenciais modificações que possam ocorrer [57]. O interesse é a continuidade do serviço, a robustez, a disponibilidade e consistência mantida de forma transparente ao usuário. Transitar por redes heterogêneas de forma a manter a conectividade contínua e garantir que o princípio ABC seja atendido, implicam em questões desafiadoras. Logo, o processo de seleção da melhor rede de acesso representa o ponto

de partida para as pesquisas sobre transição com manutenção de conectividade em redes heterogêneas.

3.4 Algoritmos, métodos, critérios e métricas

A seleção da rede de acesso em ambientes heterogêneos é realizada pelo processo de *handoff* vertical [43]. Para efetuar as transições pelas redes o handoff vertical realiza as fases de *Descoberta, Decisão e Execução.* Entretanto, a definição da melhor rede a ser escolhida depende de uma série de diferentes fatores, tais como, preferências do usuário, capacidades do dispositivo, requisitos da aplicação, segurança, recursos de rede disponíveis e cobertura. Segundo [50], esses fatores combinados com os indicadores chave de desempenho *KPIs (Key performance indicators)*, que representam um conjunto de medidas utilizadas para acompanhar as condições da rede ao longo do tempo, permitem avaliar os critérios utilizados na decisão sobre a escolha da rede de acesso.

3.4.1 Fase de descoberta e coleta de informações da rede

A fase de descoberta envolve a obtenção de informações utilizadas na fase de decisão *handoff*. Para coletar as informações disponíveis a partir de diferentes fontes, os dispositivos móveis examinam as redes vizinhas, a fim de descobrir serviços e condições como taxas de dados, largura de banda. Como forma de complemento às informações obtidas através do escaneamento, as redes também podem anunciar seus serviços suportados e os parâmetros de QoS utilizados. De acordo com [43], a coleta de informações de forma confiável é crucial para o processo de transição, pois a decisão de seleção usa esses dados como apoio para a escolha da melhor rede. A fim de maximizar os benefícios da tomada de decisão, informações de todas as camadas das pilhas de protocolos podem ser consideradas. Contudo, informações sobre as preferências do usuário são relevantes para o processo de decisão, principalmente devido ao seu impacto sobre a satisfação do usuário final.

Técnicas de coleta e estimativa de dados

O modo de coleta é fundamental para garantir a confiabilidade e a validade dos dados coletados. De acordo com [50], na maioria dos casos, as abordagens mais adequadas para a coleta de valores das alternativas não são investigadas nos trabalhos encontrados na literatura.

A *escolha dos valores médios dos estados anteriores* essa estratégia de coleta só é eficaz em redes com estados relativamente estáveis. Outra opção seria a coleta dos valores recentes, que refletem com sucesso as condições atuais das redes. No entanto, esses valores ignoram as informações que podem ser fornecidas por sessões passadas, e portanto, presumem que se ocorrer uma anomalia, ela continuará existindo.

A *técnica de previsão de dados* prever valores de atributos no futuro com base no histórico dos dados. Por exemplo, em função da hora do dia e de padrão de uso, muitos atributos de QoS, como a utilização de um ponto de acesso, podem ser previstos com um certo grau de certeza. A Predição de dados determinístico pode ser realizada como método de previsão, tal como médias simples de movimento, médias ponderadas, regressão, entre outros. As técnicas de previsão utilizadas podem ser representadas como números *fuzzy*.

Outra forma de estimativa de dados consiste em *probabilidades*. Este procedimento está relacionado com cadeias de *Markov* e é, na maioria das vezes, associadas a um conjunto limitado de parâmetros de decisão, tais como a relação de interferência de sinal, probabilidade de bloqueio e probabilidade de terminação.

Na presença de informação imprecisa, a *estimativa Bayesiana sequencial*, que tem como base parâmetros de QoS dinâmicos, estimados através da aproximação de *bootstrap*, pode ser realizada. Conceitos de aprendizagem de máquina, como *aprendizagem Bayesiana*, podem ser empregados para fornecer inferência confiável sobre o estado da rede a partir de informações incompletas [50]. A Técnica de *bootstrap* é uma abordagem com base em computador não paramétrico, onde não são feitas suposições sobre a população, a partir do qual são coletadas as amostras. Essa técnica permite estimar as distribuições de probabilidade dos parâmetros críticos de QoS a partir dos dados obtidos [50].

3.4.2 Fase de decisão de *handoff*

A fase de decisão consiste no principal momento da transição entre redes de acesso heterogêneas, uma vez que é responsável por avaliar e decidir entre as opções de rede disponíveis, qual é a mais adequada a fim de atender os requisitos do usuário, proporcionando as comunicações contínuas desejadas [43]. A fase de decisão utiliza as informações coletadas na fase de descoberta de rede para inferir qual rede é a mais adequada para transição. Devido às diferentes técnicas e os numerosos parâmetros envolvidos no processo de coleta, os pesquisadores têm tentado encontrar a solução mais adequada para seleção da melhor rede [50, 58].

Algoritmos de Decisão

Algumas técnicas adotam um modelo mais simplista com base em algoritmos que consideram individualmente critérios definidos e coletados na fase de descoberta de rede. Segundo [44], entre os critérios mais comuns é possível colocar em destaque os algoritmos baseados em:

- **Força do sinal recebido** - *RSS (Received signal strength).* Neste classe a informação de RSS é usada como o principal critério de decisão de transição. Várias estratégias foram desenvolvidas para comparar o RSS do ponto de acesso atual com o do o ponto de acesso candidato. Esse critério é amplamente o mais utilizado como forma de seleção de rede.

- **Largura de banda disponível** *(Bandwidth).* Em determinados algoritmos, a largura de banda é utilizada no processo de decisão. Quando a demanda de serviços e aplicações necessitam de maiores vazões esse critério é amplamente utilizado.

- **Função de custo** *(Cost function).* Esta classe de algoritmos combina métricas como custo monetário, largura de banda e consumo de energia, em uma função de custo. A transição é feita comparando o resultado desta função para as redes candidatas.

- **Combinação**. Algoritmos de combinação tentam usar um conjunto mais completo das entradas para a tomada de decisão. Normalmente essa classe de algoritmos combina outros diferentes algoritmos para decidir sobre a melhor rede. Xiaohuan [44], apresenta uma classificação de outros trabalhos que abordam esses modelos de algoritmos mais simplistas de decisão.

Métodos de inferência

Esses métodos realizam análises mais completas e complexas dos valores coletados na fase de descoberta de rede, para conseguir processar a seleção mais adequada. Os métodos de inferência trabalham com valores objetivos e subjetivos na composição de seus modelos, que normalmente são representados de forma analítica. As abordagens seguem diferentes estratégias como apresentadas na sequência:

1. **Método de ponderação aditiva simples** - *SAW (Simple Additive Weighting Method)* também conhecido como o método da soma ponderada. A ideia é obter a soma dos pesos normalizadas de cada parâmetro das redes candidatas.

2. **Método para a ordem de preferência por similaridade a solução ideal** - *TOPSIS (Technique for Order Preference by Similarity to Ideal Solution)*, considera que a rede candidata selecionada é a mais próxima da solução ideal possível e está mais distante da pior solução possível. A solução ideal pode ser obtida com os melhores valores possíveis para cada parâmetro coletado.

3. **Método de ponderação exponencial multiplicativo** - *MEW (Multiplicative Exponential Weighting Method)*, também conhecido como o método do produto ponderado, utiliza multiplicação de pesos para mensurar os parâmetros de classificação da rede.

4. **Método de eliminação e escolha expressando realidade** - *ELECTRE (Elimination and Choice Expressing Reality)*, tem como base uma comparação de pares entre os parâmetros das redes candidatos. Os conceitos de concordância e discordân-

cia são usados para medir a satisfação e insatisfação do tomador de decisão quando se comparam as redes candidatas.

5. **Analise hierárquica de processo** - *AHP (Analytic Hierarchy Process)*, a estratégia do método AHP é decompor um problema complicado em uma hierarquia de subproblemas simples e fáceis de resolver.

6. **Grey Análise relacional** - *GRA (Grey Relational Analysis)*, consiste de um método de classificação usado entres as redes candidatas para escolher aquela que tem o posto mais alto entre as disponíveis.

7. **Lógica Fuzzy**, permite realizar a seleção com base em limiares de qualidade da rede gerados pelos fuzzyficadores.

8. **Rede Neural**, utiliza o método de treinamento para o reconhecimento de padrões, assim a decisão de transição é tomada caso um padrão seja detectado, como por exemplo a degradação ou melhora do sinal.

9. **Método sensível ao contexto** - *(Context-aware)* tem como base o conhecimento da informação de contexto do dispositivo móvel e das redes, a fim de tomar decisões melhores e inteligentes.

10. **Teoria dos Jogos**, consiste de um método matemático utilizado para compreender e modelar situações competitivas que implicam na interação entre os tomadores de decisões racionais com interesses mútuos e possivelmente conflitantes.

Inúmeros trabalhos encontrados na literatura apresentam maiores detalhes sobre os métodos de inferência apresentados [58, 50, 43, 59, 44].

Estratégias existentes para seleção de melhor rede de acesso

Diferentes formas de inferir sobre a melhor rede de acesso podem ser vistas na literatura. Algumas estratégias consideram a combinação de técnicas e métodos apresentados anteriormente. A maioria dos trabalhos abordam o problema de seleção da melhor rede como

um problema multicritério, em que a combinação de diferentes métricas deve ser levada em conta para encontrar a rede mais adequada.

Radhika *et. al* [60] discutem a dificuldade de selecionar a rede ótima dependendo do tipo de aplicação. Os autores mencionam a inexistência de algoritmos inteligentes de seleção de redes para prover melhor desempenho na integração de redes com dispositivos *multhoming* (multi-interface). É proposto o desenvolvimento de um algoritmo de decisão de *handoff* adaptativo e multicritério que utiliza *lógica fuzzy*. O algoritmo considera valores de força do sinal recebido *(RSS)* , custo monetário *(C)*, largura de banda disponível *(BW)*, velocidade *(V)* do dispositivo móvel e preferência do usuário *(P)* para a escolha da rede de destino. Os parâmetros são classificados em altos e baixos para facilitar a normalização e utiliza o método de cálculo do vetor de peso.

Bojan *et. al* [61] realizam uma análise multicritério para a seleção da melhor rede de acesso. Os critérios utilizados são classificados em três categorias: *i)* Critérios orientados a rede: características técnicas de desempenho do enlace como cobertura, largura de banda, etc.; *ii)* Critérios orientados a serviço: parâmetros de QoS oferecidos aos usuários através de métricas como atraso, jitter, taxa de erro, taxa de perda. Essa é uma das categorias mais usadas em problemas de seleção porque envolve métricas básicas; e *iii)* Critérios orientados ao usuário: são mais subjetivos e expressam a satisfação dos usuários como custo do serviço, *QoE (Qualidade da Experiência)*, etc. Para distribuir as informações das métricas entre os dispositivos da rede é usado *CPC (Cognitive Pilot Channel)*.

Farah *et. al* [62] descrevem a seleção de tecnologias de rádio de acesso evitando o desperdício de recursos e diminuindo o atraso total no processo de seleção. Eles propõem algoritmos heurísticos para a seleção de tecnologias de redes de acesso. Os autores adotam uma abordagem global, em que o sistema aloca o tráfego *downlink* entre duas tecnologias diferentes *802.11b e 802.11g*. A estratégia utiliza os seguintes algoritmos: *i)* algoritmo de seleção com base na distância, influenciado pela potência do sinal. Cada usuário analisa a potência do sinal recebido e seleciona a rede com sinal mais forte; *ii)* algoritmo baseado em probabilidade de distância. Cada usuário utiliza uma variável aleatória e mede a potência recebida verificando se é maior que a variável corrente, e assim obtém a

probabilidade de seleção; *iii)* Algoritmo de seleção com base na taxa de pico. O usuário seleciona a rede com o pico máximo de sinal de transmissão; *iv)* algoritmo de seleção com base na probabilidade de pico máximo. Quanto maior a taxa de pico recebido maior a probabilidade de selecionar a rede.

Ying *et. al* [63] argumentam a dificuldade de selecionar a rede ótima a partir de um conjunto de redes. A existência de diferentes tipos de valores utilizados dificulta a decisão de seleção. Os autores apresentam uma árvore de decisão que usa aprendizado não supervisionado com base em um conjunto de dados de treinamento, seguindo as duas fases: *i)* fase para rotulagem hipotética para objetos de treinamento; e *ii)* fase da seleção da rede com base na aprendizagem do conhecimento. Desta forma, é realizado um processo de aprendizado e seleção para cada interação.

Joon *et.al* [64, 65] apresentam uma proposta de gerenciamento autonômico de decisões de *handoff* personalizado em redes heterogêneas chamado *AUHO (AUtonomic HandOver)*. Essa proposta usa *lógica fuzzy* e funções de utilidade como parte do processo de tomada de decisão. As preferências do usuário são consideradas como uma forma de garantir um *handoff* personalizado. Os autores definem duas métricas objetivas para analisar o desempenho dos pontos de acesso e apoiar a decisão: *i) APAV (Access Point Acceptance Value)*, que representa o grau de aceitação de um ponto de acesso por usuários finais com base nos dados de métricas de preferência do usuário (força do sinal, qualidade do serviço, custo ou tempo de vida da bateria) e os requisitos de aplicação; *ii) APSV (Access Point Satisfaction Value)*, que representa o grau com que um ponto de acesso satisfaz o usuário final com base em seu perfil de usuário, que inclui os pesos de cada item de preferência do usuário.

3.4.3 Fase de execução de *handoff*

Esta fase é responsável pela execução da transição. Após a coleta das informações realizadas na primeira fase e a decisão da rede a ser utilizada na fase dois, a fase de execução efetua uma atualização de conexão a rede. Assim, essa fase está relacionada com a gerência, execução e controle das transições contínua, além do gerenciamento de mobilidade do

dispositivo em transição.

Gerência

Durante o processo de transição, quando um dispositivo móvel atinge um novo ponto de acesso, o sistema executa procedimentos de gerência das conexões. Estes procedimentos normalmente efetuam o Registo, a Associação, Re-associação, e as tarefas de Dissociação [43]. O registro está relacionado com a solicitação de acesso à rede. A associação implica no estabelecimento de vínculo com a rede. A Reassociação representa o estabelecimento de um novo vínculo após um vínculo antigo ser quebrado. A Dissociação consiste na desconexão do ponto anteriormente associado.

Execução

O processo de execução de *handoff* acontece de dois modos: *1) Hard Handoff*, quando o nó móvel é conectado a um único ponto por vez, assim ao se deslocar de uma área para outra ele deve se desassociar do ponto de acesso anterior antes de se associar ao novo ponto. Neste processo há uma interrupção de conexão, devido a dissociação. *2) Soft Handoff*, neste modo de execução o nó móvel mantém temporariamente mais de uma única conexão. Neste caso o nó em transição se mantém associado à rede antiga até que o novo vínculo à rede de destino seja completamente estabelecido, garantindo uma transição sem interrupção de conexão e do serviço utilizado [43, 59]. Para alcançar a continuidade em cenários de mobilidade, a transição tem que ser perfeita. Isso significa que a transição para a nova rede deve ser transparente para o usuário e sem degradação perceptível dos serviços e de conectividade.

Controle

No processo de transição deve haver uma entidade responsável por controlar o *handoff* [43]. Habitualmente, a transição pode ser controlada pela rede ou pelo dispositivo móvel. No *handoff* controlado pela rede *NCHO-(Network-Controlled HandOver)*, a entidade rede

tem o controle primário sobre a transição. Esse modo de controle consiste de uma solução normalmente adotada pelos operadores de redes para alcançar funções de balanceamento de carga e de gerenciamento de tráfego. No *handoff* controlado pelo dispositivo móvel *MCHO-(Mobile-Controlled HandOver)*, o nó realiza a transição por conta própria. Este tipo de controle é o caso mais comum, geralmente com base nas avaliações preliminares da rede feitas pelo usuário.

O processo de transição envolve algumas informações e medições obtidas a partir do dispositivo móvel, da própria rede ou de ambos. O *handoff* auxiliado pelo dispositivo móvel *MAHO-(Mobile-Assisted HandOver)* acontece quando informações e medições dos nós móveis são utilizados pela rede para auxiliar a transição. Já o *handoff* auxiliado pela rede, *NAHO-(Network-Assisted HandOver)*, ocorre quando a rede recolhe informações que podem ser utilizadas pelo nó móvel em sua tomada de decisão e transição.

Gerenciamento de mobilidade

Uma das questões chave para a manutenção da conectividade dos dispositivos móveis em transição é o gerenciamento de mobilidade. As redes baseadas no protocolo *IP* possuem iniciativas para suporte à mobilidade. Estas iniciativas funcionam com as camadas intermediárias da *pilha TCP/IP*. Os protocolos mais comuns utilizados para suporte a mobilidade em redes *IP* são o *MIP v.4 (Mobility Internet Protocol), MIP v.6, SIP-(Session Initiated Protocol), NEMO-(Network Mobility Basic Support Protocol) e HIP-(Host Identity Protocol)* [59, 43].

Contudo, esses mesmos protocolos de gerenciamento de mobilidade não se adaptam as redes que não utilizam o protocolos *TCP/IP*. As redes *GSM*, por exemplo, utilizam técnicas semelhantes ao *Mobile IP*, no entanto, existem peculiaridades que não são atendidas pelo *IP Móvel*. Dado que cada rede possuir diferentes tecnologias e padrões para o gerenciamento de mobilidade, é difícil conceber uma solução que se ajuste a todas as redes de comunicação. Uma alternativa para o gerenciamento de mobilidade consiste no uso de *multhoming*, onde um único dispositivos possui várias interfaces de comunicação para as diferentes redes de acesso as quais se conecta. Assim, os dispositivos móveis passam a

ter diferentes interfaces de conexão que atendam aos padrões específicos de cada rede de acesso. No entanto, o uso de *multhoming* implica na necessidade de várias interfaces de redes para dispositivos móveis com capacidades computacionais limitadas, que demandam um gerenciamento dessas interfaces, podendo comprometer o desempenho do dispositivo.

3.4.4 Critérios e métricas de seleção em redes heterogêneas

Para a coleta de informações das condições da rede e dos dispositivos móveis são necessários critérios e métricas que possam orientar a obtenção de dados representativos. A definição de métricas adequadas é uma tarefa complexa devido à relevância dos parâmetros utilizados. Os parâmetros devem ser potencialmente mensuráveis ou representados por indicadores que possam ser aferidos. Diante da dinamicidade das redes heterogêneas, coletar valores de parâmetros representativos ainda é um desafio. Os valores coletados em determinado instante podem sofrer alterações radicais devida às novas condições topológicas, infraestruturais e lógicas da rede, e não serem representativos. Deste modo, um parâmetro contabilizado em um cenário pode ser diferente e impreciso com a mudança desse cenário.

Segundo Ramona [58], os critérios de decisão que podem ser utilizados no processo de seleção da rede são classificados em quatro categorias, dependendo da sua natureza: *Critérios baseados na Rede, nos Dispositivos Móveis, nos Serviços e Aplicações, e nas Preferências dos Usuários.*

- **Critérios com base na Rede.** Expressam as características técnicas e de desempenho das redes de acesso. Estes critérios são especificados para a rede e não para o provisionamento de serviços. Os principais parâmetros para esse critério são: cobertura, largura de banda, latência, e principalmente qualidade do enlace de acordo com intensidade do sinal recebido *RSS (Received Signal Strength)*, taxa de interferência na portadora *CIR (Carrier-to-Interferences Ratio)*, taxa sinal interferência *SIR (Signal-to-Interferences Ratio)*, taxa de erro de bit *BER (Bit Error Rate), etc.*

- **Critérios com base nos dispositivos móveis**: Os parâmetros mais utilizados

são velocidade, energia da bateria, informações de localização e formas de movimentação.

- **Critérios com base em Serviços e Aplicações**: Dizem respeito ao QoS oferecido ao usuário final através de uma série de KPIs. Esta categoria envolve métricas básicas de QoS de redes de comutação de pacotes, tais como *capacidade dos serviços, atraso, jitter, etc.*

- **Critérios com base no Usuário**: São subjetivos e expressam certos aspectos da satisfação do usuário final. Devido à imprecisão, esses critérios são muitas vezes expressos em termos linguísticos. Os parâmetros são relacionados ao *perfil do usuário, preferências, orçamento, QoE,* entre outros. A Figura 3.2 apresenta uma ilustração do exemplo do processo de escolha de melhor rede de acesso com base nos critérios mencionados.

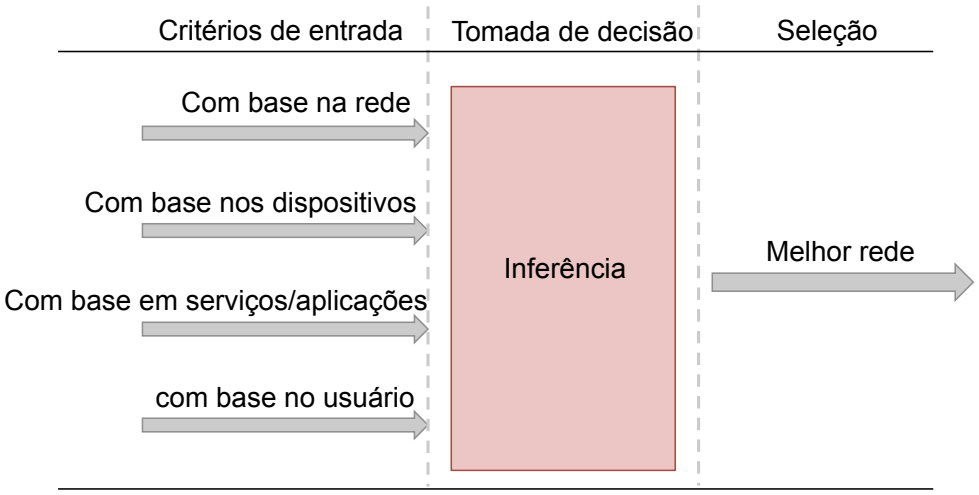


Figura 3.2: Exemplo do uso dos critérios para escolha de melhor rede

Diferentes trabalhos usam os mais variados critérios e métricas como forma de auxílio no processo de decisão. Outras formas de classificação das métricas podem ser encontradas em [59, 44, 43, 66, 50, 67, 40, 58]. A grande maioria dos trabalhos só considera critérios relacionados ao desempenho, deixando de lado critérios relacionados à segurança.

3.5 Estratégias de segurança existentes

O estudo e a proposição de estratégias de segurança são de fundamental importância para a consolidação de uma infraestrutura básica de suporte à mobilidade contínua e segura em redes heterogêneas. Diferentes abordagens têm sido apresentadas na literatura como forma de proporcionar segurança em redes heterogêneas.

Daojing *et al.* [15] discutem o problema da segurança e a ineficiência dos protocolos de autenticação para os serviços de transição *(roaming)* de usuários em redes sem fio. Os autores investigam os principais desafios inerentes ao *roaming* de usuários e os categorizam em requisitos obrigatórios e opcionais. Entre os requisitos obrigatórios são apontados a necessidade de: servidor de autenticação, validação da inscrição, provisão de revogação de usuários, estabelecimento de chaves, baixa complexidade computacional e custo de comunicação, anonimato e não rastreabilidade, e resistência a ataques. Os autores argumentam que embora as pesquisas no campo de autenticação de *roaming* têm recebido uma atenção significativa, ainda existem muitas questões que precisam ser abordadas, tais como, a unificação das credencias e dos métodos de autenticação para redes heterogêneas.

Fazirulhisyam *et al.* [45] sugerem uma abordagem bioinspirada no sistema imunológico humano pela *seleção negativa* e *teoria do perigo* para a segurança em redes heterogêneas. Os autores discutem a dificuldade de conceber um sistema que possa detectar as vulnerabilidades em todos os modelos de redes. Deste modo, a seleção negativa é utilizada para identificar ataques conhecidos, similar a um *IDS (sistema de detecção de intrusão)* por assinaturas. Já a teoria do perigo identifica um invasor mal-intencionado na rede, pelo fato de reagir às condições anormais ou de perigo, consequentemente a técnica é capaz de identificar ataques desconhecidos. Os resultados alcançados mostram que as técnicas são complementares e que o uso de ambas proporciona um esquema de mitigação via zona de perigo.

Hani *et al.* [68] discorrem sobre os ataques em dispositivos móveis de usuários finais e a sua posterior utilização como ferramentas de ataques às redes heterogêneas. Os autores comentam que as pesquisas existentes sobre a segurança de redes heterogêneos têm focado

em segurança como autenticação e autorização, principalmente, sobre a interface entre a rede e o operador. No entanto, a proteção do dispositivo móvel contra ataques, e posteriormente como uma ferramenta de ataque à rede se torna uma questão importante. Uma arquitetura com base em políticas para o gerenciamento de segurança de redes 4G, focando na detecção e prevenção de ataques maliciosos é proposta neste trabalho. Os autores apresentam um sistema de gerenciamento de segurança que detecta se o dispositivo móvel foi atacado, e deste modo evita utilizá-lo, removendo o acesso do usuário e cortando sua conexão com a rede.

Glenford *et al.* [69] propõem um modelo de segurança para redes heterogêneas com base na arquitetura *Y-Comm*. Nesse trabalho os autores discutem as vulnerabilidades de segurança em rede heterogêneas 4G, e propõem uma arquitetura de segurança integrada para proteger os dados e as entidades da rede de comunicação. A arquitetura *Y-Comm* é composta de dois *frameworks*, um para tratar dos problemas da periferia da rede e outro para os problemas do núcleo da rede. A estratégia proposta emprega um modelo de segurança multi-camada que precisa ser aplicada tanto ao *framework* de periferia quanto ao núcleo simultaneamente para proporcionar a segurança. As camadas de segurança descritas atuam no gerenciamento do transporte seguro de dados e na autenticação de serviços e dispositivos móveis. Os autores argumentam que *Y-Comm* é capaz de oferecer três modelos de segurança de redes distintos: modelo de segurança de conexão, modelo de segurança baseado em anel e modelo de segurança de *handoff* vertical.

Jiannong *et al.* [70] apresentam uma plataforma para a integração segura de redes heterogêneas sem fio denominada *SHAWK (Secure Heterogeneous Advanced Wireless networK)*. A abordagem aponta três questões chaves de segurança: o *roaming* contínuo e seguro por redes heterogêneas, a comunicação multi-salto segura e a mobilidade de aplicação segura. A plataforma implementa um servidor de autenticação central em *AAA (authentication, authorization and accounting)*, o mecanismo de gerenciamento de transições tem como base o protocolo 802.21, a segurança de comunicação multi-salto utiliza o protocolo *OLSR (Optimized Link State Routing Protocol)* para que as mensagens sejam criptografas, eliminando a bisbilhotagem e garantindo a privacidade. Os resultados

obtidos por meio de experimentos reais com redes *MESH*, *WLAN* e *GSM* emuladas mostram que esse mecanismo melhora a segurança das redes sem fio heterogêneas com pouca modificação da arquitetura da rede.

Outros projetos aplicáveis às redes heterogêneas também são encontrados na literatura como o projeto *SHAMAN* (2000-2002) [70, 71], que investiga um arquitetura de segurança para *roaming global* em redes heterogêneas com o foco na autenticação. O *3G Evolution* (2005-2008) [70, 72], que oferece um *testbed* para autenticação unificada de interoperabilidade entre redes *UMTS-WLAN*. O projeto de mobilidade contínua e segura do *NIST (National Institute of Standards and Technology - EUA)* (2006-) [70, 73], que é centrado na interconexão de redes heterogêneas e não-interoperáveis. O projeto *SeQoMo* (2000-2004) [70, 74] que tem o objetivo de alcançar a segurança e o suporte à QoS para a mobilidade dos nós em redes heterogêneas. O projeto *SECRICOM* (2008-2012) [70, 75] que aborda a interconexão de dispositivos e redes heterogêneas seguras e contínuas. O projeto *ODTONE* (2009-) [70, 76] que trabalha na implementação de código aberto do mídia independente *handoff (MIH)* do protocolo 802.21.

Apesar do considerável número de trabalhos e projetos relacionados à segurança em redes heterogêneas, a grande maioria se preocupa com métodos de autenticação de usuários durante o estabelecimento de conexão pelas diferentes redes. Devido à transição de usuários com dispositivos móveis de uma rede para outra, o controle de acesso à rede e seus recursos representa o principal foco abordado. As iniciativas têm sido direcionadas às formas de reconhecimento e autorização de acesso à rede.

Embora o processo de controle de acesso represente etapa fundamental para o oferecimento de segurança, não implica na única prioridade para garantir uma transição segura com suporte à mobilidade contínua por redes heterogêneas. A necessidade de uma avaliação das condições de segurança da rede para auxiliar no processo de decisão de escolha da rede de acesso compreende outro ponto de fundamental importância que pode evitar inúmeras consequências desagradáveis aos usuários. Uma análise das condições mínimas de segurança dos dispositivos que desejam acesso à rede também pode evitar danos maiores e garantir níveis de confiabilidade e robustez à rede. Deste modo, uma avaliação

mútua das condições de segurança da rede e do dispositivo em transição auxiliará no desenvolvimento de estratégias que proporcionem segurança tanto para a rede quanto aos dispositivos móveis em transição.

3.6 Resumo

Esse capítulo apresenta algumas técnicas de seleção de acesso e estratégias de segurança existentes na literatura. Foram detalhados os desafios da interoperabilidade e complexidade de integração de conectividade em redes heterogêneas, bem como descritos os padrões e normas relacionados à conectividade. Além disso, foram destacados os algoritmos, métodos, critérios e métricas utilizados no processo de seleção. Por fim, foram discutidos as estratégias de segurança existentes em redes de acesso.

CAPÍTULO 4

UMA ARQUITETURA PARA O GERENCIAMENTO DE CONECTIVIDADE EM REDES HETEROGÊNEAS

Este capítulo detalha a proposta de uma arquitetura para o gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas. A Seção 4.1 descreve as asserções do sistema com as hipóteses levantadas e seus objetivos. A Seção 4.2 mostra os requisitos necessários para uma conectividade segura e contínua. A Seção 4.3 detalha a proposta de arquitetura para o gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas. A Seção 4.4 resume o capítulo.

4.1 Objetivos e asserções do sistema

Diferente das concepções anteriores, que utilizam somente critérios de desempenho como forma de avaliação, a arquitetura apresentada define e utiliza métricas de segurança de forma autonômica para estimar as condições da rede e dos dispositivos móveis em transição. O uso dos coeficientes de resiliência e robustez, entre outras primitivas, permitirão aos dispositivos tomarem decisão de conexão por redes heterogêneas mais robustas e confiáveis. Do mesmo modo, os indicadores de segurança dos dispositivos possibilitarão às redes conceder ou não o acesso e recursos a determinados usuários em transição.

Os objetivos específicos para o desenvolvimento de uma arquitetura de gerenciamento integrada e adaptativa de conectividade segura em redes heterogêneas precisam considerar a definição de forma automatizada de métricas quantificáveis de resiliência e robustez, que permitam determinar índices de segurança da rede e dos dispositivos em transição; a utilização de técnicas de inferência que possibilitem processar os valores das métricas coletadas para definição da melhor rede de acesso; o desenvolvimento de uma abordagem de gerenciamento de seleção para melhor rede de acesso com base em métricas de segurança e não somente métricas de desempenho; a possibilidade de conceder ou negar

o acesso e recursos a determinados dispositivos analisando seus indicadores de segurança; o oferecimento de suporte à mobilidade com conectividade dos dispositivos móveis em redes heterogêneas; o provimento de transições transparentes aos usuários móveis com manutenção de conexão ininterruptas por redes de acesso; a garantia de proteção à rede e aos dispositivos móveis durante o processo de escolha e transição para a melhor rede disponível.

As asserções do sistema consideram que a definição de métricas de segurança possibilitam aferir coeficientes quantificáveis como de *resiliência e robustez* como forma de obter indicadores de segurança que podem ajudar na definição de melhores redes de acesso em ambientes heterogêneos. A escolha adequada da rede de acesso deve prevenir e proteger os usuários de conexões em redes inseguras e boicotadas por indivíduos maliciosos, intencionados à atacar e roubar informações para futuras personificações.

A partir dos indicadores de segurança de cada dispositivo, a rede pode decidir em oferecer ou não o acesso à conexão, como também limitar o uso de recursos para garantir sua disponibilidade e manter seus índices de confiabilidade. Deste modo, a avaliação mútua entre as redes de acesso e os dispositivos em transição auxiliam no desenvolvimento de uma solução de conectividade segura em redes de acesso heterogêneas.

4.2 Requisitos para uma conectividade segura e contínua

Os requisitos de um sistema especificam o conjunto de funcionalidades que ele deve prover para satisfazer as necessidades e restrições a que está sujeito [77]. A partir do estudo realizado sobre redes heterogêneas, mobilidade com conectividade, seleção de rede de acesso e segurança é possível determinar e definir um conjunto de requisitos necessários para a concepção de uma abordagem de gerenciamento do acesso seguro em redes heterogêneas com conectividade contínua. Esses requisitos são classificados em requisitos gerais, requisitos de seleção de rede de acesso, requisitos de transição, requisitos de mobilidade e requisitos de segurança, enunciados na sequência.

4.2.1 Requisitos gerais

Os requisitos gerais compreendem as exigências globais para a criação de uma estratégia completa de conectividade, mobilidade e segurança em redes heterogêneas. Esses requisitos são:

- **Conectividade**. Requisito referente à conexão em diferentes tecnologias de redes de comunicação;
- **Continuidade**. Preservação das transmissões realizadas entre os usuários, para tanto, deve-se garantir a entrega/recebimento ininterrupto dos dados dos usuários durante transição de uma rede para outra;
- **Acesso otimizado**. Assegurar o acesso por redes mais adequadas às necessidades de cada usuário;
- **Segurança**. Proteção mútua à rede e aos usuários móveis no processo de transição, bem como ser um indicador determinante na escolha de melhor rede.
- **Confiabilidade**. Esse requisito condiciona a mobilidade com conectividade dos dispositivos móveis por redes genuínas. No entanto, a execução de transições deve ser efetuada somente por redes seguras e confiáveis;
- **Estabilidade de serviços e aplicações**. Manutenção do funcionamento de serviços e aplicações de redes garantindo QoS mínimo para o bom desempenho da rede.

4.2.2 Requisitos de seleção de rede de acesso

A escolha da rede mais adequada às necessidades dos usuários é um dos desafios da seleção de redes de acesso. Devido à coexistência de diferentes perfis de usuários na rede, as estratégias de seleção devem ser simples e eficientes, de modo que os usuários menos familiarizados com as tecnologias de comunicação sejam capazes de usufruir de seus recursos. Os requisitos de seleção estão relacionados à escolha da melhor rede de acesso entre as redes disponíveis. Esses requisitos são:

- **Melhor conexão**. Seleção de melhor rede de acesso entre redes disponíveis.
- **Dinamicidade**. A seleção da rede deve ser dinâmica e de forma transparente e contínua aos usuários;
- **Autonomia**. Seleção de rede sem a necessidade de interferência manual do usuário. A Seleção deve ser automática (autonômica) em ambiente multiusuário, multitecnologia.
- **QoE**. Respeitar as opções do usuário no processo de escolha; para tanto, a seleção deve considerar suas experiências, preferências e seu perfil;
- **Justiça**. Decisão justa na escolha da melhor rede de acesso. A seleção deve considerar abordagens monocritério ou multicritério para definição de melhor rede;
- **Fidelidade**. Cumplicidade às etapas essenciais dos métodos de seleção. A seleção de melhor rede deve obedecer as seguintes etapas:
  - Definição dos critérios e métricas de decisão;
  - Coleta de valores dos parâmetros das métricas definidas;
  - Inferência de melhores redes com base na análise dos valores obtidos;
  - Classificação das melhores alternativas encontradas;
  - Escolha da melhor rede com base na classificação.

4.2.3 Requisitos de transição

Os requisitos de transição envolvem a mudança de conexão de uma rede para outra sem que as trocas de dados sejam comprometidas e nem as conexões interrompidas. Os requisitos são:

- **Melhor Transição**. As transições devem ser efetuadas sempre para as melhores redes disponíveis;

- **Autonomia**. Transições de modo autônomo que dispensem a intervenção manual no processo de migração. As transições devem ser transparentes aos usuários e à rede de acesso sem interferir em seu desempenho;
- **Conectividade**. As transições devem acontecer sem interrupção de conectividade;
- **Continuidade**. Manutenção dos serviços e aplicações dos usuários e da rede em razão das transições dos usuários. As transições devem ser suaves ao usuário e suas aplicações, como também às redes de acesso;
- **Eficiência**. Transições de uma rede para outra com pouco ou nenhum atraso nas conexões;
- **Eficácia**. Evitar que os dispositivos móveis fiquem continuamente migrando entre duas redes de acesso sobrepostas, para tanto é necessário a execução de transições sem efeito *ping-pong*.[1]
- **Fidelidade**. As transições entre as redes de acesso devem obedecer as etapas de monitoração, seleção/decisão e execução

4.2.4 Requisitos de mobilidade

O suporte à mobilidade não foi contemplado nos modelos de redes tradicionais devido à outras necessidades como a conectividade. Atualmente, os anseios são de mobilidade com suporte à conectividade em todo momento, assim, a concepção de qualquer estrutura de rede que não contemple os requisitos de mobilidade com manutenção de conectividade está fadada ao fracasso. Os requisitos de mobilidade correspondem ao suporte a mobilidade dos usuários com seus dispositivos, serviços, aplicações. Os requisitos são:

- **Mobilidade ilimitada**. Permitir o livre trânsito entre diferentes redes de acesso.
- **Continuidade**. Suporte à mobilidade com manutenção da conectividade;

[1]Constante mudança entre duas redes que oscilam sua qualidade/desempenho.

- **Disponibilidade**. Garantir a continuidade de acesso independente da rede e área de cobertura na qual o usuário esteja.

- **Diversidade**. Suporte à mobilidade dos dispositivos, às aplicações e a rede, de forma a manter a conectividade e o oferecimento de seus serviços, independentemente do elemento móvel e do tipo de rede de acesso.

4.2.5 Requisitos de segurança

Os requisitos de segurança compreendem linhas de defesa que atuem de modo preventivo, reativo e tolerante no processo de gerenciamento de seleção, transição e mobilidade em redes de acesso heterogêneas. Os requisitos são:

- **Integridade**. As propriedades originais das redes devem ser preservadas, evitando que elas possam ser manipuladas por atacantes no decorrer do tempo para induzir a seleção inadequada da rede de acesso;

- **Confidencialidade**. Restrição ao acesso às informações ou a determinadas redes por dispositivos credenciados, evitando que dados privados possam ser divulgados;

- **Disponibilidade**. Manutenção da proteção dos dispositivos durante seu trânsito pelas redes;

- **Proteção**. Garantia que os dispositivos móveis possam se proteger de redes de acesso boicotadas e inseguras e que as redes também possam estar imunes a ações de usuários maliciosos que transitam por diferentes redes;

- **Autonomia**. As soluções de segurança devem ser independentes do tipo de rede de acesso a que elas estejam vinculadas para garantir a maior abrangência possível de proteção, reação e tolerância.

- **Adaptabilidade**. As abordagens de segurança devem ser adaptáveis às condições da rede e dos dispositivos móveis;

- **Dinamicidade**. Assegurar que os mecanismos de segurança não afetem a dinâmica da rede;

A preocupação com a segurança da infraestrutura da rede, com a proteção do tráfego de informações, com a integridade e confidencialidade dos dados dos usuários, etc. tem aumentado significativamente. As ações de usuários maliciosos devem ser reprimidas a fim de proporcionar ambientes mais confiáveis. Atender aos requisitos mínimos de segurança com abordagens de proteção, reação e tolerância é fundamental para as novas concepções de estratégias direcionadas às rede heterogêneas.

A lista de requisitos apresentada, apesar de extensa não é considerada exaustiva e novas demandas podem ser adicionadas. Para cumprir o conjunto de requisitos apontados, inúmeras técnicas devem ser utilizadas a fim de satisfazer todas as exigências. Iniciativas existentes que atendam a determinados requisitos de modo parcial podem ser ajustados para uma abordagem mais completa. Deste modo, considera-se que alternativas que cubram os requisitos indicados proporcionarão acesso seguro às redes heterogêneas com suporte à mobilidade com manutenção de conectividade contínua.

4.3 Especificação da arquitetura

Esta seção apresenta a definição de uma arquitetura de gerenciamento integrada e adaptativa (autonômica) que permita acesso seguro às redes heterogêneas com suporte à mobilidade com conectividade contínua. A arquitetura busca atender ao maior número possível dos requisitos definidos na Seção 4.2. A arquitetura está organizada em três planos de ação: *Plano de Gerência, Plano de Conectividade e Plano de Segurança*. Além dos três planos de ação, a arquitetura consiste de cinco módulos, denominados de *Módulo de Coleta de Informações, Módulo de Decisão, Módulo de Transição, Módulo de Supervisão e Módulo de Segurança*, como ilustrado na Figura 4.1. Esses módulos estão em todos os dispositivos móveis e nos pontos provedores de acesso da rede que disponham da solução.

Os módulos da arquitetura se relacionam para oferecer um mecanismo de gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas. O processo

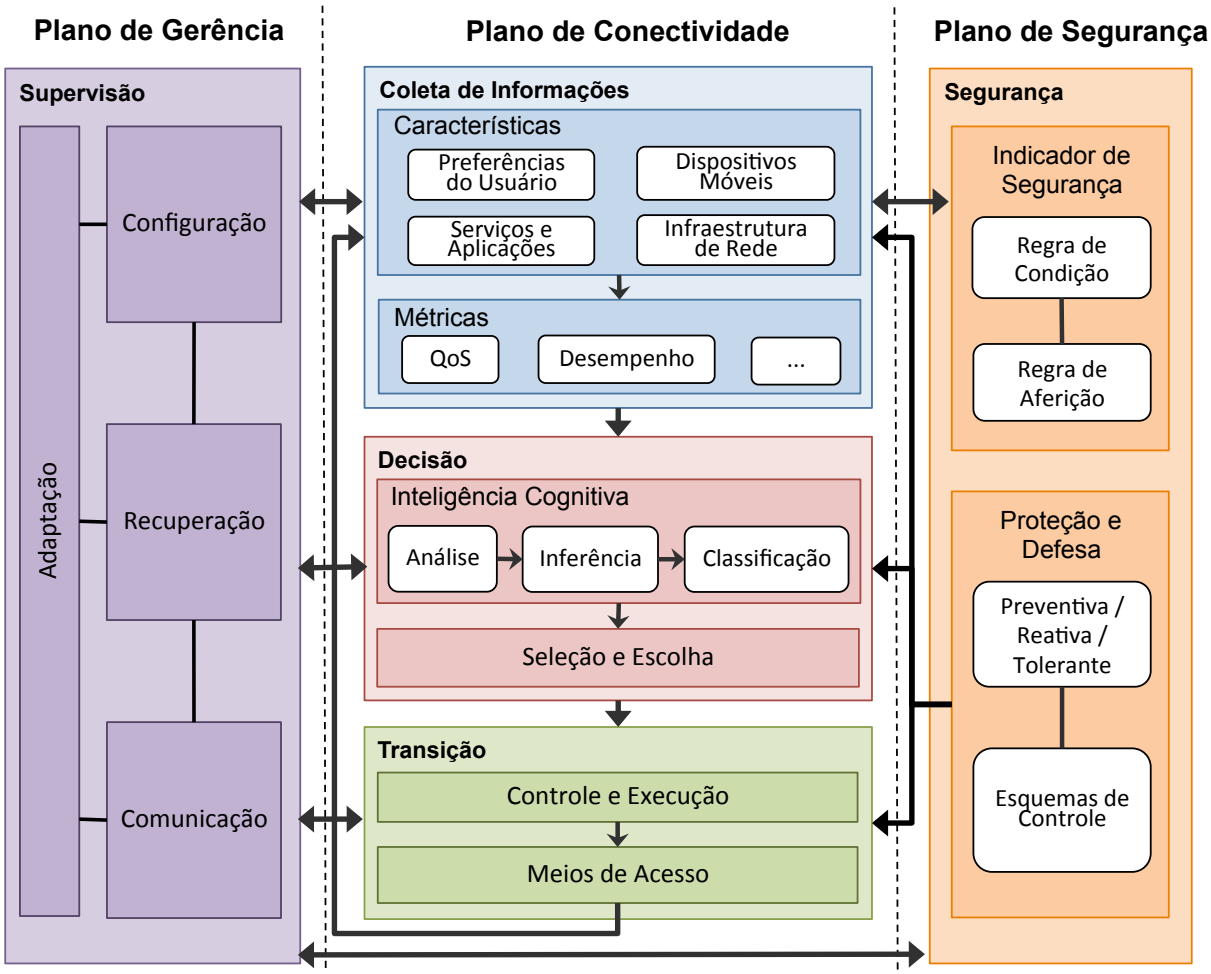


Figura 4.1: Arquitetura para o gerenciamento de conectividade

de transição é realizado a partir das etapas de monitoramento, decisão e execução efetuados pelos módulos de *Coleta de Informações, Decisão e Transição* respectivamente. Dois novos módulos são adicionados ao processo para garantir uma gerência autonômica e segura das transições com manutenção da conectividade. O módulo de *Supervisão* é o responsável pelo monitoramento e controle de todos os relacionamentos entre os demais módulos da arquitetura, bem como o gerenciamento de serviços relacionados a transição entre redes heterogêneas com manutenção de conectividade. O módulo de *Segurança* tem o papel de proteger as etapas do processo de transição e do gerenciamento, e oferecer novos critérios e métricas que possam ser aferidas e utilizadas como indicadores de segurança da rede e dos dispositivos móveis, auxiliando desta forma na escolha da melhor rede de acesso ou no dispositivo candidato à conexão. A descrição e o detalhamento dos módulos da arquitetura são apresentados na sequência.

4.3.1 Módulo de coleta de informações

O *Módulo de Coleta de Informações* é responsável pela entrada dos dados para auxiliar na decisão da melhor rede de acesso. Esse módulo é composto de dois componentes, chamados de componente de *Características* e componente de *Métricas*. O primeiro componente define quais critérios são utilizados na coleta dos dados empregados na escolha da rede. As características podem ser definidas com base nas *Preferências do Usuário*, como o custo a ser pago pelo serviço, a experiência do usuário vivenciada com determinado recurso, a rede, a aplicação, dentre outros critérios diretamente ligados ao usuário. Outros critérios têm como base os *Dispositivos Móveis* que analisam informações referentes à mobilidade do dispositivo, recursos disponíveis, e demais informações do dispositivo móvel. Critérios com base nos *Serviços e Aplicações* que dispõem sobre as características essenciais às aplicações de rede como largura de banda, atraso, taxa de entrega, etc. Os últimos critérios têm como base a *Infraestrutura da Rede* dispondo sobre as características exclusivas da rede de acesso tais como área de cobertura, topologia e modelo de propagação.

O segundo componente do módulo de *Coleta de Informações* está relacionado com as métricas utilizadas para aferir valores dos critérios definidos. Comumente essas métricas estão relacionadas com a questão de qualidade ou desempenho e avaliam quantitativamente o comportamento de determinado sistema/processo em um instante de tempo contínuo ou discreto. Contudo, outras métricas podem ser utilizadas sem estar diretamente relacionadas à qualidade ou desempenho, como é o caso da segurança.

As informações obtidas pelo *Módulo de Coleta de Informações* são a base para a classificação da melhor rede. Assim como as informações são utilizadas pelo dispositivo móvel para classificar as melhores redes, as redes também utilizam as informações referentes aos dispositivos móveis obtidas nesta fase para classificar os nós candidatos a fazerem parte da rede de acesso.

4.3.2 Módulo de decisão

O *Módulo de Decisão* define a melhor rede de acesso ou os melhores dispositivos candidatos à conexão. O módulo é formado por dois componentes: o componente de *Inteligência*

Cognitiva e o componente de *Seleção e Escolha*. O componente de *Inteligência Cognitiva* é composto por um elemento de *Análise*, que é responsável pela tabulação e preparação dos dados advindos das métricas coletadas no módulo de coleta, um elemento de *Inferência* que processa os dados das diferentes redes ou de diferentes dispositivos e os encaminha para o elemento de *Classificação* que é responsável por ranquear as melhores redes de acesso entre às redes disponíveis ou os melhores dispositivos móveis candidatos a fazer parte da rede.

O componente de *Seleção e Escolha* tem como finalidade a indicação da melhor rede de acesso ou melhor dispositivo candidato com base na *ordem* criada pelo elemento de *Classificação*. A partir desta informação a decisão é encaminhada para o próximo módulo da arquitetura responsável pela execução da transição.

O *Módulo de Decisão* é considerado o núcleo da arquitetura, pois no seu componente de *Inteligência Cognitiva* são definidas as técnicas de inferência usadas para encontrar as melhores redes de acesso ou melhores dispositivos candidatos a fazer parte da rede. Diferentes técnicas de inferência como as apresentadas na Seção 3 podem ser utilizadas de forma individual ou mesmo combinadas para a obtenção de maiores índices de precisão. O resultado da decisão é a indicação da melhor rede ou dispositivos entre os disponíveis no momento, e essas informações são encaminhadas para a efetivação das transições no módulo subsequente.

4.3.3 Módulo de transição

O *Módulo de Transição* é o responsável por efetivar as mudanças de conexão de uma rede para outra a partir dos resultados da escolha de melhor rede ou de melhor dispositivo candidato a entrar na rede. Este módulo é composto por dois componentes: o componente de *Controle e execução* e o componente de *Meios de Acesso*. O objetivo do componente de *Controle e execução* consiste em efetivar a mudança de uma rede para outra com a manutenção da conectividade e fluxo de dados dos dispositivos móveis. Este componente faz a negociação do acesso às diferentes redes disponíveis. O componente de *Meios de Acesso* detecta as diferentes redes disponíveis na área de cobertura em que os dispositivos

transitam. Esse componente realiza uma monitação com o propósito de encontrar diferentes redes disponíveis para que elas possam ser avaliadas a fim de encontrar a melhor e dar início ao processo de seleção.

O *Módulo de Transição* realiza a migração de acesso de uma rede para outra em ambientes heterogêneos. Por se tratar da etapa de efetivação da mudança de rede, ela é considerada uma etapa muito propícia a ataques e descontinuidade das comunicações. No *Módulo de Transição* acontecem as trocas de credenciais para o controle de acesso à rede e essas informações devem ser restritas aos usuários dos dispositivos em trânsito, e ao provedor de acesso da rede, evitando que terceiros possam capturá-las e fazer uso no futuro. Apesar do processo de parecer completo, dois novos módulos são adicionados a arquitetura como forma de garantir maior autonomia e segurança, são eles o *Módulo de Supervisão e o Módulo de Segurança*.

4.3.4 Módulo de supervisão

O *Módulo de Supervisão* é responsável por gerenciar todas as relações entre os outros módulos da arquitetura, e pelo gerenciamento de serviços diretamente ligados à conectividade e segurança das redes de acesso. O modulo possui um componente de *Configuração*, um componente de *Recuperação*, um componente de *Comunicação* e outro componente de *Adaptação*. O componente de *Configuração* realiza todas as configurações dos dispositivos móveis e dos pontos de acesso da rede para os ajustes necessários à troca de dados, como as configurações dos endereços de rede, os ajustes das potências de transmissão, dentre outros. O componente de *Recuperação* é responsável pela restauração de configurações ou estados dos sistemas que devido a algum acontecimento podem estar inoperantes. O componente de *Comunicação* é o gerenciador das comunicações entre os dispositivos móveis e os pontos de acesso da rede. Esse componente é o responsável direto pela troca de informações como a solicitação e a concessão ou não de acesso à rede. O componente de *Adaptação* torna o processo de seleção e a gerência dos módulos autonômica e adaptativa.

O *Módulo de Supervisão* monitora e controla todos os relacionamentos entre os outros módulos, sendo o responsável pela característica autonômica e adaptativa do gerencia-

mento dos serviços na rede, sem a necessidade de intervenção humana e adaptativo às condições de contexto da rede e dos dispositivos móveis.

4.3.5 Módulo de segurança

O *Módulo de Segurança* é um dos principais módulos da arquitetura, ele tem papel decisivo na seleção de melhor rede de acesso em ambientes heterogêneos. O módulo é formado por dois componentes distintos: um componente de *Indicadores de Segurança* e um componente de *Proteção e Defesa*. O primeiro componente atua em conjunto com o módulo de *Coleta de Informações* oferecendo a possibilidade de utilização de *Características e Métricas* de segurança para a análise e decisão da melhor rede, a partir dos índices de segurança da rede e dos dispositivos candidatos a conexão. Essa abordagem é inovadora tendo em vista que os trabalhos anteriores não utilizam métricas de segurança no processo de escolha de melhor rede de acesso. As *Características e Métricas* de segurança utilizadas no processo de decisão devem ser aferidos dinamicamente por parâmetros quantificáveis que indicam determinados coeficientes de aspectos de segurança da rede ou dos dispositivos, como a *robustez, fragilidade, resiliência, antifragilidade* entre outras propriedades possíveis de serem quantificadas.

O segundo componente, *Proteção e Defesa* é o responsável por prover a proteção e a segurança ao processo de escolha da melhor rede e melhor dispositivo, evitando que usuários maliciosos ou mal intencionados interfiram no processo de decisão de forma a induzir o erro na escolha adequada. O componente de *Proteção e Defesa* é formado por dois elementos. O primeiro elemento é responsável pelas ações *Preventivas, Reativas e Tolerantes* que devem ser oferecidas pelas estratégias de proteção e defesa do sistema. O segundo componente compreende os *Esquemas de Controle* para as ações preventivas, Reativas e Tolerantes. O componente de *Proteção e Defesa* está diretamente relacionado aos princípios de *Confidencialidade, a Integridade e a Disponibilidade* que devem ser assegurados aos módulos de *Coleta, Decisão e Transição*, módulos propícios a ação de atacantes.

O *Módulo de Segurança* é a base para o gerenciamento de seleção segura, dinâmica e

adequada da melhor rede acesso em ambientes heterogêneos. Esse módulo proporciona a seleção com base em indicadores de segurança diminuindo as chances de uma escolha equivocada por redes de acesso boicotadas, ou permitindo que usuários mal intencionados façam parte e usufruam dos recursos da rede. Outra vantagem do módulo é a proteção que ele proporciona para as fases de coleta de informações, decisão e execução das transições por diferentes redes de acesso. Essa característica evita que atacantes interfiram na transição entre redes, induzindo os usuários ou os provedores de acesso ao erro de seleção e causando danos maiores após a conexão estabelecida.

A arquitetura apresentada atua de forma integrada e adaptativa, permitindo acesso seguro às redes heterogêneas com suporte a mobilidade com conectividade contínua. A arquitetura provê um acesso otimizado pela seleção de rede mais adequada, a continuidade de conectividade dos dispositivos que transitam de uma rede para outra, a segurança no processo de seleção da rede de acesso ou de dispositivos candidatos ao estabelecimento de conexão, a transição por redes confiáveis e a garantia de estabilidades de conectividade dos serviços e aplicações de redes.

Taxonomia de segurança

Para categorizar os desafios inerente ao *Módulo de Segurança* é apresentado uma taxonomia ilustrada na Figura 4.2. Essa taxonomia classifica os esquemas de segurança em *soluções, técnicas, linhas de defesa e princípios*, que devem ser analisados para quantificar os indicadores de segurança da rede ou dos dispositivos em transição por redes heterogêneas. Essa categorização permite identificar uma sequência lógica das estratégias de segurança e correlacioná-las com os princípios nos quais são baseados.

Os *Princípios* de segurança são divididos em *Fundamentais e Secundários*; os princípios fundamentais compreendem a *Confidencialidade, Integridade e Disponibilidade*, que são a tríade base para qualquer abordagem de segurança. A partir do relacionamento dos princípios fundamentais, são definidos outros princípios de segurança secundários, como a *Privacidade, o Anonimato, a Legalidade, a Autenticidade*. A relação da confidencialidade e da privacidade geram o anonimato, a confidencialidade, legalidade, integridade e

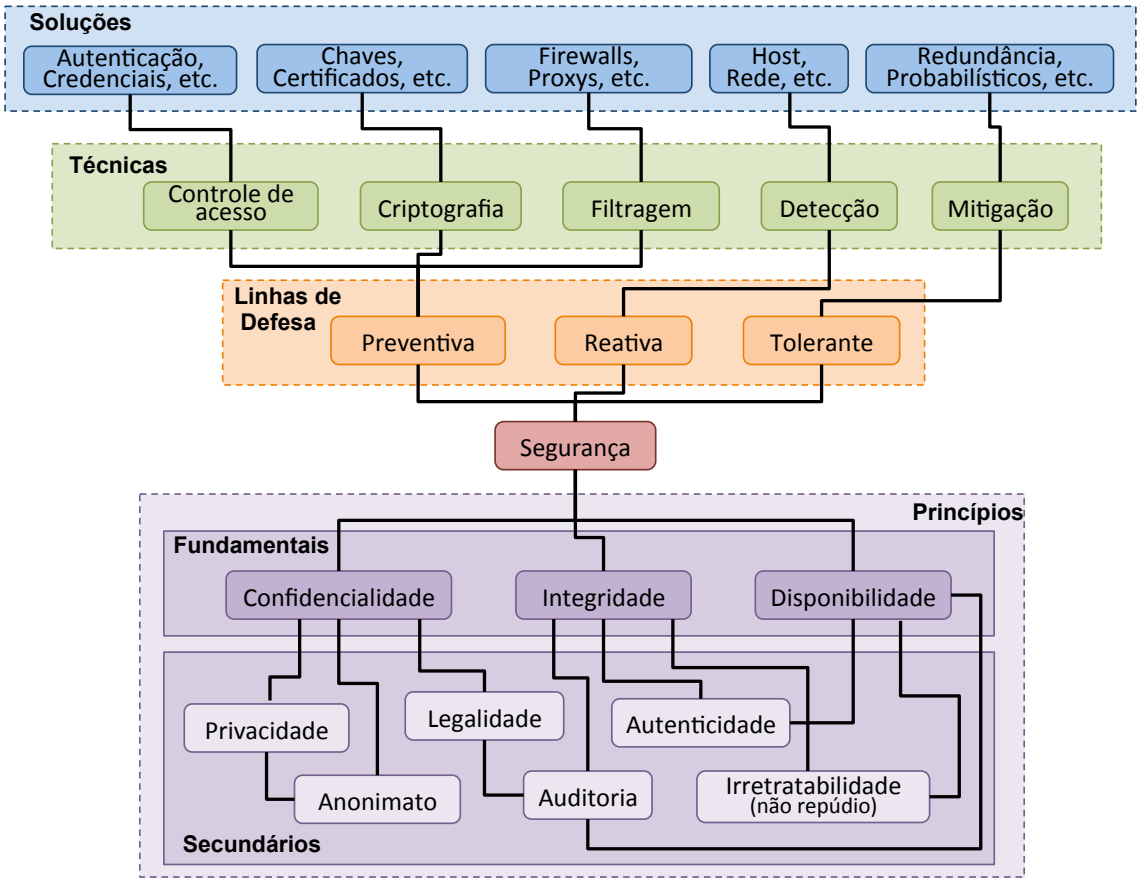


Figura 4.2: Taxonomia de segurança

disponibilidade compõem a auditoria, a mesma lógica é utilizada em outros princípios, como ilustrado pelas relações na Figura 4.2.

No outro lado da taxonomia estão as *Linhas de Defesa* classificadas como *Preventiva, Reativa e Tolerante* que são desenvolvidas para a proteção contra ataques e usuários maliciosos. Para a concepção das *Linhas de defesa* é necessária a utilização de diferentes *Técnicas* que garantam mecanismos de prevenção, reação e tolerância. Entre as técnicas de prevenção estão o *controle de acesso, a criptografia* e os *filtros de pacotes* que realizam análises prévias dos dados trafegados na rede. Dentre as técnicas de reação, a *detecção* é a principal, por onde se iniciam as ações de contramedidas. Para a linha de defesa tolerante, a *mitigação* representa a técnica em destaque.

As *Soluções* são implementadas a partir das técnicas para executar as ações da linha de defesa, e consequentemente satisfazer determinados requisitos dos princípios de segurança. Dentre as técnicas de controle de acesso estão as soluções com base em *autenticação, troca*

de credencias, etc. Para a criptografia existem as soluções com os *certificados digitais, troca de chaves pública-privada, dentre outras.* Para as técnicas de filtragem, existem as soluções de *Firewall, sniffers, proxys, etc.* Para as técnicas de detecção, consideram-se soluções com base nos *hosts, rede* ou soluções *híbridas.* Para as técnicas de mitigação, existem as soluções inspiradas na *redundância*, nas abordagens *probabilísticas e/ou bio-inspiradas.* Apesar de ampla, a taxonomia de segurança apresentada não é considerada exaustiva e novas *soluções, técnicas, linhas de defesa e princípios* podem ser adicionados. Com a definição da taxonomia, o processo de quantificação de segurança será facilitado, tendo em vista que a análise pode ser realizada em diferentes níveis para auxiliar na medição dos coeficientes de segurança.

4.4 Resumo

Este capítulo apresenta uma arquitetura para o gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas. Foram discutidas as asserções do sistema com as hipóteses levantadas e os objetivos da arquitetura. Também foram definidos os requisitos para uma conexão segura e contínua em redes de acesso, e foram detalhados os módulos, os componentes e as relações entre os módulos da arquitetura de gerenciamento de conectividade.

CAPÍTULO 5

INDICADOR DE RESILIÊNCIA DE CONECTIVIDADE EM REDES HETEROGÊNEAS

Esse capítulo apresenta o indicador de resiliência de conectividade em redes heterogêneas, utilizado para análise das condições de segurança das redes de acesso. A Seção 5.1 descreve a caracterização do ambiente de rede utilizado. A Seção 5.2 define a métrica de antifragilidade de conectividade usada como indicador das condições de segurança das redes de acesso. A Seção 5.3 apresenta a arquitetura de um sistema indicador de resiliência de conectividade em redes heterogêneas, bem como seu funcionamento. A Seção 5.4 mostra a avaliação do sistema, como também a descrição dos resultados e a Seção 5.5 apresenta um resumo do capítulo.

5.1 Caracterização do ambiente de rede

Esta seção descreve as premissas e definições de conectividade e dos enlaces críticos para redes heterogêneas sem fio. O sistema é caracterizado por uma rede heterogênea formada por diferentes tipos de tecnologias de comunicação. Os dispositivos que compõem a rede são móveis e migram suas conexões de uma rede para outra à medida que se movem. Os provedores de acesso de cada rede são fixos e possuem informações completas sobre a topologia de conectividade da rede. O modelo de conectividade da rede e a criticidade dos enlaces de comunicação são detalhados a seguir.

5.1.1 Modelo de conectividade da rede

A conectividade da rede consiste na existência de uma conexão, direta ou através de enlaces intermediários, entre quaisquer dois dispositivos na rede, independentemente 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 heterogênea sem fio, em que V corresponde a um conjunto finito de vértices que representam os dispositivos (nós) da rede, e E 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 incidente em u e $v \in V$. Logo, uma aresta entre u e v representa um enlace na rede entre os respectivos nós com comunicação em ambos os sentidos [78].

O grafo G' obtido a partir de G representa um instante qualquer t, em que a rede está conectada. Assim, em cada instante t, existe um grafo conexo para a topologia de conectividade da rede. Um grafo G' é dito conexo, se existe um *caminho* P_v^u para quaisquer $u, v \in V$. Logo, um caminho significa uma sequência de vértices tal que de cada um de seus vértices há uma aresta para o próximo vértice da sequência, assim 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 existe um P_v^u. Na rede, um *caminho* compreende uma conexão (rota) entre dois nós ligados diretamente ou através de nós intermédios, 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* $d(u, v)$. A *distância* entre dois nós na rede consiste no número de enlaces existentes na conexão, e o *caminho mínimo* corresponde a uma conexão com menor número de enlaces.

5.1.2 Modelo de enlaces críticos na rede

Um enlace crítico corresponde a 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 críticos, os quais são mais propícios a falhas de conectividade da rede, causando sua separação em pelo menos duas novas redes distintas. 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, 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 de P_v^u em T_C é um $mincut_v^u$ de G'. Para a rede, T_C significa uma subrede 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* auxilia na identificação de pontos de vulnerabilidades de enlaces na rede [79].

5.2 Antifragilidade de conectividade

Esta seção apresenta a métrica *antifragilidade de conectividade* (AC). Essa métrica permite avaliar o nível de criticidade de conexões de uma rede sob interrupções. Por criticidade, considere a probabilidade de desconexão resultante de interrupções causadas por ataques, falhas, acidentes ou situações inesperadas. Esta métrica fornece informações para ajudar os dispositivos em transição por redes heterogêneas a escolher a melhor rede de acesso em áreas de sobreposição, além de possibilitar a rede a "aprender"com as suas condições e estar preparada para lidar com elas de modo autônomo.

A métrica tem como base o conceito de *antifragility* que vai além da capacidade de resiliência e robustez, promovendo a autoaprendizagem e auto-adaptação, suportando falhas e aplicando mecanismos de baixo custo capazes de resolvê-las [80]. A antifragilidade tem como premissa que todos os sistemas estão sujeitos a falhas em maior ou menor escala e em vez de criar somente soluções para evita-las são necessárias soluções para aprender com as falhas e evoluir. A antifragilidade da rede implica na capacidade de aprender

com as condições prévias e adaptar-se proativamente contra falhas, ataques e eventos indesejados ou inesperados, independente de serem maliciosos ou não.

A métrica de antifragilidade de conectividade foi concebida para possibilitar a identificação das conexões mais vulneráveis e quantificar a robustez e segurança da rede. Esta métrica permite a quantificação de um índice de fragilidade da conectividade de redes heterogêneas e também seu grau de robustez. Deste modo, as técnicas de *árvore de corte mínimo* e *coeficiente de agrupamento* (clusterização) foram empregadas em sua composição. Essas duas técnicas fornecem informações de conectividade da rede e agrupamento entre os dispositivos, possibilitando calcular um índice geral das condições de conectividade da rede.

Se aplicada parcialmente, a métrica AC pode identificar as conexões mais frágeis da rede usando um algoritmo de árvores de corte mínimo. A métrica também pode avaliar a redundância de rotas através de conexões entre os dispositivos por meio do coeficiente de agrupamento. Essas medidas permitem a rede prever e adaptar suas condições de conectividade.

Fragilidade da rede

A fragilidade da rede (NF) está diretamente relacionada com a vulnerabilidade à falhas 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 desconectá-lo. 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 de um dispositivo da rede.

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 T_C. Os pesos W_c correspondem a todos os cortes mínimos $mincut_v^u$ entre todos os pares de vértices u, v de T_C. O $mincut_v^u$ representa o menor número de enlaces entre u, v que, se removidos,

desconectam o grafo T_C.

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 [81] [82], a fragilidade da rede é obtida por uma relação entre o menor e o maior número de enlaces expostos a perturbações na rede. 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 5.1. 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*.

$$NF = \frac{min\{w \mid \forall\ w \in W_c\}}{max\{w \mid \forall\ w \in W_c\}} \tag{5.1}$$

Robustez da rede

A existência de rotas redundantes representa a robustez de conectividade da rede (NR). 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 existentes 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 entre ambos. O grau de v corresponde à quantidade 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 d_v o número real de arestas que v possui, o seu número real de vizinhos, o coeficiente de agrupamento de v é definido pela Equação 5.2. 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.

$$C_v = \frac{E_v}{B} = \frac{2 \cdot d_v}{d_v \cdot (d_v - 1)} = \frac{2}{d_v - 1} \tag{5.2}$$

O coeficiente de agrupamento local C_v dos vértices possibilita calcular um valor global para a rede toda, C_{Global}. Neste caso, C_{Global} é definido como o menor C_v entre todos os vértices de G', como mostrado na Equação 5.3.

$$C_{Global} = min\{C_v \mid \forall\ v \in V_{G'}\} \tag{5.3}$$

Os valores de C_{Global} e C_v permitem calcular o valor da NR, denotada pela Equação 5.4. Esta medida incide sobre os enlaces e os nós mais frágeis da rede. 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.

$$NR = \frac{C_{Global}}{max\{C_v \mid \forall\ v \in CV\}} \tag{5.4}$$

Correlação da fragilidade e robustez na antifragilidade

As medidas auxiliares NF e NR obtidas respectivamente pelo uso das técnicas de *árvore de corte mínimo* e *coeficiente de agrupamento* complementam-se na composição da métrica de *antifragilidade de conectividade* (AC). A primeira medida, NF indica e quantifica as conexões mais vulneráveis na rede por meio do processamento de T_C e W_c. Já a segunda, NR calcula a robustez dos vértices mais vulneráveis e de sua vizinhança através de C_v e C_{Global}. A utilização destas duas medidas combinadas permite localizar os enlaces mais frágeis na rede e posteriormente identificar e quantificar a existência de rotas alternativas entre os nós presentes nos enlaces considerados críticos.

A quantificação e localização dos enlaces críticos, que (se removidos) podem desconectar a rede, é fundamental para o desenvolvimento de contramedidas para a prevenção e resiliência à falhas na conectividade da rede. Já a descoberta de enlaces alternativos entre os nós críticos permite a criação de ações proativas que evitem a interrupção no

oferecimento dos serviços da rede. A fim de aproveitar esses dois tipos de conhecimento, a métrica *antifragilidade de conectividade*, definida pela Equação 5.5 é apresentada.

$$AC = 1 - (\alpha \times NF + \beta \times NR) \tag{5.5}$$

Diferentes obras na literatura [83, 84, 85, 86] utilizam técnicas para a atribuição de pesos de importância dado a cada medida utilizada na composição de suas métricas. Neste trabalho, foi utilizado as variáveis α e β para representar o peso de importância dado a NF e NR, medidas usadas na composição da *antifragilidade de conectividade*. Como NF representa o ponto de partida para toda a análise posterior, esta medida tem um impacto maior no cálculo do nível de antifragilidade das conexões. A fragilidade da rede indica os enlaces mais vulneráveis, e com base nesta medida, a ligação entre os nós fornecida pelo relacionamento entre seus vizinhos pode ser calculado. Assim, o valor de α que representa o peso de importância atribuído à NF tende a ter sempre maior valor do que β, que corresponde ao peso de importância dado a NR. Assim, $\beta = 1 - \alpha$ e $\alpha + \beta = 1$

5.3 Sistema indicador de resiliência em redes heterogêneas

As redes heterogêneas possuem topologias de conectividade dinâmicas devido às frequentes conexões e desconexões de dispositivos móveis em trânsito, e pelo uso de diferentes tipos de tecnologias de comunicação. A análise da disponibilidade de conectividade dessas redes ainda representa desafios a serem superados. A análise da antifragilidade de conectividade de redes heterogêneas tem como base uma estratégia temporal. Assim, a cada instante uma observação das condições de conectividade deve ser realizada. Esta abordagem permite uma avaliação aproximada das condições reais da rede com base em seu histórico de dinamicidade.

O sistema indicador de resiliência na conectividade das redes heterogêneas sem fio calcula os índices de antifragilidade e indica quais redes são momentaneamente mais seguras em termos de disponibilidade de conectividade. Essa abordagem possibilita a escolha adequada do acesso em um ambiente sobreposto por inúmeras redes heterogêneas sem fio.

Além disso, esse indicador auxilia na definição de estratégias e contramedidas a serem desenvolvidas para prover princípios de resiliência e segurança à rede e aos dispositivos móveis em trânsito.

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, fornece um índice de fragilidade e robustez da conectividade de cada uma das redes disponíveis, e a partir desses valores processa o coeficiente de antifragilidade de conectividade dessas redes. Para realização destas operações o sistema possui dois módulos: *Regra de Condição* e *Regra de Aferição*, conforme ilustrado na Figura 5.1.

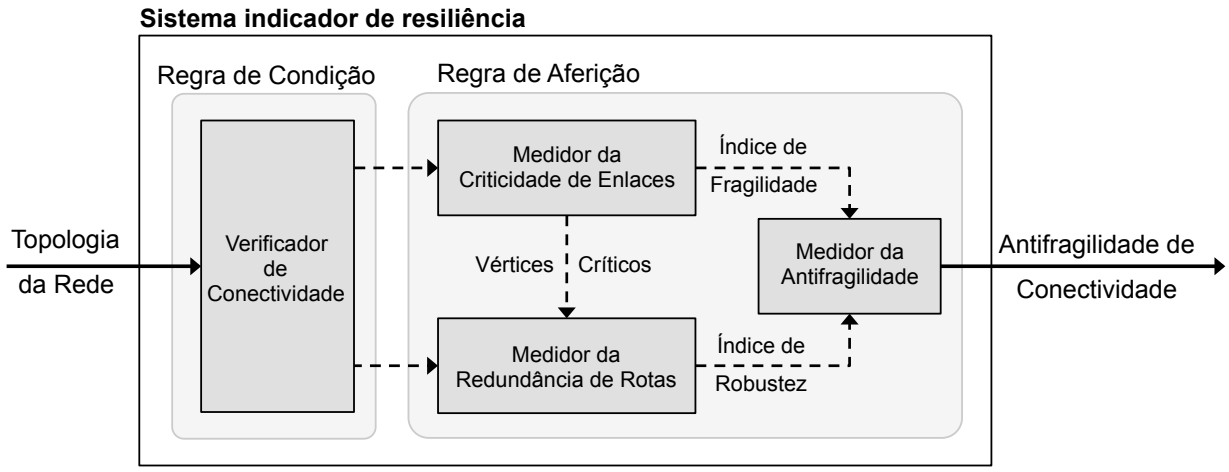


Figura 5.1: Arquitetura do sistema indicador de resiliência

O Módulo *Regra de Condição* compreende o componente *Verificador de Conectividade* que 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. Na sequência, o grafo de conectividade é encaminhado para o módulo *Regra de Aferição*.

O Módulo *Regra de Aferição*, responsável pelo cálculo do coeficiente de antifragilidade da rede compreende três componentes: *Medidor de Criticidade de Enlaces*, *Medidor de Redundância de Rotas* e *Medidor da Antifragilidade*. O componente *Medidor de Criticidade de Enlaces* recebe o grafo de conectividade e calcula os enlaces críticos, aqueles que

se removidos são capazes de desconectar a rede. A partir desta informação também é determinado o conjunto de vértices críticos, aqueles presentes nos enlaces críticos. Esses enlaces são referência para o cálculo do índice de *Fragilidade de Conectividade da Rede* ou apenas *Fragilidade da Rede* (NF).

O componente *Medidor de Redundância de Rotas* utiliza o grafo de conectividade da rede e o conjunto de vértices críticos processados pelo *Medidor de Criticidade de Enlaces* para verificar a existência de enlaces entres os vizinhos de um nó. A identificação destes enlaces permite descobrir a *cliques de tamanho 3* no grafo, o que representa a existência de uma rota alternativa entre esses vértices. O resultado desta análise é utilizado para calcular o índice de *Robustez de Conectividade da Rede* ou simplesmente *Robustez da Rede* (NR). O *Medidor de Antifragilidade* consiste do último componente do módulo *Regra de Aferição* e utiliza a combinação dos resultados da *Fragilidade da Rede* e *Robustez da Rede* como medidas parciais para calcular o coeficiente de *Antifragilidade de Conectividade da Rede* ou simplesmente *Antifragilidade de Conectividade* (AC).

5.3.1 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 5.2. Antes de se conectar em qualquer uma das redes o sistema indicador avalia as condições de conectividade indicando os índices antifragilidade de ambas as redes. Com esse indicador o usuário pode se conectar na rede mais segura em termos de disponibilidade de conectividade.

O sistema indicador inicia sua operação a partir 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 módulo *Regra de Condição* por meio do 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 5.3(a) ilustra o grafo de conectividade da "Rede A".

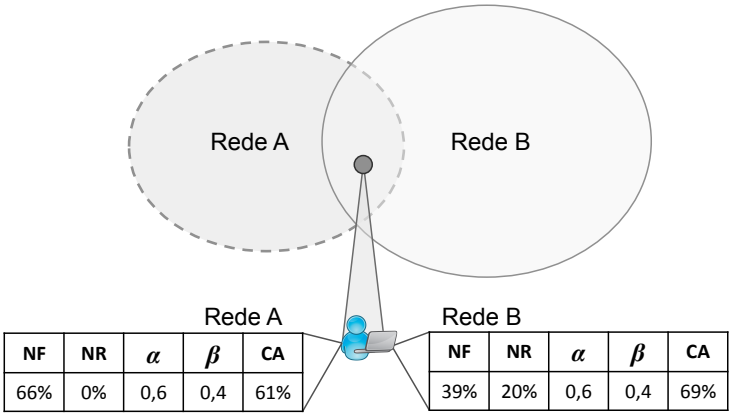


Figura 5.2: Cenário de funcionamento do sistema indicador de resiliência

O módulo *Regra de Aferição* através do componente *Medidor de Criticidade de Enlaces* recebe o grafo de conectividade e identifica o conjunto de enlaces críticos através de uma árvore de cortes mínimos. Neste trabalho, a árvore de cortes mínimos é obtida por meio do algoritmo de Gomory-Hu [87]. O algoritmo de Gomory-Hu tem como entrada um grafo da topologia de conectividade e retorna uma árvore de cortes mínimos. A árvore de corte mínimo T_C e o conjunto de pesos W_c, obtidos com o algoritmo são construídos com a computação de $|V| - 1$ cortes mínimos [79].

A Figura 5.3(a) mostra um grafo G' que representa uma topologia de conectividade da "Rede A" em um instante t. A Figura 5.3(b) ilustra uma árvore de corte mínimo T_C extraído do grafo G' e seus pesos w representam a quantidade de arestas, entre os vértices indicados, que são necessários para desconectar G'. Por exemplo, T_C ilustrada pela Figura 5.3(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.

Na Figura 5.3(b), nas arestas de T_C, o peso w mínimo corresponde 2 e o máximo 3, para todo conjunto W_c. Assim, usando a Equação 5.1, 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 5.3(c) pelas linhas tracejadas. Logo, os vértices conectados por enlaces críticos são denominados como vértices

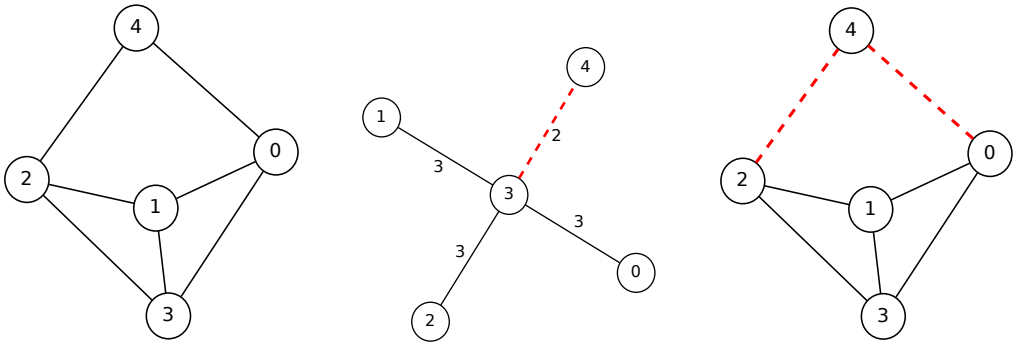


Figura 5.3: Análise de fragilidade

críticos. Na Figura 5.3(c), os vértices críticos são 4, 2 e 0.

Em paralelo à operação realizada pelo componente *Medidor de Criticidade de Enlaces*, o componente *Medidor de Redundância de Rotas* também é executado. Esse componente calcula o coeficiente de agrupamento dos vértices do grafo de conectividade da rede G‘ para a obtenção do índice de robustez. A Figura 5.4(a) mostra o coeficiente de agrupamento local C_v calculado para cada vértice e a Figura 5.4(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 vértices V do grafo G', o valor de C_{global} para a rede exemplificada pela Figura 5.4(a) corresponde a 0,0. Deste modo, utilizando a Equação 5.4, 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 é 0,0, e indica o índice de robustez da rede.

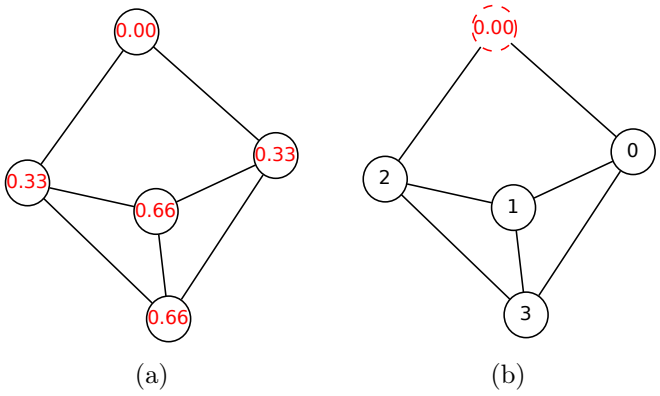


Figura 5.4: Análise de robustez

O componente *Medidor de Antifragilidade* recebe os valores dos índices de fragilidade

e robustez da rede e calcula o valor da antifragilidade através da Equação **??**. 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 da antifragilidade de cada rede o dispositivo móvel em transição poderá se conectar na rede de acesso mais segura em termos de disponibilidade de conectividade. Além disso, uma avaliação momentânea das condições de conectividade da rede ajuda a evitar que os dispositivos móveis em transição se conectem em redes de acesso comprometidas e tenham 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.

5.4 Análise do sistema indicador de resiliência de conectividade

Esta seção apresenta uma avaliação da eficácia do sistema indicador de resiliência, por meio da métrica de *antifragilidade de conectividade*. Foram realizados dois estudos de caso para a avaliação. O primeiro estudo analisa uma rede *mesh* de tecnologias heterogêneas e topologia dinâmica e o segundo estudo considera uma rede *celular 3G* de tecnologias de transmissão heterogêneas, topologia estática e diferentes operadoras de serviço.

5.4.1 Metodologia e avaliação em redes de topologia dinâmica

A análise do sistema indicador de resiliência em redes de topologia dinâmica foi realizada utilizando traços reais da rede *mesh* do projeto *UCSB MeshNet* da Universidade da Califórnia em Santa Barbara, nos Estados Unidos. A rede é composta por 19 nós que operam nos padrões *802.11a/b*, criando uma rede heterogênea em termos de seus padrões de comunicação [88]. Os dispositivos móveis conectados na rede fazem transições de suas conexões durante a sua mobilidade pela área de cobertura, mudando constantemente a topologia de conectividade da rede. Os dados utilizados resultaram de testes realizados em 2007 e foram disponibilizados no repositório web CRAWDAD[1].

[1]http://crawdad.cs.dartmouth.edu/meta.php?name=ucsb/meshnet

A base de dados é formada por 900 arquivos contendo as listas de adjacências da topologia da rede. Cada arquivo representa um instante com as condições de conectividade da rede. Com o objetivo de avaliar apenas os instantes em que a rede era conexa, foram subtraídos 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, 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 conectividade da rede, a Figura 5.5 ilustra seis topologias da mesma rede em diferentes instantes t.

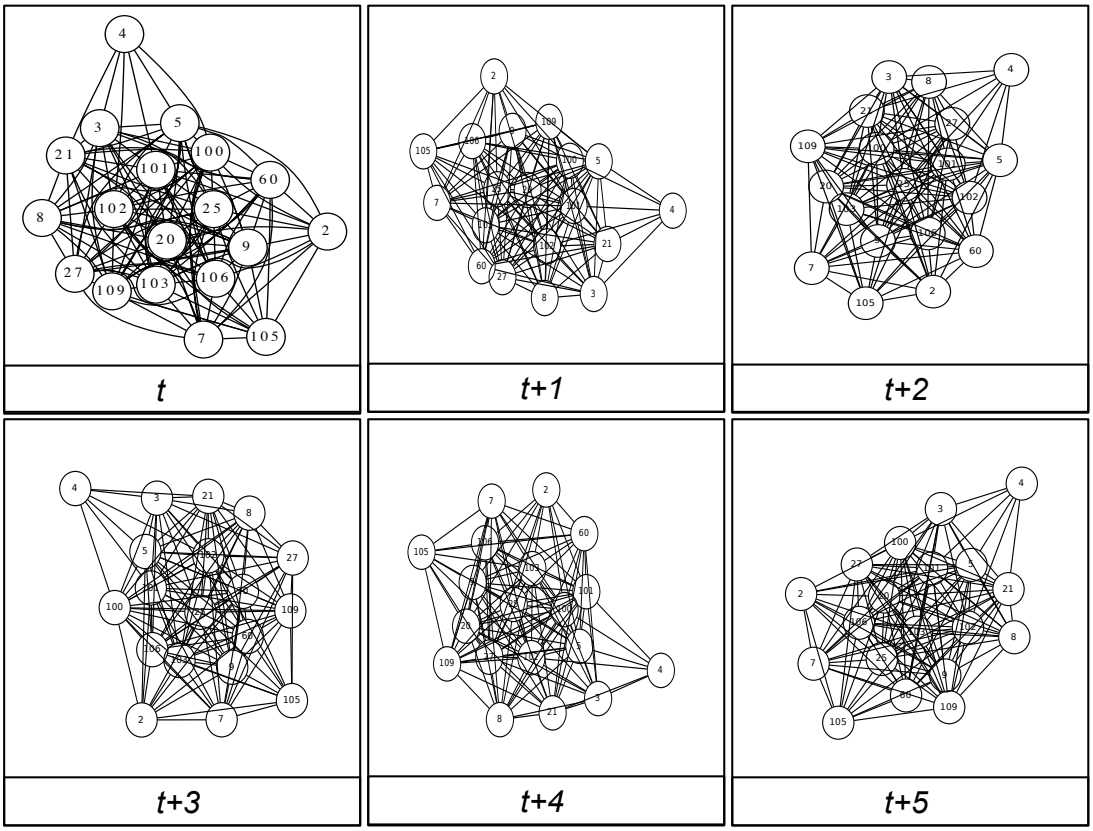


Figura 5.5: Exemplos de grafos de conectividade da rede em diferentes instantes

A partir do grafo de conectividade é possível definir uma estrutura de dados para operação do componente *Medidor de Criticidade de Enlace* calcular o índice de fragilidade da rede, através da execução do algoritmo de árvores de cortes mínimos de *Gomory-Hu* [87]. O componente *Medidor de Redundância Rotas* processa o índice de robustez através do 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 [89]. 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 para a biblioteca LEMON e nessa etapa as informações necessárias são coletadas para o cálculo do coeficiente de agrupamento. Na etapa seguinte o algoritmo de *Gomory-Hu* é executado e o coeficiente de agrupamento é calculado. A partir do algoritmo, os cortes mínimos são calculados. Na última etapa o valor de Antifragilidade da rede é processado e o script organiza esses dados em uma tabela para análise futura.

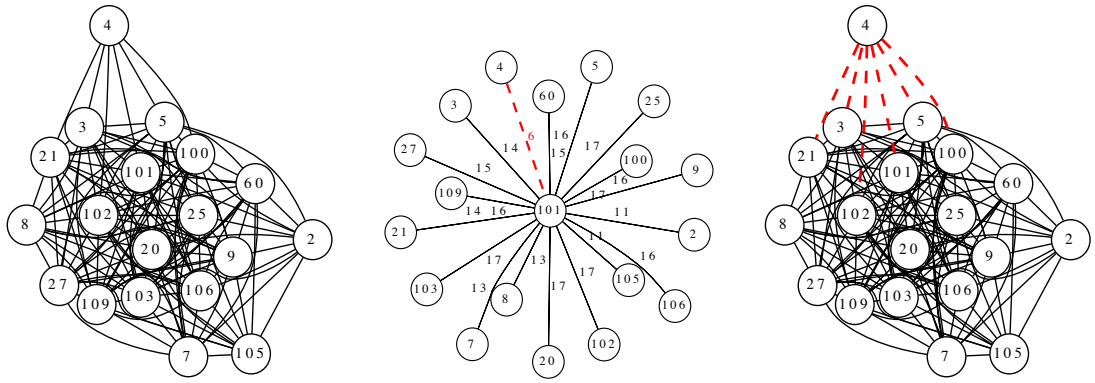
5.4.2 Descrição dos resultados

Os resultados apresentados e discutidos com base na avaliação da fragilidade, robustez e antifragilidade da conectividade da rede, obtidos pelo sistema indicador de resiliência para redes heterogêneas.

Avaliação da fragilidade

A *fragilidade alta* consiste na menor quantidade de enlaces necessária para a desconexão da rede. 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 5.6(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 5.6(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 que desconectam a rede, realizamos a identificação e a localização destas arestas no grafo original, indicadas pelas linhas tracejadas na Figura 5.6(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.

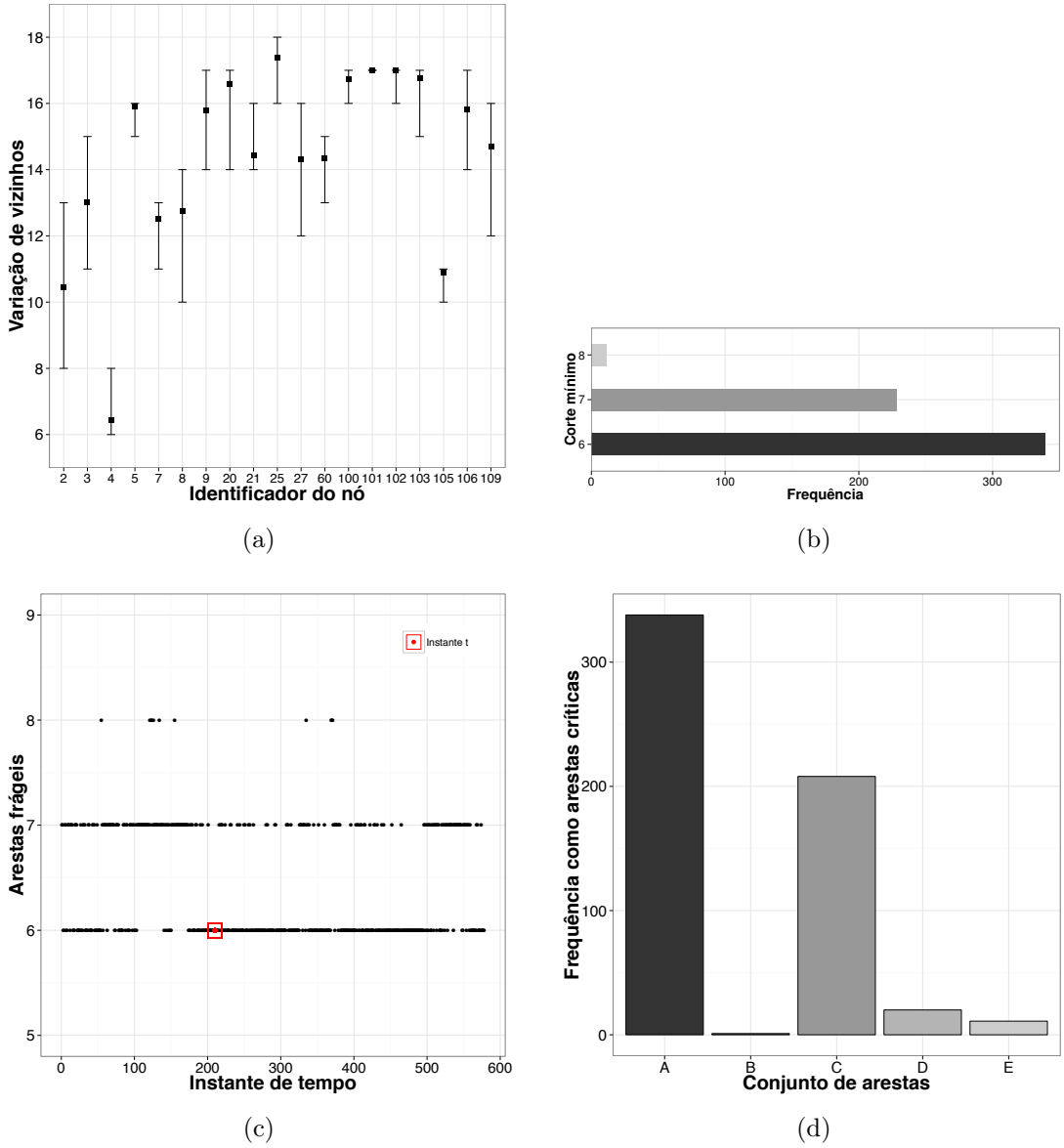


(a) (b) (c)

Figura 5.6: 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 globais da rede para todo seu período de funcionamento. A Figura 5.7(a) ilustra a variação (mínimo, média e máximo) da quantidade de vizinhos de cada nó em todos os instantes da rede, o que mostra a dinamicidade durante seu funcionamento. Pelos resultados verifica-se que o nó 25 tem o maior número de vizinhos, e nó 4 o menor.

A Figura 5.7(b) mostra o número de arestas críticas identificadas na rede durante todos os instantes de funcionamento. A Figura 5.7(c) apresenta a variação do número de arestas críticas. 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.



(a) (b)

(c) (d)

Figura 5.7: Avaliação da fragilidade

A existência de enlaces específicos que constantemente estão presentes no grupo de *fragilidade alta* é outro ponto evidenciado pelos resultados. Isto indica que estes enlaces podem ser considerados os mais críticos da rede, como ilustra o conjunto A da Figura 5.7(d). A Tabela 5.1 correlaciona os enlaces de fragilidade alta com os respectivos conjuntos frágeis mais frequentes em todos os instantes de funcionamento 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

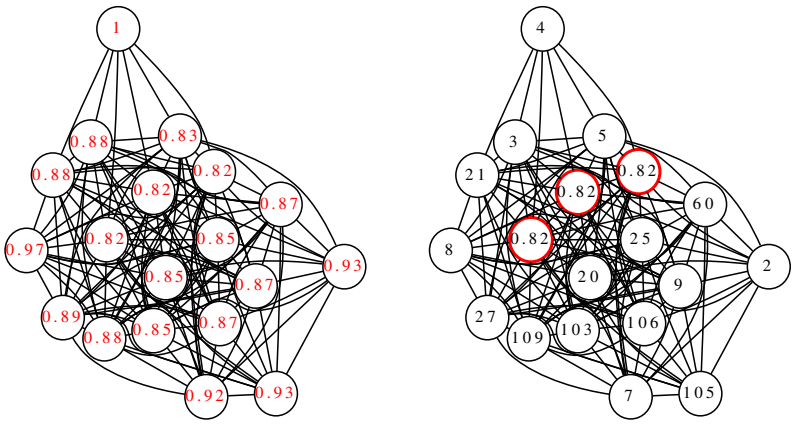
Tabela 5.1: Descrição do conjunto de arestas da Figura5.7(d).

Avaliação da robustez

A robustez foi calculada de forma local através do número de conexões entre os vizinhos de um nó. A forma global para toda a rede é obtida pelo menor valor local entre todos os valores encontrados na rede. A robustez da conectividade da rede é determinada pela relação entre o índice global e o maior índice local, como definido na Equação 5.3. Deste modo, nenhum nó frágil será ocultado pela média do coeficiente de agrupamento. Essa estratégia foi adotada com base no conceito de que nunca deve-se considerar uma corrente mais forte do que seu elo mais fraco [81] [82].

Dado um determinado instante t de conectividade da rede ilustrado pela Figura 5.6(a), foi calculado os valores dos coeficientes de agrupamento locais, como observado na Figura 5.8(a), em que os valores de cada nó representam seu índice de robustez local. Como o agrupamento global da rede é representado pelo menor índice local, a Figura 5.8(b) ilustra o grafo de conectividade da rede no instante t com o nó que determina o valor do coeficiente de agrupamento global. Como visto na Figura 5.8(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 uma avaliação do instant t, uma análise geral para todo o período de funcionamento da rede foi feita, a fim de identificar a variação dos valores do coeficiente de agrupamento de cada dispositivo, bem como da rede. Essa avaliação geral permite mensurar a robustez em razão da dinamicidade da rede. A Figura 5.9(a) mostra a variação (média, mediana, quartis) do coeficiente de agrupamento local C_v para cada nó ao longo de todos 577 instantes de observação da rede. Os resultados mostram que o dispositivo 4 se mantém constante durante todos os momentos de observação da rede. O valor do

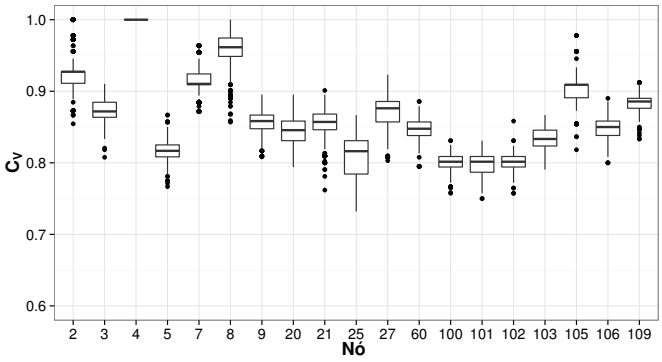


(a) (b)

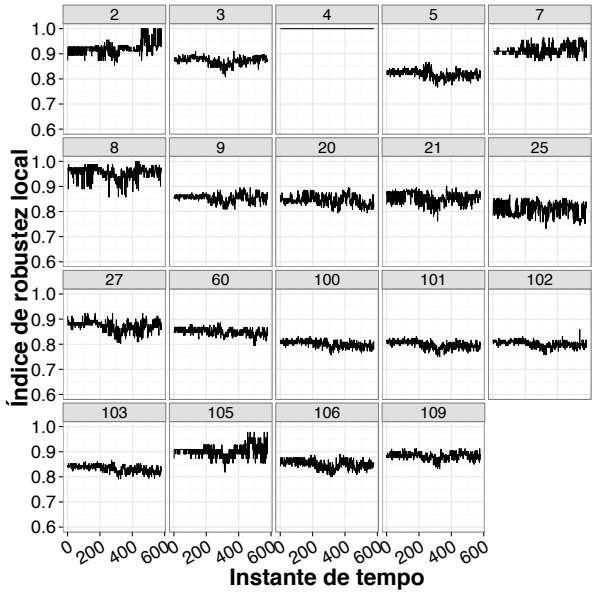
Figura 5.8: Análise de agrupamento da rede

coeficiente de agrupamento local C_v para esse dispositivo se mantém igual a 1,0, o que indica a existência de completa conexão entre seus vizinhos, fornecendo rotas alternativas para alcançá-los. A Figura 5.9(b) mostra o comportamento do coeficiente de agrupamento de cada dispositivo durante o funcionamento da rede. A Figura 5.9(c) mostra a variação do valor do coeficiente de agrupamento global C_{Global} para a rede. Os resultados indicam uma variação dos valores de C_{Global}, que vão de 0,65 a 0,85. O ponto em destaque na figura indica o instante t utilizado nos exemplos apresentados na análise do coeficientes de agrupamento.

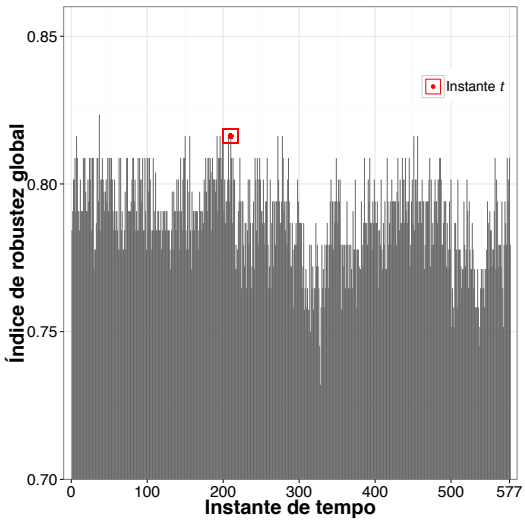
Os resultados das análises também permitem identificar os nós com os menores valores de C_V e que consequentemente determinam o valor de C_{Global} da rede por mais vezes. Os nós com identificadores 25, 100, 101 e 102 determinam com maior frequência o valor de C_{Global} da rede durante todo seu funcionamento. O nó 101 corresponde ao nó que mais vezes define o valor de C_{Global}. A Figura 5.9(d) mostra a frequência com que cada nó determina o valor de C_{Global}. O nó 101 representou mais de 300 vezes o valor do coeficiente de agrupamento global da rede C_{Global}. Esse resultado confirma que este nó corresponde ao dispositivo menos robusto da rede, de modo que a conectividade entre seus vizinhos é baixa em relação aos outros dispositivos.



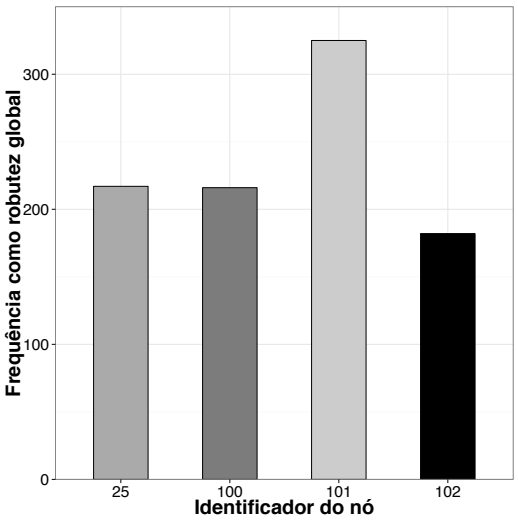
(a)



(b)



(c)



(d)

Figura 5.9: Avaliação da robustez

Avaliação da antifragilidade

A métrica de antifragilidade de conectividade é calculada a partir dos valores dos índices de fragilidade e robustez da rede. A Figura 5.10 ilustra os valores das medidas auxiliares NF e NR para os 577 instantes, que correspondem às diferentes condições de conectividade da rede. Rotulamos o tempo variando de 0-600 instantes. Os valores de NF variam entre 0,3 e 0,45, o que corresponde a um índice de fragilidade entre 30% e 45% sobre a conectividade da rede. Os valores de NR oscilam entre 0,75 e 0,85. Estes resultados indicam que os vértices críticos apresentam uma elevada ligação entre os seus vizinhos.

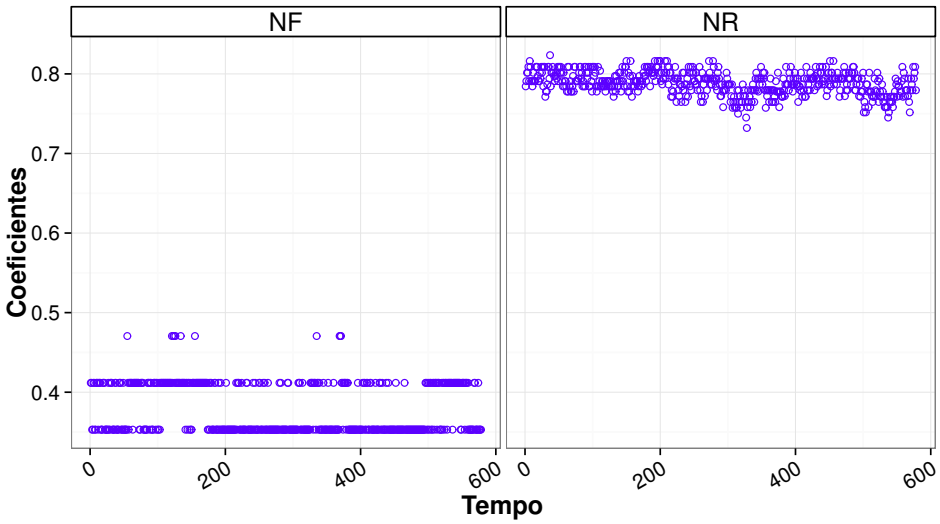


Figura 5.10: Valores de NF e NR para os diferentes instantes da rede

A Figura 5.11 ilustra os resultados do cálculo da antifragilidade de conectividade da rede MeshNet. Os resultados consideram uma variação dos valores dos pesos de importância α e β. O valor de NF indica o nível de fragilidade da rede a partir dos enlaces mais críticos. Esta medida tem um impacto maior sobre o cálculo da antifragilidade. Foi realizada uma variação dos pesos de importância de modo que o valor de α é sempre maior do que β, contudo, $\alpha + \beta = 1$.

Para um dos casos extremos o valor de $\alpha = 0,6$ e $\beta = 0,4$, AC varia entre 0,4 e 0,5. Já para o outro caso em que o valor de $\alpha = 0,9$ e $\beta = 0,1$, observa-se uma oscilação no valor de AC entre 0,5 e 0,6. Os resultados obtidos correspondem à análise realizada para todos os instantes de funcionamento da rede. A partir desses resultados, observa-se que

os valores de α e β têm uma forte influência sobre a antifragilidade de conectividade.

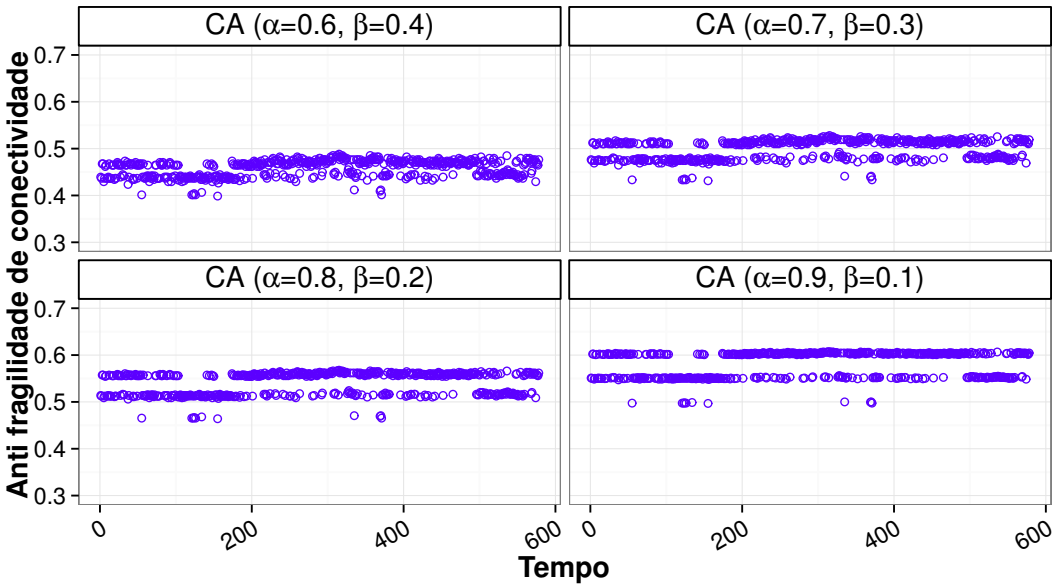


Figura 5.11: Antifragilidade de conectividade em redes mesh heterogêneas

Foi verificado que a métrica pode indicar individualmente as ligações mais vulneráveis na rede, e em vez de usar essa informação como medida absoluta, a métrica de antifragilidade de conectividade também pondera a existência de ligações entre os nós críticos e seus vizinhos.

5.4.3 Metodologia e avaliação em redes de topologia estática

Esta seção apresenta a segunda avaliação da eficácia do sistema indicador de resiliência na conectividade em rede celular heterogênea de topologia estática. Neste estudo, o sistema utilizou traços reais da rede celular da cidade de Curitiba-PR para a avaliação das condições de conectividade. Os traços estão disponíveis em um repositório público[2] mantido pela Agência Nacional de Telecomunicações (ANATEL) e são referentes ao segundo semestre de 2013. Os arquivos de traços contém uma lista de coordenadas de latitude e longitude de cada Estação Rádio Base (ERB).

A rede celular é composta de 191 ERBs espalhadas na cidade, e cinco operadores diferentes oferecem seus serviços. Cada operadora emprega diferentes tecnologias de comunicação, tais como 3G e 4G para oferecer serviços a seus usuários, caracterizando a

[2]http://sistemas.anatel.gov.br/stel/consultas/ListaEstacoesLocalidade/tela.asp?pNumServico=010

heterogeneidade da rede. Diferente da primeira avaliação, essa rede não possui um topologia de conectividade dinâmica, em razão dos pontos provedores de acesso serem fixos. Deste modo, a rede se caracteriza com topologia de conectividade estática.

A Figura 5.12 mostra o mapa da cidade com a rede formada pelas ERBs das diferentes operadoras. As diferentes ERBs empregam tecnologias heterogêneas no oferecimento de seus serviços, resultando em diferentes áreas de cobertura. No entanto, neste estudo, foi investigado um cenário em que todas as ERBs têm o mesmo raio de transmissão de 2 km, sem perder a generalização dos resultados e considerando a sua área de cobertura modelada por um círculo. A localização precisa de cada ERB é indicada na figura pela marca vermelha, e círculos coloridos representam sua área de cobertura de transmissão. Cada cor representa uma ERB de uma operador de serviço que pode operar com diferentes tecnologias.

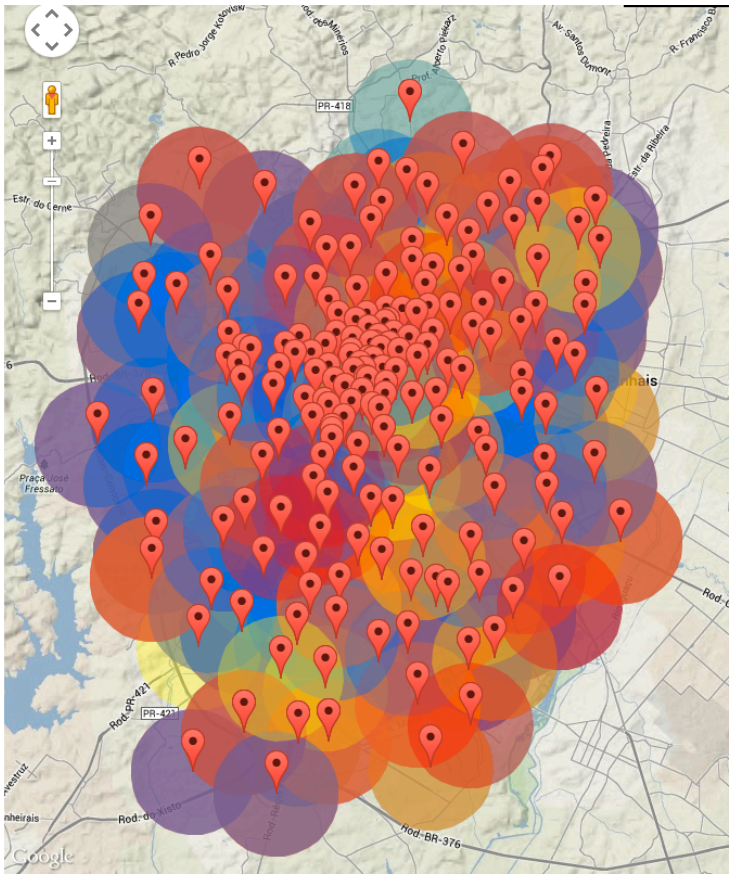


Figura 5.12: ERBs distribuídos na cidade de Curitiba-PR

A rede de telefonia celular foi modelada como um grafo não direcionado, tendo como

base a localização das ERBs e suas áreas de cobertura. Deste modo, as ERBs representam os vértices e as interseções entre suas áreas de cobertura correspondem às arestas. Diferente do primeiro estudo da avaliação da eficácia do sistema indicador resiliência, o grafo que representa a rede é o mesmo para os diferentes instantes t, uma vez que as ERBs são fixas. A Figura 5.13 ilustra o grafo correspondente à rede e a Figura 5.14 mostra a densidade de ERBs pela área da cidade. Nesta figura observa-se a alta densidade no centro, representado na figura pela região mais escura.

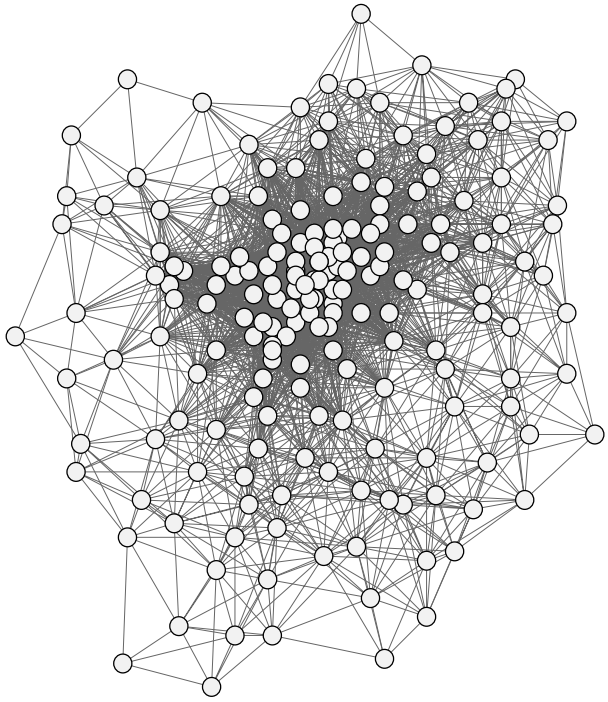


Figura 5.13: Grafo das ERBs da rede celular de Curitiba-PR

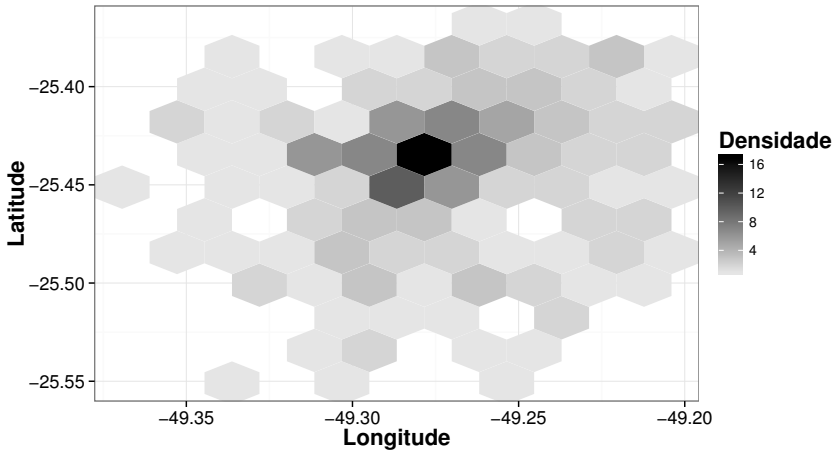


Figura 5.14: Densidade dos nós no perímetro da cidade

5.4.4 Descrição dos resultados

Essa seção apresenta os resultados obtidos com o sistema indicador de resiliência aplicado na rede celular. Esses resultados consideram o mesmo modo de avaliação realizada no primeiro estudo de caso. Os resultados são apresentados e discutidos com base na avaliação da fragilidade, robustez e antifragilidade da conectividade da rede.

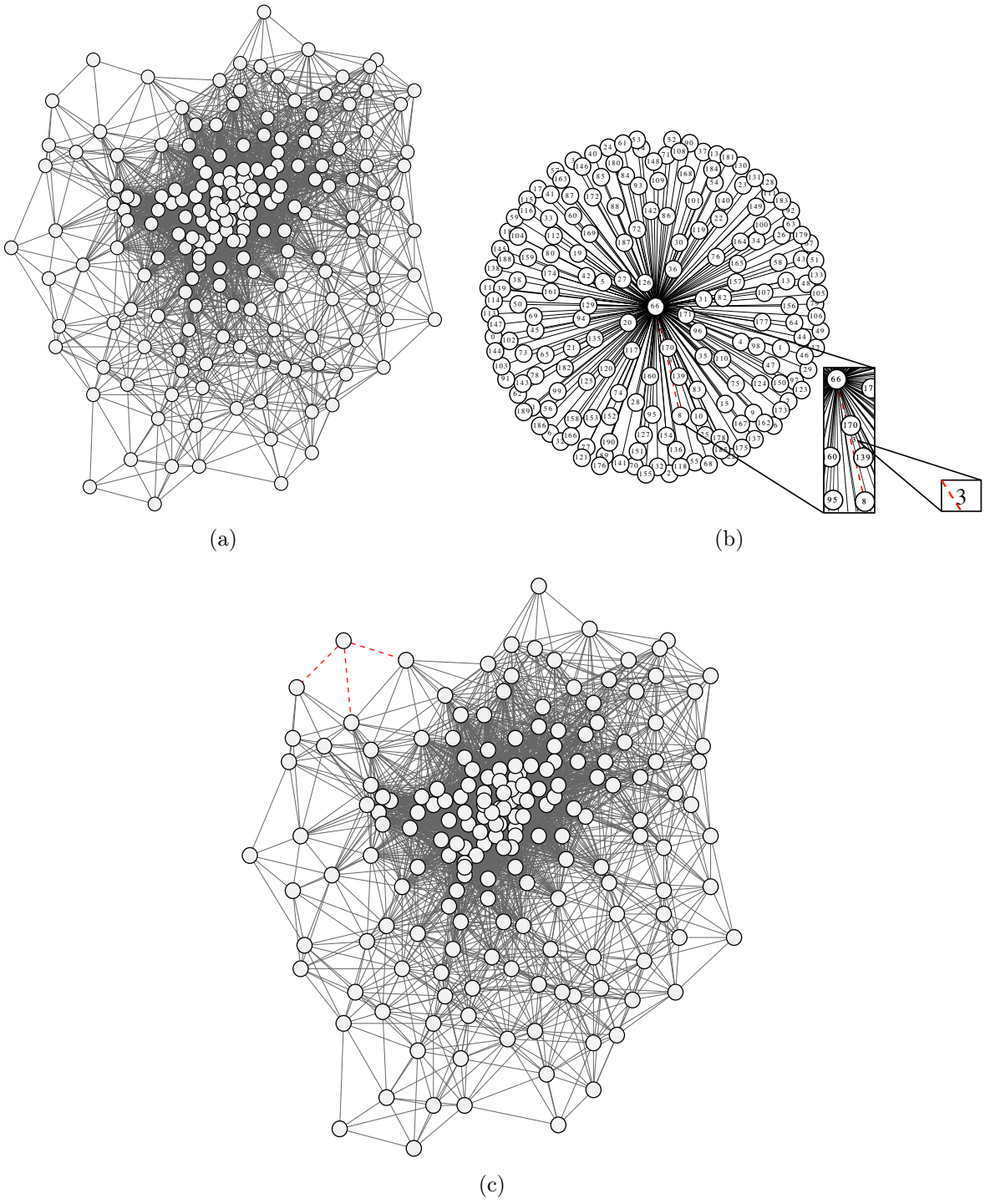
Avaliação da fragilidade

A Figura 5.15(a) ilustra o grafo de conectividade da rede celular de topologia estática e a Figura 5.15(b) mostra a árvore de corte mínimo T_C, calculada para o grafo. A parte ampliada desta figura ilustra o menor valor de corte mínimo da árvore T_C, esse resultado indica que o número de arestas críticas identificados corresponde a 3. Essas arestas são ilustradas pelas ligações tracejadas no grafo da Figura 5.15(c). Esses resultados indicam que, apesar da grande quantidade de arestas existente no grafo, um número pequeno de arestas removidas é capaz de desconectá-lo.

Avaliação da robustez

A Figura 5.16 mostra a distribuição de graus dos vértices para o grafo da rede celular. Esse dado indica a disposição dos vizinhos dos dispositivos na rede, determinando a quantidade de enlaces de cada nó. Os graus dos vértices do grafo variam de 3 a 80 arestas e a média corresponde a 58,19. O comportamento dos graus dos vértices foi ajustado por uma distribuição de densidade de probabilidade de *Poisson e de Bernoulli* com μ igual a 1,91. O comportamento observado mostra uma pequena quantidade de vértices com um grau elevado e uma grande quantidade de vértices com um grau baixo. Esta distribuição de graus corresponde à mesma encontrada em diferentes redes complexas, incluindo a distribuição de graus do núcleo da topologia da Internet [90].

O gráfico da Figura 5.16 mostra a grande concentração de conexões com uma pequena quantidade de nós, e também confirma a existência de maior número de arestas críticas na periferia da rede e não no núcleo.



(a) (b)

(c)

Figura 5.15: Avaliação da fragilidade

Avaliação da antifragilidade

A antifragilidade de conectividade da rede é calculada a partir das medidas auxiliares da fragilidade e robustez. A Tabela 5.2 mostra os valores das medidas auxiliares NF, NR, assim como o índice de agrupamento e menor corte mínimo calculados para o grafo de

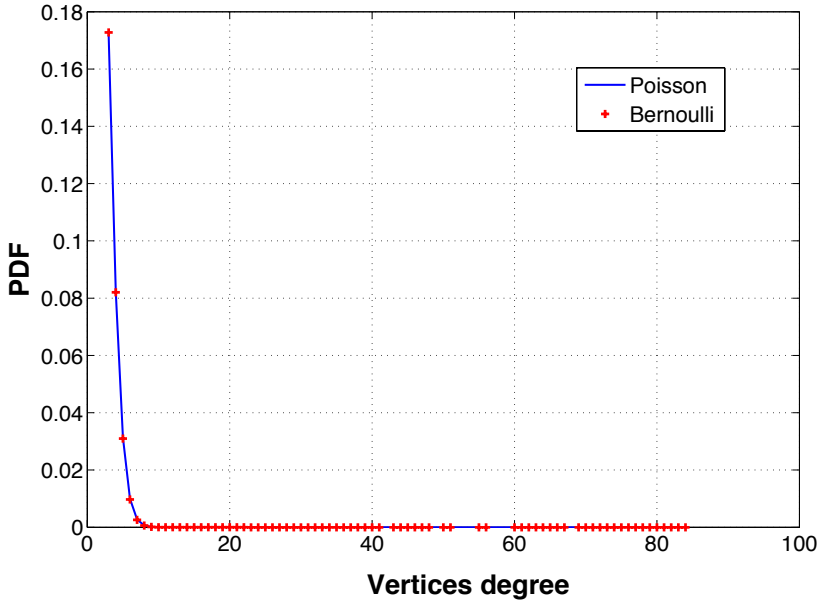


Figura 5.16: Distribuição de graus dos vértices para o grafo da rede celular

conectividade da rede celular. A análise realizada permite identificar um pequeno número de arestas no conjunto de menor corte mínimo em comparação com o total de arestas na rede. Esta situação procede da reduzida densidade de arestas na periferia da rede, diferentemente da região central, que apresenta uma alta densidade, tal como ilustrado na Figura 5.14. Os resultados indicam que o conjunto de arestas mais criticas nessa rede está localizado na periferia, como observado na Figura 5.15(c).

NF	**NR**	**Agrupamento**	**Corte mínimo**
0.15	0.75	0.5036	3

Tabela 5.2: Resultados para rede celular

O índice do grau de robustez da rede celular, calculado pela relação entre o C_{Global} e maior C_v, indica a existência de alta ligação dos vértices do grafo, a alta conexão entre os vizinhos de um dispositivo, o que proporciona a existência de rotas alternativas na comunicação dos nós. Os resultados indicam que apesar da distribuição desigual de arestas no grafo, os nós críticos apresentam uma alta conectividade com seus vizinhos, o que ajuda na antifragilidade rede.

A Figura 5.17 mostra o valor da AC calculada para a rede celular heterogênea de topologia estática, variando os valores dos pesos de importância α e β. Os resultados

mostram que a antifragilidade de conectividade aumenta a medida que o valor de α cresce. No cenário em que o valor de α corresponde a 0,9 e β a 0,1, o valor da AC da rede é maior do que 0,75. Para o cenário em que o valor de α corresponde a 0,6 e β a 0,4, o valor de AC equivale a 60 %. Esses resultados permitem afirmar que a antifragilidade de conectividade para a rede analisada varia de 60 % até 75 %. Esse comportamento resulta da alta conectividade entre os nós que compõem o núcleo da rede, fornecendo diferentes caminhos alternativos para comunicação entre os dispositivos.

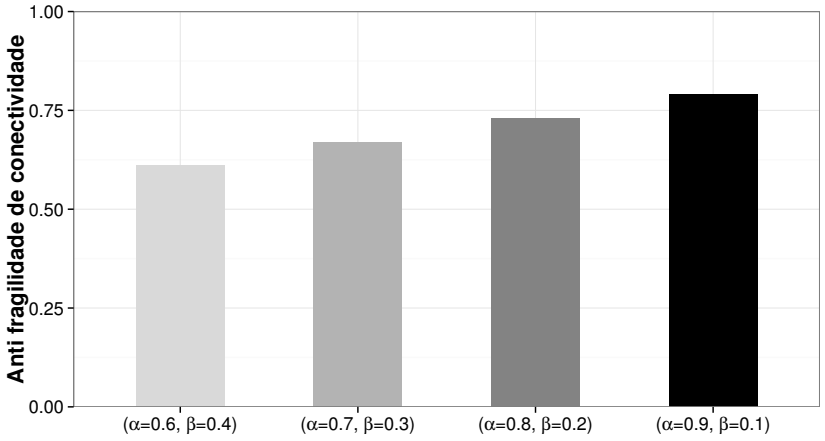


Figura 5.17: Antifragilidade da conectividade da rede celular

5.5 Resumo

Neste capitulo foi apresentado o sistema aferidor de resiliência de conectividade de redes heterogêneas. A antifragilidade de conectividade calculada pelo sistema corresponde ao indicador das condições de segurança da rede. Foram detalhadas as medidas auxiliares de fragilidade e robustez utilizadas na composição da métrica de antifragilidade. Um exemplo de funcionamento do sistema foi apresentado, bem como avaliações de dois cenários de redes distintas, uma de topologia de conectividade dinâmica e outra com topologia de conectividade estática. Os resultados obtidos apontam a eficiência do sistema na avaliação das condições das redes em diferentes momentos de atividade, o que comprova sua eficácia na aferição do indicador segurança de redes heterogêneas.

CAPÍTULO 6

ESTRATÉGIA DE ESCOLHA DA REDE SEGURA PARA CONEXÃO CONTÍNUA EM REDES HETEROGÊNEAS

Esse capítulo descreve uma estratégia de tomada de decisão sobre acesso seguro em redes heterogêneas sem fio. A tomada de decisão auxilia na escolha da rede de acesso mais confiável em ambientes de redes sem fio sobrepostas. A Seção 6.1 detalha a caracterização do problema de decisão de acesso. A Seção 6.2 descreve o sistema de tomada de decisão de acesso seguro em redes heterogêneas. A Seção 6.3 apresenta a análise e avaliação do sistema, bem como a descrição de seus resultados e a Seção 6.4 apresenta um resumo do capítulo.

6.1 Caracterização do problema de decisão de acesso

As redes de acesso de tecnologias de comunicação sem fio tem passado por uma evolução expressiva nas últimas décadas. No passado, o número de redes de acesso sem fio era reduzido, e a manutenção da conectividade se restringia à área de cobertura da tecnologia de rede utilizada. Atualmente, com a proliferação do número de redes de acesso sem fio, a área de cobertura não representa um grande desafio. As regiões de cobertura sobrepostas tem aumentado significativamente, principalmente devido à expansão de redes sem fio de tecnologias heterogêneas.

As redes heterogêneas sem fio permitem que usuários portadores de dispositivos computacionais móveis transitem por diferentes áreas e estejam sempre assistidos por algum tipo de rede de acesso. Um dos principais desafios pertinente a esse novo contexto corresponde à escolha adequada da rede. Apesar do requisito de mobilidade com manutenção de conectividade ainda presente, outras exigências, como a segurança, passam a fazer parte da demanda dos usuários. A escolha da rede de acesso dentre um conjunto de redes disponíveis se torna fundamental para a garantia da qualidade dos serviços utilizados e

da segurança e satisfação dos usuários.

Um usuário, portador de um dispositivo computacional móvel, transita por diferentes áreas. Durante seu percurso detecta a existência de redes de acesso de tecnologias heterogêneas. Dado que seu dispositivo possui recursos para conectar em todas elas, como decidir pela conexão na melhor rede de acesso, de modo que sua conectividade seja contínua e segura? Neste cenário, o processo de tomada de decisão sobre o acesso utiliza dados coletados das redes detectadas durante a movimentação do usuário. Esses dados são processados para auxiliar na escolha pela melhor rede, de acordo com as caraterísticas desejadas. Somente após a escolha da melhor rede o dispositivo móvel deve efetuar sua conexão. Esta sequência de etapas possibilita a extração de características do processo que devem ser respeitadas para um sistema de tomada de decisão justa e eficaz.

A existência de diferentes tipos de redes por onde o usuário transita representa o *ambiente de decisão*. A quantidade de redes e suas respectivas qualidades são *eventos aleatórios*, que variam de acordo com o tempo. As *ações* que podem ser executadas pelo processo de decisão consistem de *monitoração, conexão e desconexão* da rede. O *estado* em que o dispositivo móvel pode estar consiste em *conectado* ou *desconectado*. A *política de decisão* compreende as conexões em redes mais seguras e confiáveis durante o percurso do usuário. A satisfação do usuário corresponde à *recompensa* pela conectividade segura e contínua. Essa definição do problema juntamente com a extração de características bem definidas, como as apresentadas, permite a sua representação por meio do *Processo de Decisão de Markov*.

6.1.1 Representação do processo de decisão de acesso

A tomada de decisão de acesso seguro e confiável em redes heterogêneas sem fio é representada por um Processo de Decisão de Markov - MDP *(Markov Decision Process)*. Este método permite a representação de processos de transição de estados probabilísticos, com possibilidade de observação do estado e possível interferência, executando ações em época de decisão [91]. Neste método, cada ação possui uma recompensa ou custo, dependendo do estado em que o processo esteja. O MDP obedece propriedade de Markov, em que

o efeito de uma ação em um estado depende apenas da ação e do estado atual, sem necessidade de informações sobre ações e estados anteriores. O método é conhecido como um *"processo de decisão"* pois modela a possibilidade de um agente tomador de decisões interferir periodicamente no sistema executando ações, diferentemente das *Cadeias de Markov*, onde não há possibilidade de interferência no processo [91].

O processo de decisão markoviano modela situações em que seja necessário executar ações em sequência em ambientes com incerteza. O MDP representa um sistema com vários estados, ações que modificam os estados e a percepção do resultado de cada ação executada. Assim, dado a descrição de um problema, resolvê-lo significa determinar que ação tomar para maximizar a recompensa esperada (ou minimizar o custo esperado). Esta ação pode ser definida como uma *Política Optimal*.

A Figura 6.1 ilustra a dinâmica de funcionamento de um sistema modelado como um MDP. O agente tomador de decisões verifica o estado atual (s) do sistema, consulta uma política Optimal (π) e executa uma ação (a). A ação pode ter um efeito sobre o ambiente (e) e modificar o estado atual. O agente tomador de decisões verifica o novo estado para tomar a próxima decisão, na futura época de decisão (d).

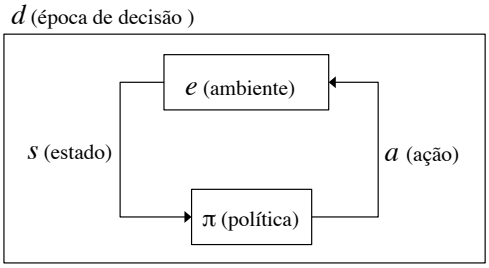


Figura 6.1: Dinâmica de funcionamento de um MDP

Formalmente o Processo de Decisão Markoviano – MDP consiste de uma *4-tupla (S, A, T, R)* onde:

- S = representa o conjunto de estados em que o processo (sistema) pode estar;
- A = compreende o conjunto de ações que podem ser executadas em diferentes épocas de decisões;

- $T : S \times A \times S \longmapsto [0, 1]$ implica em uma função que dá a probabilidade de um sistema passar para o estado $s' \in S$, dado que o processo esteja em um estado $s \in S$ e o agente tomador de decisão decidiu executar uma ação $a \in A$ (denotada por $T(s' \mid s, a)$);

- $R : S \times A \longmapsto \mathbb{R}$ representa uma função que dá o custo ou recompensa, por tomar uma decisão $a \in A$ quando o processo estiver em um estado $s \in S$.

A cada *época de decisão (d)*, o agente tomador de decisões usa uma *regra de decisão (r)* para escolher a próxima *ação (a)*. Uma forma simples de regra de decisão consiste em um mapeamento direto de estados em ações como $r : S \longmapsto A$. Assim, uma regra de decisão r para um MDP em uma época de decisão d consiste de uma função $rd : S \longmapsto A$, que determina a ação a ser executada, dado o estado do sistema. O conjunto de todas as regras de decisão (uma para cada época de decisão) é chamado de *Política*. Normalmente o principal objetivo do processo consiste em encontrar uma política que otimize um dado critério de desempenho [92]. Uma política pode ser classificada como: Markoviana (ou sem Memória), quando a escolha da ação depende apenas do estado corrente; e Não-Markoviana, quando a escolha da ação depende de todo o histórico de ações e estados do sistema até o momento.

No contexto da redes heterogêneas, o processo de decisão de acesso seguro é apresentado a seguir, juntamente com a Figura 6.2 que ilustra a dinâmica do MDP para uma política de melhor acesso nessas redes. Neste trabalho, o melhor acesso à rede representa a conexão na rede mais segura e confiável.

- S= [Conectado, Desconectado]

- A= [Monitoração, Conexão, Desconexão]

- $T : S \times A \times S \longmapsto [0, 1]$ probabilidade de estar em um estado de S

- $R : S \times A \longmapsto \mathbb{R}$ custo ou recompensa por tomar uma decisão

- $\pi-$PoliticaOptimal = melhor rede

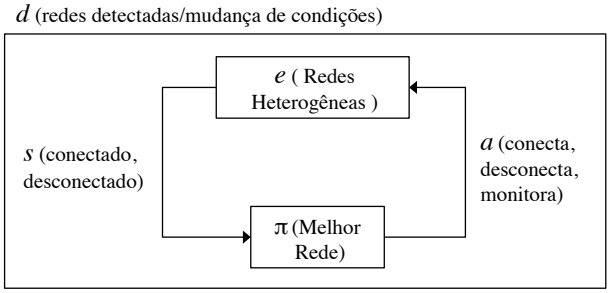


Figura 6.2: Dinâmica de funcionamento de um MDP em redes heterogêneas

O agente tomador de decisões consulta o ambiente (redes heterogêneas), verifica o estado atual do sistema (conectado ou desconectado), consulta uma política optimal (conexão em melhor rede entre redes disponíveis) e executa uma ação (monitora novas redes, conecta ou desconecta). Esse ciclo se repete em todas as épocas de decisões. Caso uma ação (a partir de uma política) leve a uma mudança para um novo ambiente, ou um estado (a partir do ambiente) leve a uma nova política. O ciclo operacional do agente tomador de decisão pode ser encadeado as diferentes épocas de decisão. Esse processo cíclico não necessita do conhecimento dos estados anteriores do sistema e utiliza apenas de informação atuais, obedecendo o princípio markoviano. A Figura 6.3 ilustra o funcionamento do processo MDP de ciclo contínuo.

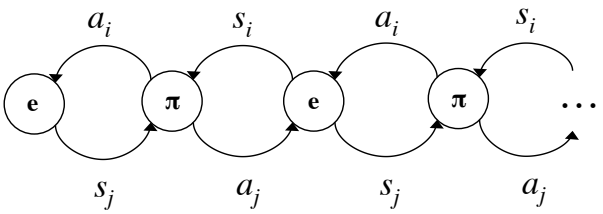


Figura 6.3: Dinâmica de funcionamento de um MDP de ciclo contínuo

Em uma época de decisão (d), o ambiente (e) possibilita ao agente tomador de decisão verificar um estado (s_j) do sistema que leva a uma política (π). A partir da política (π) uma ação (a_j) pode induzir o sistema a um novo ambiente, ou a um ambiente anterior, executando a ação (a_i). Neste novo ambiente (e), um estado (s_j) leva o sistema a uma nova política, ou a uma política anterior, com o estado (s_i). Esse processo se perpetua durante todas as épocas de decisões (d), assegurando a propriedade markoviana, de modo que uma decisão não depende de informações sobre ações nem de estados anteriores,

bastando apenas conhecer a situação atual do sistema para a tomada de decisão.

6.2 Um sistema de decisão de acesso em redes heterogêneas

O sistema de tomada de decisão proposto tem como objetivo auxiliar os usuários de dispositivos computacionais móveis a escolher e transitar por redes de acesso heterogêneas com conectividade segura e contínua. Para isso, o sistema obedece o processo de decisão markoviano, utilizando dados das condições atuais das diferentes redes detectadas e realizando um processo de inferência para decidir qual a melhor rede entre todas as redes disponíveis. Diferente das estratégias existentes na literatura, a escolha de melhor rede considera os critérios relacionados a *conectividade* e principalmente *segurança* como principais fatores de decisão. A Figura 6.4 lustra a arquitetura do sistema de decisão proposto.

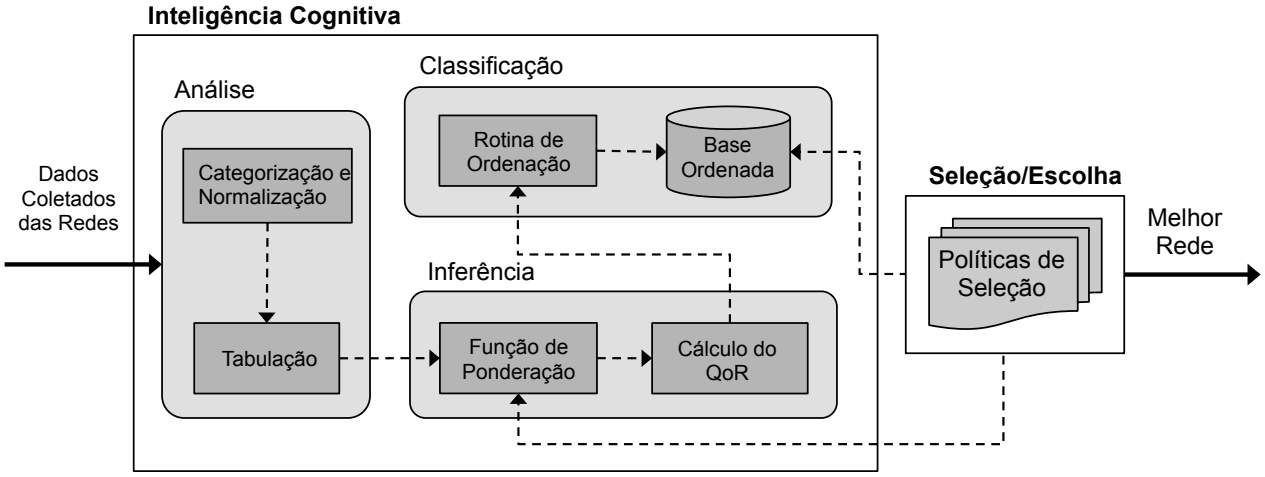


Figura 6.4: Arquitetura do sistema de tomada de decisão de acesso seguro

O sistema de tomada de decisão de acesso em redes heterogêneas sem fio compreende dois módulos. O primeiro denominado de *Inteligência Cognitiva*, tem o papel de processar os dados coletados do ambiente das diferentes redes detectadas, para inferir a melhor rede disponível, sob o aspecto de segurança e conectividade. O segundo, *Seleção/Escolha* tem como objetivo escolher a rede de acesso mais segura e confiável durante a transição dos usuários móveis pelos ambientes heterogêneos.

O módulo de *Inteligência Cognitiva* compreende os componentes de *Análise, Inferência*

e Classificação. O componente de *Análise* corresponde à primeira fase para o cálculo da melhor rede. Esse componente envolve os elementos de *Categorização e Normalização, e a Tabulação* de dados com as características das redes detectadas, obtidos na fase de coleta. A *Categorização e Normalização* separa os dados coletados da rede em diferentes categorias e aplica técnicas de padronização dos valores coletados a fim normaliza-los em uma mesma ordem de medida. A *Tabulação* recebe os dados normalizados e os organiza em um conjunto que será encaminhado para a fase de *Inferência*, e utilizado para o cálculo das condições de qualidade da rede.

A *Categorização e Normalização* dos dados coletados utiliza a razão entre o valor ótimo de referência para determinado critério (c), em um tipo de rede específico, e as condições atuais desse mesmo critério para a rede analisada. A fórmula para a normalização é definida pela Equação 6.1.

$$NCi = \frac{ValorOtimo\ i}{ValorAtual\ i} \quad \forall \quad i = \{1, 2, 3, ..., c\} \tag{6.1}$$

Onde, i implica o conjunto de critérios utilizados para a análise da rede e NCi corresponde a normalização do *i-ésimo* critério. A normalização feita por NCi é dada pela razão entre o *valor ótimo* (referência) de um critério (c) para determinada tecnologia da rede, e o *valor atual* do mesmo critério, obtido no momento de funcionamento da rede. Note que os valores normalizados para cada critérios estão no intervalo entre 0 e 1.

A *Tabulação* realiza uma operação de organização dos valores normalizados em um conjunto de critérios Cc. Após serem organizados esses valores são encaminhados para uma função de ponderação, onde receberão pesos de importância. A *Tabulação* é realizada obedecendo a Operação 6.2.

$$Cc = \bigcup_{i=1}^{c} NCi \quad \forall\ 1 \leq i \leq c \tag{6.2}$$

Onde, Cc corresponde ao conjunto de critérios já normalizados, utilizados para análise das condições da rede.

A *Inferência* corresponde o segundo componente do processo de decisão. Esse componente do módulo de inteligência cognitiva é responsável pelo cálculo do índice de qualidade da rede. Os elementos *Função de Ponderação e Cálculo da Qualidade da Rede (QoR)* formam o componente de Inferência. A Função de *Ponderação* atribui pesos de importância aos critérios utilizados na avaliação da rede. Nesse trabalho, para a *Função de Ponderação* cada peso w é representado em um intervalo [0,1] e a soma dos pesos deve ser igual a 1, como mostra a equação 6.3.

$$\begin{aligned} \sum_{j=1}^{k} w_i = 1 \; onde \; w_i > 0 \; \forall \; 1 \leq i \leq k \\ Cp = [w_1, w_2, w_3, ...w_n] \\ |Cp| = |Cc| \\ \forall \; i \in Cp \; \exists \; j \in Cc \end{aligned} \tag{6.3}$$

Onde, Cp compreende o conjunto de pesos de importância representados por $w_1, w_2, w_3, ..., w_n$. Cc representa o conjunto de critérios. A Cardinalidade de Cp é igual a de Cc. O somatório dos elementos de Cp deve ser igual a 1, e para cada elemento de Cp existe um elemento correspondente em Cc.

O *Cálculo do QoR* pode utilizar diferentes abordagem mono ou multicritério para calcular um índice de qualidade da rede com base nos critérios e métricas utilizadas na avaliação. Neste trabalho, o processo de inferência de melhor rede utiliza uma abordagem multicritério inspirada no método NWAUF *(Normalized Weighted Additive Utility Function)* [93], fundamentado nos estudos que mostram o seu baixo custo computacional em comparação a outros métodos MCDA *(Multiple-criteria decision analysis)*, como o AHP *(Analytic Hierarchy Process)* [94] ou ELECTRE *(ELimination and Choice Expressing REality)* [95], e as suas variantes [93, 96]. O método NWAUF utiliza múltiplos critérios normalizados e com pesos de importância para calcular uma função de utilidade. Esse método tem como base o somatório dos pesos utilizado juntamente com os critérios normalizados. A função de utilidade calculada determina o valor da qualidade da rede,

pelo fato de considerar pesos de importância sobre os valores coletados previamente de cada critério. A Equação 6.4 ilustra a fórmula utilizada para o *Cálculo do QoR*.

$$QoR = \sum_{i=1}^{c} w_i \times NCi, \ \forall \ i = 1, 2, 3, ..., c \tag{6.4}$$

Onde, QoR corresponde a qualidade da rede, verificada pela soma de cada critério NCi multiplicado por seu peso w_i, que correspondente a sua importância na avaliação das condições da rede.

O terceiro componente do módulo de *Inteligência Cognitiva* corresponde à *Classificação*. O componente de *Classificação* compreende uma *Rotina de Ordenação* e uma *Base Ordenada*. O elemento de *Rotina de Ordenação* recebe os valores de QoR das diferentes redes analisadas e os organiza para um armazenamento ordenado. Já a *Base Ordenada* consiste de um repositório contendo a lista de todas as redes avaliadas com seus respectivos valores de QoR organizados de forma decrescente. Deste modo, as redes com melhores valores de QoR serão as primeiras na base. A função de ordenação obedece a Equação 6.5.

$$\begin{aligned} Cr &= [QoR1, QoR2, QoR3, ...QoRN] \\ Cro &= [QoR1', QoR2', QoR3', ...QoRN'] \\ onde &: QoR1' \geq QoR2' \geq QoR3' \geq ... \geq QoRN' \end{aligned} \tag{6.5}$$

Cr corresponde a um vetor com os índices de qualidade das redes detectadas. Cro representa o vetor ordenado de modo que os melhores valores de qualidade da rede aparecem primeiro no vetor. A *Base ordenada* consiste de um lista armazenando o vetor ordenado dos valores de qualidade de cada rede.

O segundo módulo do sistema de tomada de decisão corresponde a *Seleção e Escolha*. Este módulo tem como base um componente de *Políticas de Seleção*. Essas políticas definem que rede, da base de dados ordenada, será selecionada para o acesso do dispositivo em transição. Caso a base não contenha nenhuma rede que satisfaça plenamente todas as

características da política definida, a seleção se dará pela rede que possuir condições mais próxima das desejadas, garantindo assim a conectividade do dispositivo móvel. A seleção de acesso em redes mais seguras corresponde um exemplo de *Políticas de Seleção*.

A *Política de Seleção* indica o uso de determinada rede da base de classificação, assim como, a classificação das redes disponíveis podem definir a alteração de uma política de seleção em determinadas condições do ambiente. Neste trabalho, a política de seleção de acesso é fortemente influenciada pelas condições de conectividade e segurança da rede. A seleção de acesso opta pelas redes mais segura e conexas. Vale ressaltar que uma determinada política de seleção pode influenciar a atribuição dos pesos de importância da *Função de Ponderação* do componente de *Inferência*. Esse processo, permite uma seleção da rede de modo mais personalizado e de acordo com características e preferências dos usuários e dos ambientes heterogêneos.

6.3 Análise e avaliação do sistema de decisão

O sistema de tomada de decisão sobre o acesso seguro em redes heterogêneas sem fio foi implementado no *Network Simulator 3* (NS-3) utilizando a linguagem de programação C++ e tendo como base o módulo do MIHF *(Media Independent Handover Function)*. O MIHF consiste no núcleo do protocolo 802.21 sendo responsável pela comunicação com diferentes tipos de redes [97, 98]. Tanto o MIHF quanto o próprio protocolo 802.21 não tratam do aspecto de decisão e seleção da rede de acesso e nem do aspecto de seguraNça. Assim, a implementação do sistema de tomada de decisão permitiu a análise de seu funcionamento, bem como a verificação das decisões de acesso e as transições em redes heterogêneas sem fio. A Figura 7.7 ilustra em alto nível o diagrama de classes da implementação.

A implementação do sistema de tomada de decisão como um módulo do simulador NS- 3 envolveu o uso do framework *MIH-Salumu* [99], responsável pela execução das funções do protocolo 802.21. Além do framework MIH a implementação compreende a criação das classes *Dispositivos, Interfaces e Redes* derivadas do próprio NS-3. Essas classes contribuíram com funções e métodos para a realização das simulações utilizando

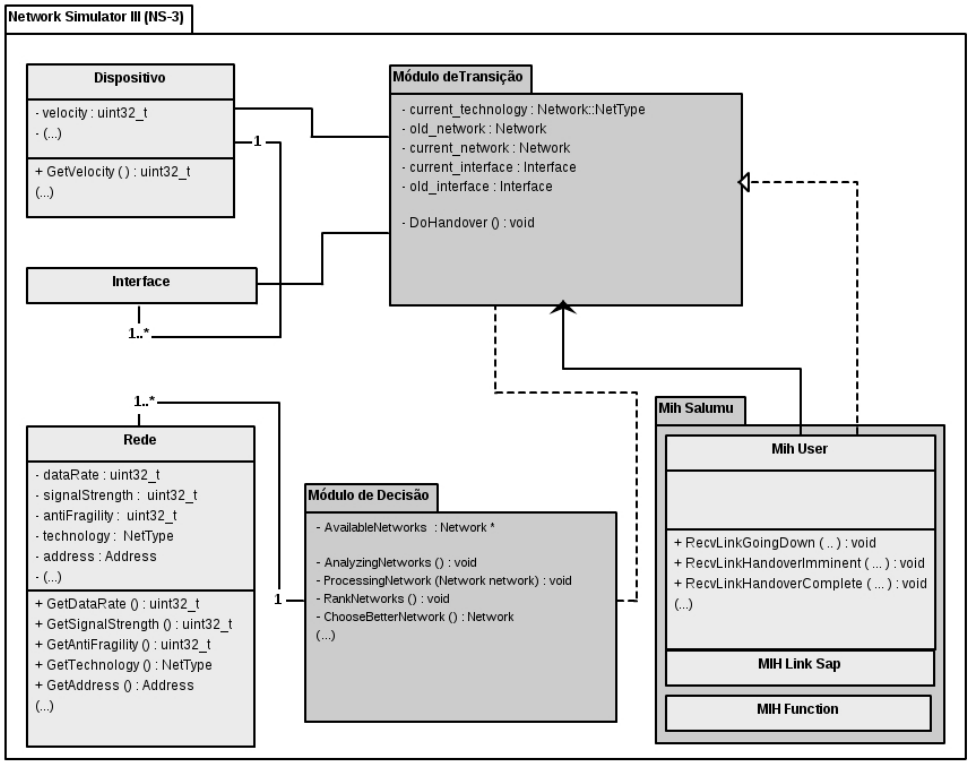


Figura 6.5: Diagrama de classe da implementação do sistema de tomada de decisão

dispositivos móveis que possuem várias interfaces de redes e transitam por diferentes redes de acesso sem fio com conectividade contínua. O *Módulo de decisão* se relaciona com um módulo auxiliar, implementado para realizar as transições a partir das decisões tomadas. Esse *Módulo de transição* efetua as mudanças de conexão nas diferentes redes de acesso com manutenção da conectividade, com base nos resultados das decisões realizadas pela análise das diferentes redes.

6.3.1 Descrição dos cenários

A avaliação do sistema de tomada de decisão foi realizada considerando três cenários distintos de simulação com diferentes velocidades de mobilidade dos dispositivos, e diferentes áreas de sobreposição de redes heterogêneas sem fio. A variação da velocidade de deslocamento do usuário móvel corresponde a um *pedestre* (1m/s), um *ciclista* (3m/s) e um *motorista* de automóvel (12m/s). A mobilidade aleatória dos usuários representa condições de mobilidade urbana. A área de sobreposição de redes utilizada compreende um ambiente realista de caráter *domiciliar* como uma casa que possui *baixa sobreposição*

de redes (duas redes sem fio sobrepostas), uma área *residencial* como um bairro ou um conjunto de apartamentos em um prédio, com *média sobreposição* de redes (dez redes sem fio sobrepostas) e uma região de um *centro comercial* com *alta sobreposição* de redes (vinte redes sem fio sobrepostas). Neste trabalho utilizaremos a sigla *BSR* para representar o cenário 1, com baixa sobreposição de redes em um ambiente domiciliar, *MSR* para o cenário 2 com média sobreposição ambiente residencial e *ASR* para o cenário 3 com alta sobreposição de redes em um ambiente comercial, como ilustrado na Figura 6.6.

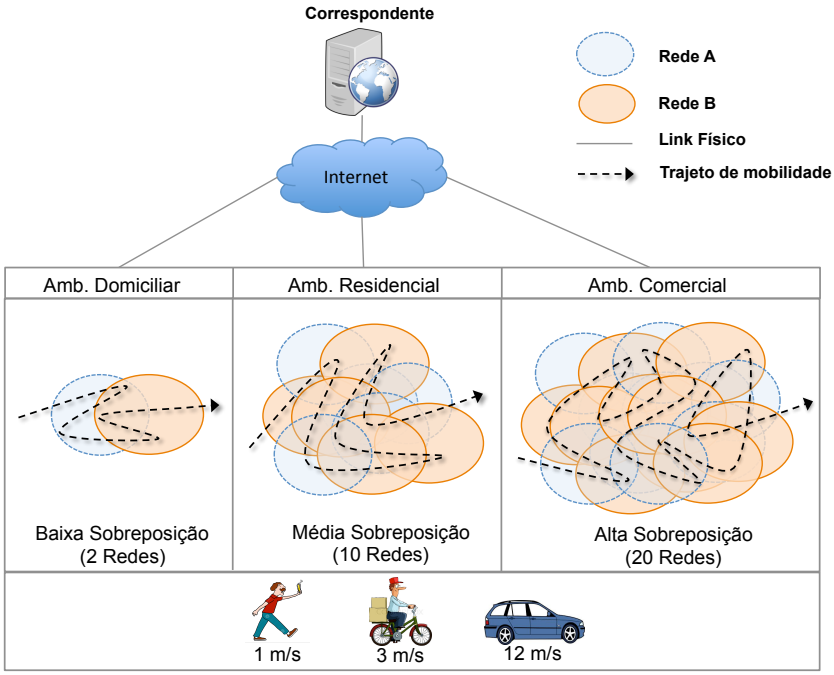


Figura 6.6: Cenários de simulações

As redes utilizadas na simulação consistem de tecnologia de comunicação WiFi e WiMAX. Essas redes heterogêneas são utilizadas sem a perda de generalidade para a execução de transições de conexões em um ambiente sobreposto por redes de diferentes tecnologias de comunicação. As condições de cada rede se alteram constantemente de forma aleatória, em um intervalo de *5s* para representar sua dinamicidade. Os critérios utilizados para o processo de tomada decisão de acesso à rede correspondem à *Antifragilidade, Taxa de Transmissão e Largura de Banda*. Outros critérios podem ser usados sem a perda de generalidade e impacto no processo de decisão, a Tabela 6.1 apresenta os parâmetros utilizados em cada cenário.

Parâmetro	Valor	
Áreas	Domiciliar	100 x 100
	Residencial	150 x 150
	Comercial	200 x 200
Redes sobrepostas	BSR	2
	MSR	10
	ASR	20
Raio de cobertura	100 m^2	
Interfaces do nó móvel	WiFi e WiMAX	
Velocidade de mobilidade	1m/s; 3m/s; 12m/s	
Intervalo de dinamicidade	5 s	
Critérios de decisão e pesos de importância	Antifragilidade - 50%	
	Tx. Transmissão - 25%	
	Largura de Banda - 25%	
Tempo de simulação	200 s	

Tabela 6.1: Parâmetros das simulações do sistema de tomada de decisão

6.3.2 Discussão dos resultados

Para análise da eficácia do sistema de decisão foram utilizadas as métricas: *i) número de decisões realizadas*. Essa métrica indica quantas decisões são realizadas pelos dispositivos móveis em transição por uma determinada área de redes sobrepostas. *ii) número de transições*. Nesta avaliação considera-se o número de transições a partir das decisões de escolha de melhor rede entre todas disponíveis. Para a análise da eficiência foi considerado a métrica *Tempo de decisão*. Esta métrica verifica o tempo gasto para decidir pela melhor rede disponível em ambientes sobrepostos com redes heterogêneas.

Número de decisões

A análise do número de decisões sobre a rede de acesso foi realizada considerando intervalos de 10, 15 e 20 segundos. Esses intervalos são utilizados para verificação das condições das redes, que devido a sua dinamicidade, podem ser alterados a todo instante (nesta avaliação, as alterações da rede ocorrem a cada 5 segundos). Assim, as decisões de seleção da rede acontecem à medida que eventos como a detecção de novas redes, mudanças das condições da rede atual ou mesmo a saída da área de cobertura da rede ocorram ou até que os valores dos intervalos sejam obedecidos.

A Figura 6.7 ilustra o número de decisões para cada intervalo, variando a velocidade do dispositivo móvel nos três cenários de avaliação, *BSR, MSR e ASR*. O gráfico da Figura 6.7(a) mostra que com a velocidade de um pedestre, o número de decisões pela redes mais segura se manteve constante independente do tipo de cenário avaliado. Já com a velocidade de um ciclista existe um aumento do número de decisões quando o número de sobreposições de redes é alto. No caso de velocidade de um motorista foi verificado uma variação do número de decisões de acordo com cada cenário avaliado. Os resultados permitem concluir que a medida em que a velocidade do dispositivo móvel aumenta e o número de sobreposições de redes também aumenta, o número de decisões realizadas pelo sistema de tomada de decisão de acesso à rede é incrementado. Isso ocorre porque o dispositivo em transição detecta mais redes e precisa escolher mais vezes pela melhor rede disponível.

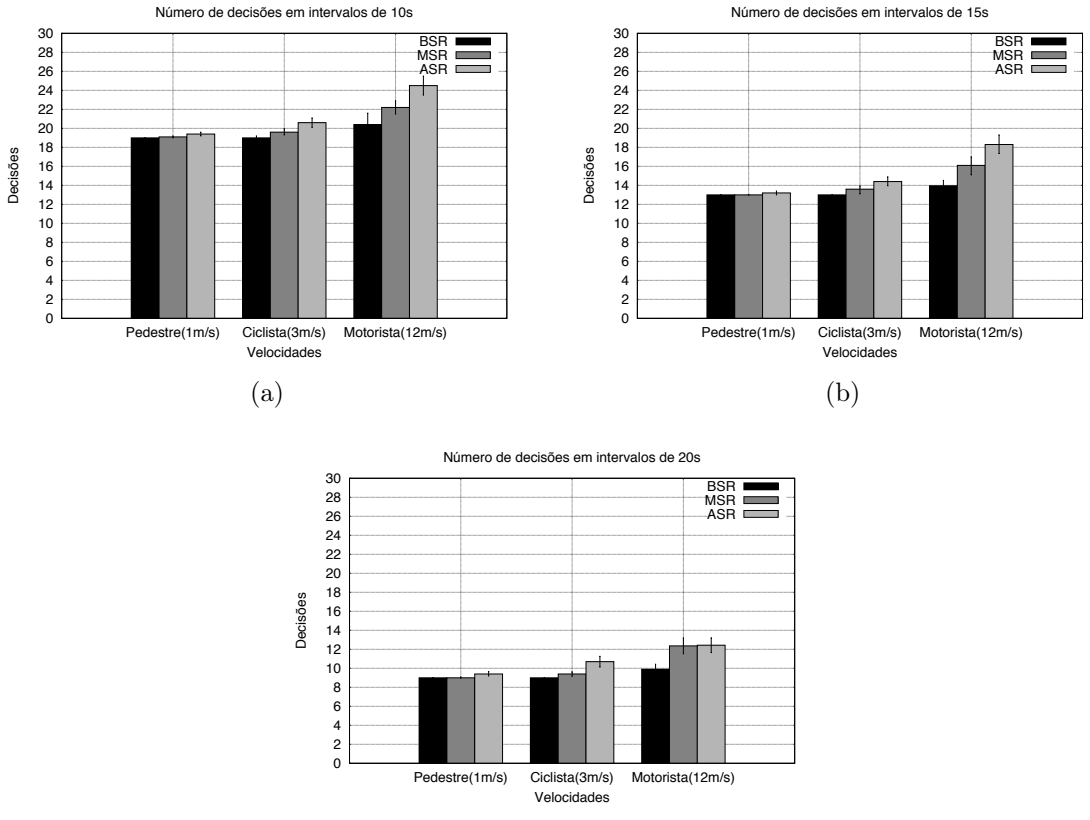


Figura 6.7: Avaliação do número de decisões

O mesmo comportamento identificado no gráfico da Figura 6.7(a) também é encon-

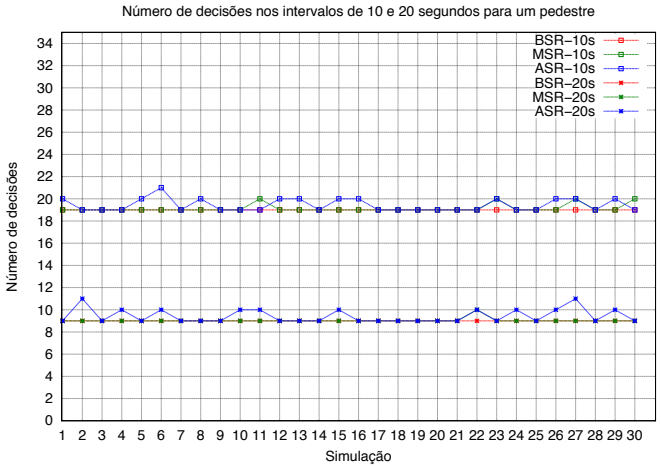
trado nas Figuras 6.7(b) e 6.7(c). Os valores relacionados ao número de decisões são inferiores, devido ao aumento do intervalo de decisões realizadas pelo sistema. Na Figura 6.7(c), com um intervalo de 20s de decisão, o dispositivo móvel com velocidade de um motorista a 12m/s estabiliza o número de decisões nos cenários *MSR e ASR*. Isso ocorre porque mesmo que a sobreposição e a dinamicidade das redes sejam de média à alta o intervalo de decisão de 20s faz com que as consultas sobre as condições das redes e consequentemente o número de decisões de melhor rede sejam os mesmos.

Além dos valores obtidos pela média do número de decisões de transições ilustrados nos gráficos anteriores, também foi feita uma análise do comportamento desses resultados obtidos em todas as simulações realizadas. O gráfico da Figura 6.8 mostra os resultados comparativos desse comportamento para o melhor caso, o número de intervalos corresponde a 10 segundos e o pior caso, o número de intervalos de decisões consiste em 20 segundos. Essa análise foi realizada para a velocidade de pedestre, Figura 6.8(a), ciclista Figura 6.8(b) e motorista Figura 6.8(c).

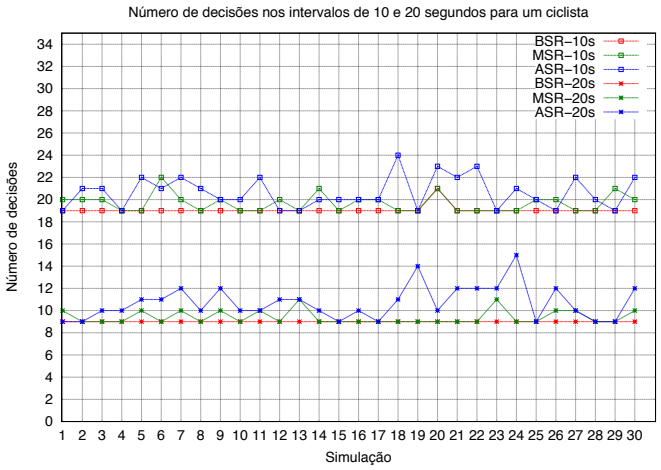
Número de transições

O número de transições de acesso de uma rede para outra também foi avaliado considerando o mesmo ambiente utilizado para a avaliação do número de decisões. Nesta avaliação, as transições de acesso só ocorrem a partir da decisão da escolha da rede mais segura dentre as redes disponíveis. A transição de uma rede para outra implica na manutenção da conectividade contínua e para redes com os melhores valores dos critérios analisados na seleção.

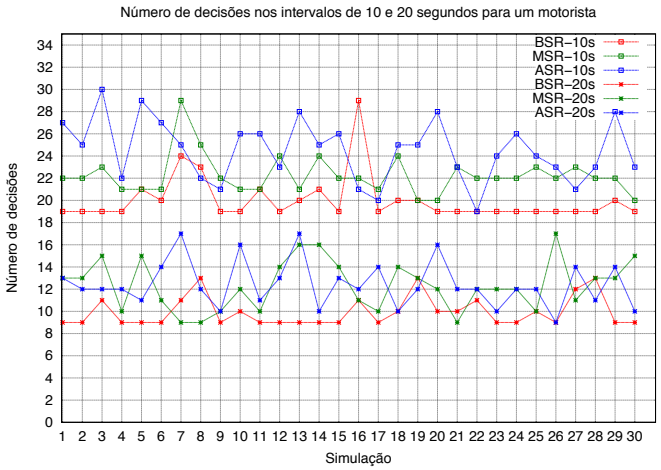
A Figura 6.9, os gráficos do número de transições realizadas a partir das decisões de acesso sobre a rede para cada intervalo, variando a velocidade do dispositivo móvel nos três cenários de avaliação. O gráfico da Figura 6.9(a) mostra que, independente da velocidade do dispositivo, o número de transições para melhores redes se manteve constante quando as sobreposições de redes são baixas. Em casos de média sobreposição de redes *MSR*, o número de transições tem uma variação comparando todas as velocidades. Já com alta sobreposição de redes, os números de transições são maiores quando as velocidades



(a)



(b)



(c)

Figura 6.8: Avaliação do comportamento do número de decisões em intervalos de 10 e 20s

também são altas, o que pode ser explicado pela constante detecção de novas redes em razão da mobilidade pelo ambiente. O gráfico da Figura 6.9(b) apresenta comportamento similar, mas com valores de transições reduzidos em razão do maior intervalo de decisão. O gráfico da Figura 6.9(c) mostra uma certa estabilidade no número de transições em cenários de *MSR*. Os valores de transição entre 10 e 20 redes sobrepostas são similares na maioria dos casos.

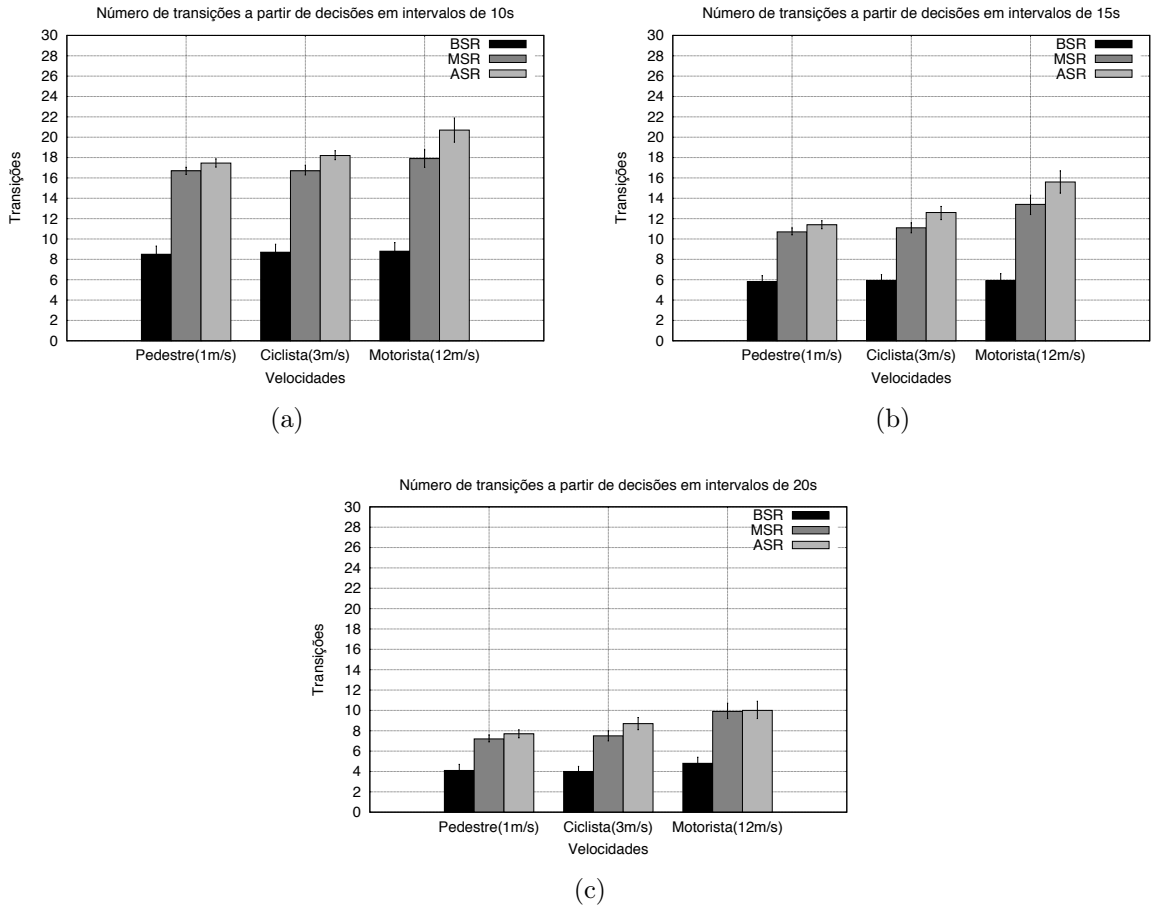


Figura 6.9: Avaliação do número de transições a partir das decisões

Número de decisões × número de transições

Os resultados da avaliação do número de decisões e do número de transições mostram que o sistema de decisão reduz a realização de transições desnecessárias em áreas de redes heterogêneas sobrepostas. Dispositivos móveis que transitam sobre redes sobrepostas realizam trocas de uma rede para outra em razão da detecção de novos eventos. O

gráfico da Figura 6.10 mostra a comparação do número de decisões e número de transições realizadas para todos os cenários de simulação e em todos os intervalos de consulta das condições da rede e decisão de acesso.

Em todos os resultados ilustrados nas Figuras 6.10(a), 6.10(b) e 6.10(c) o número de transições foi inferior ao número de decisões, o que mostra que decidir pela melhor rede evita transições desnecessárias e garante a mobilidade de modo seguro e com conectividade contínua.

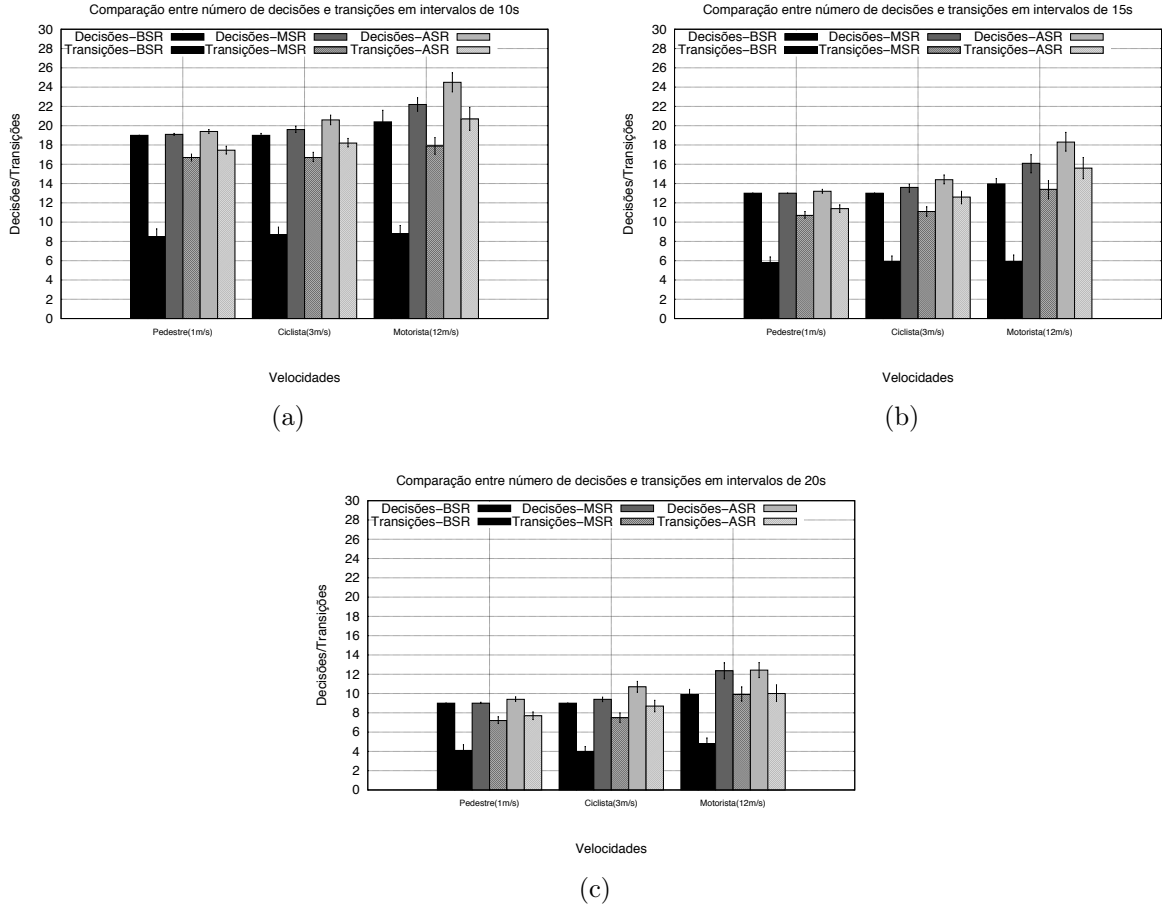


Figura 6.10: Comparação entre o número de decisões e o número de transições realizadas

Tempo de decisão

A avaliação do tempo de decisão verifica a eficiência do sistema em decidir pela rede de acesso mais segura nos três cenários utilizados na simulação. Em cada cenário foram considerados os intervalos de decisão referentes a 10, 15 e 20 segundos. Os resultados

apresentados no gráfico da Figura 6.11 mostram que o tempo de decisão é similar considerando os diferentes intervalos de decisão em cada cenário de avaliação. Contudo, existe um acréscimo do tempo de decisão à medida que aumenta o número de redes sobrepostas, o que faz com que o sistema tenha que analisar mais redes disponíveis na mesma área de cobertura do dispositivo móvel. Outro ponto evidenciado pelos resultados consiste no baixo tempo necessário para decidir qual é a melhor rede disponível. No pior caso, em que existe alta sobreposição de redes o tempo gasto para decidir sobre a melhor rede corresponde a 270 milisegundos. Já no melhor caso, com apenas 2 redes sobrepostas o tempo de decisão é de 150 milisegundos. Esses resultados mostram que o sistema de tomada de decisão não tem impacto significativo na sobrecarga de tempo de transição de uma rede para outra independente de sua tecnologia de comunicação.

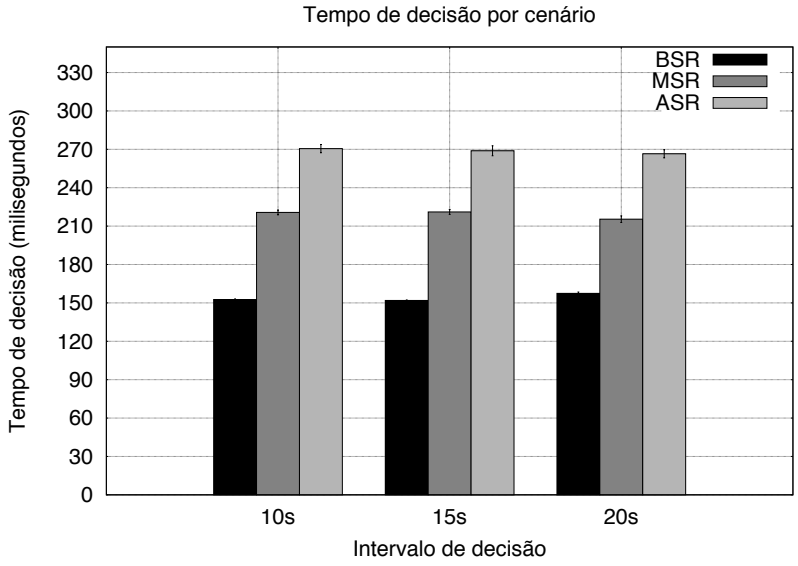
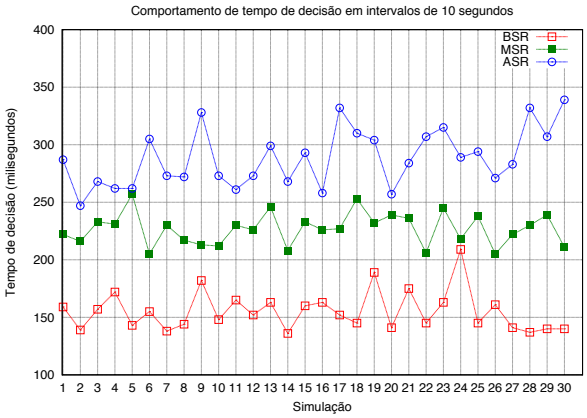
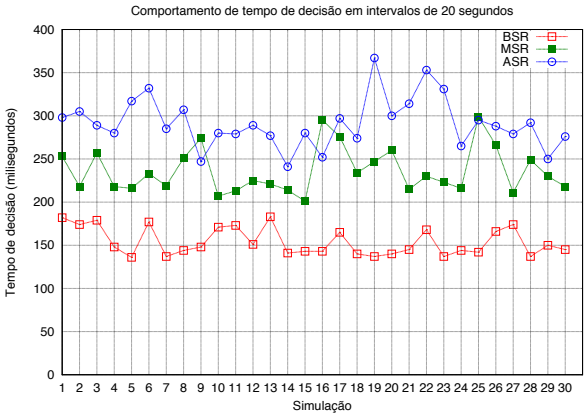


Figura 6.11: Avaliação do tempo decisão

Os gráficos das Figuras 6.12 ilustram o comportamento do tempo de decisão em todas as simulações realizadas. Os resultados mostram uma variação do tempo de decisão nas diferentes areas de sobreposição em intervalos de 10 (Figura 6.12(a)) e 20 segundos (Figura 6.12(b)).



(a)



(b)

Figura 6.12: Comportamento do tempo de decisão para 10 e 20s em todos os cenários

6.4 Resumo

Neste capitulo foi apresentada uma estratégia de escolha da rede segura para o conexão contínua em redes de heterogêneas. A caracterização do problema de decisão foi discutida. A representação do processo de decisão foi realizado através do Processo de Decisão Markoviano - MDP. Um sistema de tomada de decisão de acesso seguro em redes heterogêneas foi apresentado, bem como sua análise e avaliação, seguida de um descrição dos cenários de simulação e discussão dos resultados alcançados.

CAPÍTULO 7

GERÊNCIA AUTONÔMICA DO SERVIÇO DE ENDEREÇAMENTO EM REDES HETEROGÊNEAS

Esse capítulo descreve um esquema de gerência autonômica do serviço de endereçamento dinâmico em redes heterogêneas sem fio. O serviço de gerenciamento de endereços em redes heterogêneas auxilia a disponibilidade de conectividade, durante a transição de acesso de uma rede para outra. A Seção 7.1 descreve o processo de gerência do serviço de endereçamento em redes heterogêneas sem fio. A Seção 7.2 detalha o sistema de gerência de endereçamento em redes de acesso heterogêneas. A Seção 7.3 apresenta a análise e avaliação do sistema, bem como a descrição de seus resultados e a Seção 7.4 resume o capítulo.

7.1 Gerência do serviço de endereçamento em redes heterogêneas sem fio

A capacidade de identificação e localização de um dispositivo móvel dentro das redes sem fio representa a base para a manutenção de um fluxo de dados já existente e garantia de conectividade contínua. Em grande parte das redes de transmissão de dados esse processo ocorre através do serviço de endereçamento dos dispositivos. O endereço de um dispositivo possibilita sua identificação e localização de modo que outros dispositivos correspondentes sejam capazes de encaminhar pacotes de dados independentemente de onde estejam. As diferentes redes de acesso também possuem formatos distintos de endereçamento em função das tecnologias de comunicação utilizadas.

As redes sem fio com tecnologia de comunicação WiFi, por exemplo, utilizam o *Internet Protocol* (IP) para identificar e localizar os dispositivos na rede. A identificação da rede ocorre através do *NetID (network identification)* e a identificação do dispositivo

por meio do *HostID (host identification)*. A localização dos dispositivos acontece através do roteamento hierárquico realizado pelo *CIDR (Classless Inter-Domain Routing)*, que tem como base a identificação oferecida pelo protocolo IP. O formato do endereço IP foi projetado para identificar e localizar os dispositivos de forma fixa, sem mobilidade. No entanto, variantes como o *Mobile IP* tem sido apresentados para suprir essa deficiência [100].

Em outras tecnologias de redes de comunicação como *Bluetooth*, por exemplo, o formato de endereçamento não segue o padrão das redes IP. O Bluetooth usa o *BD_ADDR (Bluetooth Device Address)* como estratégia de endereçamento. As redes de telefonia celular como o *GSM (Global System for Mobile Communications)* utilizam a Identificação Internacional de Equipamento Móvel - IMEI *(International Mobile Equipment Identity)* que também não segue o formato de endereçamento utilizado nas rede IP. Esses diferentes padrões e formas de endereçamento dificultam a integração das tecnologias de comunicação e a transição dos dispositivos móveis com a conectividade contínua por diferentes redes de acesso.

A forma de atribuição de endereços aos dispositivos corresponde outro aspecto que tem forte impacto na manutenção da conectividade durante a transição por redes de acesso sem fio. Ao migrar de uma rede para outra, o dispositivo em transição deve configurar seu endereço de acordo com as características da rede para a qual está migrando. Assim, ao realizar o estabelecimento da conexão em nível físico é necessário a atribuição de um endereço em nível de rede para que a comunicação possa ser iniciada ou continuada. Para redes do tipo infra estruturadas uma entidade central controla a distribuição de endereços respeitando as características da rede. O DHCP *(Dynamic Host Configuration Protocol)* é o protocolo mais utilizado para atribuição de endereços em redes do tipo IP devido a sua capacidade de distribuição automática, reduzindo substancialmente a necessidade de um operador humano para a realização desse processo [101].

O DHCP é um protocolo cliente-servidor que provê parâmetros de configuração e aloca endereços para um dispositivo através de troca de mensagens [102]. Esse protocolo é responsável pela definição, negociação e atribuição do endereço ao dispositivo. Devido

ao formato diferenciado dos endereços dos dispositivos que transitam entre redes heterogêneas, o processo de negociação do endereço tem de ser modificado para atender às necessidades de diferentes redes de comunicação sem fio. A gerência do serviço de endereçamento representa um dos principais desafios para a manutenção da conectividade contínua durante a transição entre redes heterogêneas.

7.2 Sistema de gerência autonômica para o serviço de endereçamento dinâmico em redes heterogêneas

O sistema de gerência de endereçamento em redes de acesso heterogêneas sem fio tem por objetivo oferecer um serviço que suporte à manutenção da conectividade contínua aos dispositivos computacionais móveis, que migram suas conexões de uma rede para outra. Esse sistema utiliza princípios da computação autonômica como o autogerenciamento para diminuir, ou mesmo eliminar, a necessidade de intervenção humana no processo de gerência. A estratégia de gerência proposta atua na perspectiva de três eixos de gerenciamento como ilustrado na Figura 7.1. O sistema proposto exerce o gerenciamento de endereços em redes heterogêneas para a disponibilidade de conectividade.

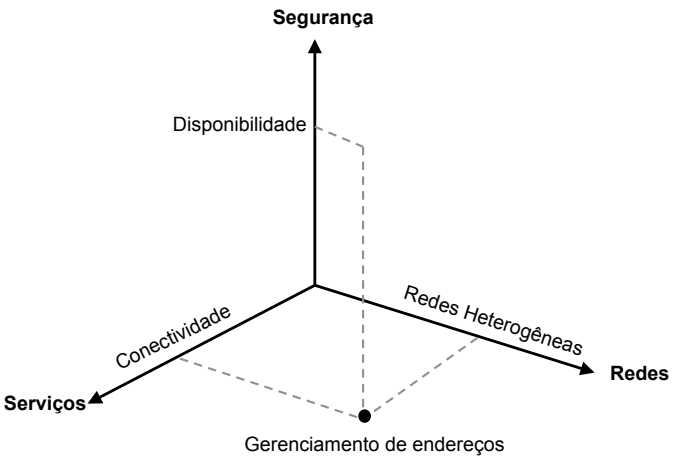


Figura 7.1: Eixos de gerenciamento

Eixo de Rede. No eixo de rede o sistema de gerenciamento busca garantir a convergência de comunicação para os dispositivos móveis que transitam em redes de acesso heterogêneas sem fio. As tarefas de registo, associação, reassociação e dissociação do dis-

positivo são realizadas de modo autonômico. Contudo, a concessão de acesso acontece a medida em que o dispositivo em transição possua as credenciais adequadas à rede. Além disso, uma avaliação prévia do dispositivo que solicita o acesso é realizada, a fim de garantir as condições mínimas de segurança tanto para a rede de acesso quanto para os dispositivos em transição.

Eixo de Serviço. No eixo de serviço o mecanismo de gerenciamento tem como foco a conectividade. Neste contexto, o endereçamento dos dispositivos recebe maior atenção. O endereçamento corresponde a um dos principais serviços de apoio à manutenção da conectividade dos dispositivos em transição por redes heterogêneas sem fio. O sistema apresentado tem por objetivo gerenciar a concessão de endereços por meio de um esquema de negociação entre os dispositivos em transição e as diferentes redes de acesso.

Eixo de Segurança. No eixo de segurança o gerenciamento acontece de modo a garantir a disponibilidade do serviço de endereçamento, bem como proteger e defender os dispositivos em transição e as redes de acesso de ações maliciosas.

Além dos eixos de gerência apresentados, o sistema atende aos princípios autonômicos do autogerenciamento através da i) Autoconfiguração *(Self-Configuration)*, que corresponde à capacidade do sistema de se adaptar às condições do ambiente, previsíveis ou não, ajustando sua configuração dinamicamente; ii) Autocura *(Self-Healing)*, que pode prevenir e recuperar uma falha, buscando, diagnosticando e corrigindo pontos que possam causar paradas nos serviços oferecidos; e iii) Autoproteção *(Self-Protection)*, que corresponde à capacidade de detectar, identificar e defender-se contra ataques e/ou situações indesejáveis.

O objetivo de utilizar estratégias de computação autonômica no gerenciamento de redes heterogêneas sem fio é simplificar o processo de gerência e reduzir a intervenção humana. A complexidade desses ambientes, associados à necessidade de alta disponibilidade de conectividade pode tornar a intervenção humana um ponto de falha no gerenciamento de serviços [103]. O sistema de gerência de endereçamento para redes heterogêneas sem fio proposto compreende duas etapas. A primeira, consiste no uso de um método de unificação dos formatos de endereços. Já a segunda, define de um processo de atribui-

ção desses endereços. O desenvolvimento destas duas etapas possibilitam a concepção de uma estratégia de endereçamento para redes heterogêneas sem fio, e a manutenção da conectividade contínua de dispositivos moveis em transição por diferentes redes de acesso.

7.2.1 Método de unificação dos formatos de endereços

A primeira etapa para a concepção de um sistema de gerência de endereçamento eficaz para redes heterogêneas sem fio consiste na elaboração de um método de unificação dos formatos de endereços. Unificar os formatos dos endereços representa uma premissa importante para permitir que os dispositivos possam se conectar em diferentes tipos de redes, sem que o fluxo de dados de suas comunicações sejam interrompidos. Essa interrupção acontece devido uma alteração de conexão em diferentes tecnologias das redes de acesso.

A estratégia utilizada para a unificação dos formatos de endereços para as diferentes redes de acesso consiste em dividir o endereço em duas partes, como já é feito no protocolo IP [104]. Uma parte correspondendo ao identificador da rede - NetID (independente de tecnologia) e outra parte referente ao identificador do dispositivo - HostID . A Figura 7.2 ilustra essa estratégia.

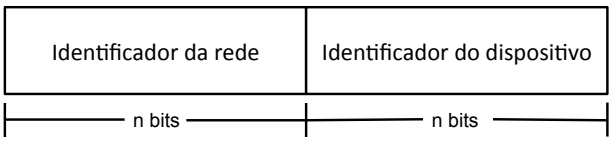


Figura 7.2: Formato de unificação de endereços para redes heterogêneas

O *Identificador da rede* (NetID) consiste de uma cadeia de bits com valor único, conhecido como *Basic Service Set Identification* (BSSID). O BSSID corresponde ao endereço MAC *(Media Access Control)* do provedor de acesso da rede. Essa abordagem garante que cada rede será unicamente identificada, permitindo localizar os destinos dos pacotes pelos dispositivos. O *Identificador do dispositivos* (HostID) consiste de outra cadeia de bits responsável pela identidade do dispositivo dentro da rede. Essa identidade permite à adequação de diversos formatos de endereços em um padrão único, independente do tipo de tecnologia da rede.

Um dispositivo que suporte tecnologias de comunicação WiFi e Bluetooth, por exemplo, possuirá endereços MAC para ambas as interfaces físicas de comunicação, mas na camada de rede, a interface WiFi terá o endereço IP enquanto a interface Bluetooth terá o endereço BD_ADDR *(Bluetooth Device Address)*. Ambos os padrões podem ser encapsulados no campo *HostID*, tornando a rede apta a identificar ambas interfaces através de um mesmo formato final de endereço. Assim como no WIFI e no Bluetooth, esse estratégia pode ser adotada em qualquer tecnologia de comunicação.

Processo de atribuição de endereços

A definição de um formato de endereço, adequado à transição entre redes heterogêneas, faz com que seja necessário definir um processo de atribuição de endereço ao dispositivo móvel após a requisição e concessão de acesso à rede. A definição de um provedor de endereços capaz de gerenciar de forma adequada esse processo consiste da segunda etapa necessária para manutenção da conectividade contínua de dispositivos em transição. Para a realização desta tarefa o sistema de endereçamento autonômico dispõe de um método de negociação de endereços.

7.2.2 Método de negociação de endereços

Quando um dispositivo deseja se conectar à rede, um endereço deve ser lhe atribuído para que sua transmissão de dados se inicie ou seja mantida. Neste caso, é fundamental que o dispositivo descubra qual é o servidor de endereçamento presente na rede. Assim, o dispositivo em transição inicia o processo de negociação enviando em broadcast uma mensagem de *Descoberta de servidor*, incluindo seu identificador de dispositivo. Quando o servidor de endereçamento recebe essa mensagem, efetua o cálculo do endereço utilizando os valores dos identificadores da rede e o identificador do dispositivo. Em seguida, o servidor salva esse endereço localmente e envia uma mensagem de *Oferta de concessão* ao dispositivo em transição (cliente). Mediante o recebimento da oferta de concessão, o cliente realiza o *Pedido de endereço* ao servidor detectado. Finalmente, ao receber o pedido, o servidor atualiza sua tabela de roteamento e envia uma mensagem de *Endereço*

ACK, confirmando a atribuição de endereço ao cliente. Neste momento, com o endereço atribuído o cliente pode começar e/ou continuar suas transmissões de dados na nova rede de acesso. A Figura 7.3 ilustra a realização desse procedimento.

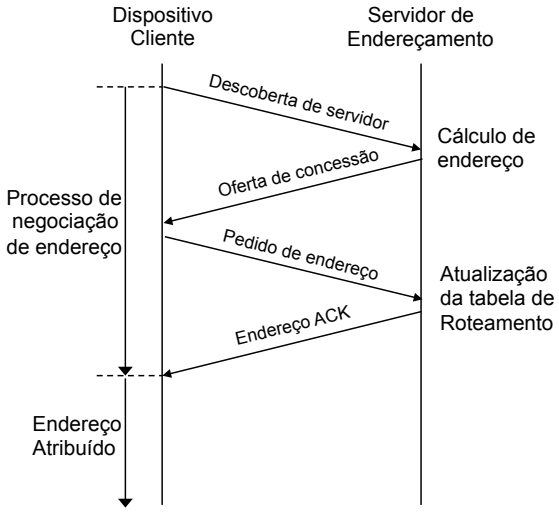


Figura 7.3: Processo de negociação de endereços

O processo de negociação de endereços do sistema de gerenciamento também pode ser representado por uma máquina de estados. As máquinas de estados permitem a representação de processos computacionais através de diagramas de transição de estados. Os estados da máquina são representados por um circulo, que corresponde um dado instante de operação do sistema. Para cada estado existe um arco de transição levando a um estado seguinte. Assim, após a leitura de uma entrada, uma função de transição indica um novo estado do sistema. A Figura 7.4 ilustra a máquina de estados utilizada para representar o processo de negociação de endereços do sistema de gerenciamento autonômico de redes heterogêneas sem fio.

De acordo com a máquina de estados ilustrada pela Figura 7.4, o dispositivo inicia o processo de negociação de endereço no estado de *Entrada na rede*. Assim, ele envia a mensagem de *ServerDiscover* em broadcast para a rede com o objetivo de identificar algum servidor de endereços. Neste momento, o dispositivo entra em um estado de *Descoberta de servidor*. Então, o dispositivo aguarda a resposta de algum servidor de endereçamento da rede. Casa não haja resposta durante um certo tempo ele volta para o estado de *Entrada na rede* e envia outra mensagem de *ServerDiscover*. Caso o dispositivo receba

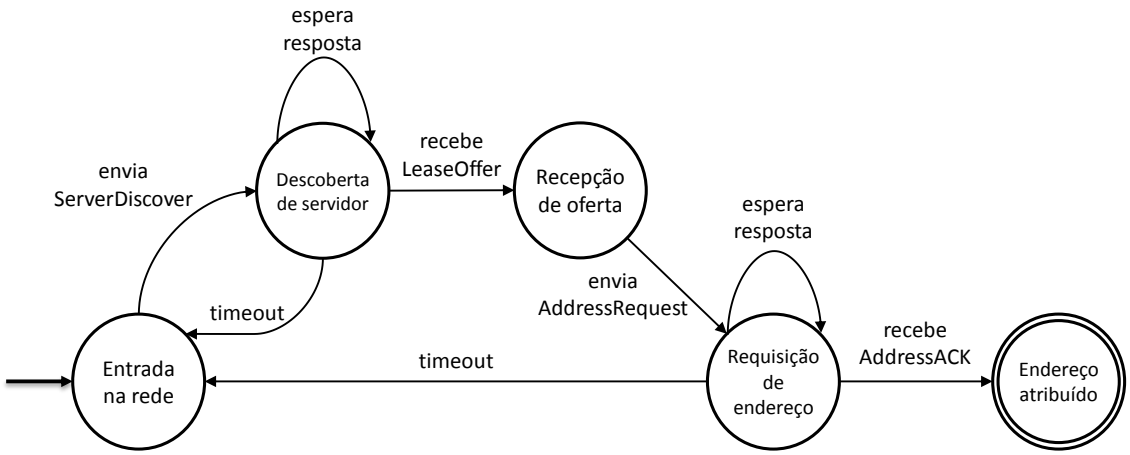


Figura 7.4: Máquina de estados do processo de negociação de endereço

uma mensagem de *LeaseOffer* de algum servidor, contendo um endereço de rede oferecido ao dispositivo, ele segue imediatamente para o estado de *Recepção de oferta*. Neste estado, o dispositivo cliente faz a requisição do endereço através do envio da mensagem *AddressReques* e prossegue para o estado de *Requisição de endereço*. Neste estado, o dispositivo espera a resposta de confirmação do endereço pelo servidor. Caso um temporizador de espera estoure, o dispositivo volta para o estado de *Entrada na rede* e inicia todo o processo novamente. Caso o dispositivo receba a mensagem de confirmação de endereço *AddressACK*, atualiza sua configuração local com o endereço que lhe foi alocado e entra no estado de *Endereço atribuído*. Neste estado final, o dispositivo já está apto a iniciar/continuar a sua comunicação na rede.

Formalização do método de negociação de endereços

O diagrama de estados e suas respectivas funções de transição ilustradas pela Figura 7.4 permitem a representação do processo de negociação de endereços do sistema de gerenciamento autonômico por meio de um *autômato finito determinístico* (AFD). Os AFDs são amplamente utilizados em modelagens de protocolos de redes devido a características como as transições entre estados [105]. As funções de transição são efetuadas por processamentos de condições de eventos, que quando satisfeitos, indicam uma mudança para um próximo estado do sistema. O determinismo do processo deve-se ao fato de sempre ser possível definir qual será o próximo estado, dado um evento ou valor de entrada. For-

malmente um autômato finito determinístico consiste em uma $5 - tupla$ $(Q, \sum, \delta, q0, F)$ onde:

- Q corresponde um conjunto finito de estados;
- $\sum$ consiste de um conjunto finito de símbolos de entrada chamado Alfabeto;
- $\delta : Q \times \sum \rightarrow Q$ compreende uma função de transição;
- $q0 \in Q$ indica um estado inicial;
- $F \subseteq Q$ representa um conjunto de estados de aceitação

Assim, seja $w = a1, a2, ..., an$ uma cadeia de símbolos sobre o alfabeto δ, o autômato aceita a cadeia w se e somente se existe uma sequência de estados, $r0, r1, ..., rn$, em Q com as seguintes condições:

$$r0 = q0$$
$$ri + 1 = \delta(ri, ai + 1), para\ i = 0, ..., n - 1$$
$$rn \in F$$

A primeira condição afirma que o autômato M começa no estado inicial $q0$. A segunda diz que, dado cada símbolo da entrada w, o autômato muda de estado em estado de acordo com a função de transição δ. A terceira e última condição diz que o autômato aceita w se e somente se o último símbolo da entrada leva o autômato a parar em um estado final f tal que $f \in F$. Caso contrário, diz-se que o autômato rejeita a entrada. O conjunto de cadeias que M aceita é chamado de *Linguagem* reconhecida por M e é simbolicamente representado por $L(M)$. O autômato finito determinístico M, que representa o processo de negociação de endereço é ilustrado pela Figura 7.5 é formalmente definido da seguinte forma:

- Um conjunto finito de estados $Q = \{I, D, O, R, E\}$, representando respectivamente o conjunto estados da máquina *M, {EntradaNaRede, DescobertaDeServidos, RecepçãoDeOferta, RequisiçãoDeEndereço. EndereçoAtribuido}*

- Alfabeto $\sum = \{d, o, r, a, w, t\}$, representando os eventos que ocorrem no sistema, *{EnviaServerDiscover, RecebeLeaseOffer, EnviaAddressRequest, RecebeAddressACK, EsperaResposta, TimeOut}*

- A função de transição ($\delta : Q \times \sum \rightarrow Q$), que compreende a aceitação das condições em que os eventos acontecem. A Tabela 7.1 ilustra todas as funções de transição do AFD.

		Entrada					
		d	o	r	a	w	t
Estados	I	D					
	D		O			D	I
	O			R			
	R				E	R	I
	E						

Tabela 7.1: Tabela de transição de estados de M

- O estado inicial $q0 = I$, tal que ($q0 \in Q$), representando o estado *EntradaNaRede*.

- O conjunto de estados de aceitação $F = E$, tal que ($F \subseteq Q$), representando o estado final *EndereçoAtribuído*.

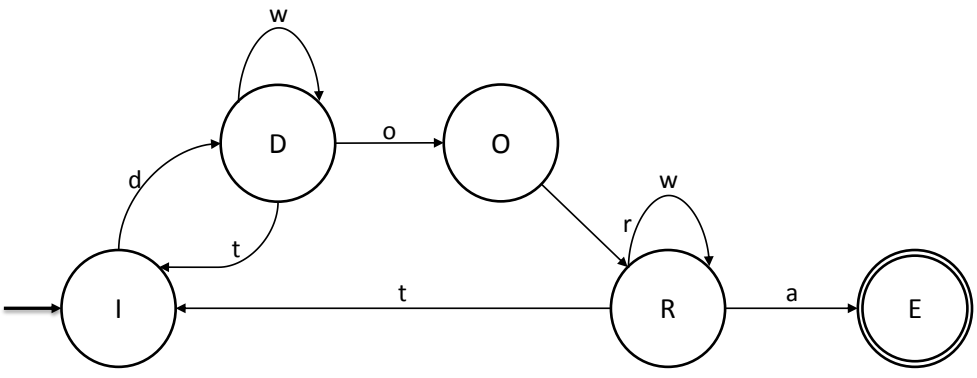


Figura 7.5: Autômato finito determinístico M

A gramática regular na *Forma Normal de Greibach* (FNG) que determina a linguagem reconhecida $L(M)$ aceita pelo AFD é ilustrada a seguir:

$I \rightarrow dD$

$D \rightarrow oO \mid wD \mid tI$

$O \rightarrow rR$

$R \rightarrow aE \mid wR \mid tI$

$E \rightarrow \epsilon$

De acordo com a gramática, estando no estado I e com a entrada de d o sistema vai para o estado D. No estado D com entrada o o sistema vai para o estado O ou com entrada w vai para o estado D, ou com entrada t retorna para o estado I. No estado O com entrada r vai para o estado R. No estado R com entrada a vai para o estado final E ou com entrada w permanece no estado R ou com entrada t retorna ao estado inicial I.

7.2.3 Arquitetura do sistema de gerência de endereçamento

O sistema de gerenciamento autonômico para o endereçamento dinâmico em rede heterogêneas sem fio foi projetado com dois módulos. O módulo *Cliente* e o módulo *Servidor*, como ilustrado na Figura 7.6. O módulo cliente é formado pelos componentes: *Condição de mudança, Configuração e Comunicação.* O componente de *Condição de mudança* recebe a decisão de transição de uma rede para a outra e inicia o processo de negociação de endereços fornecendo o $HosID$ do dispositivo, que será enviado para o servidor de endereço da rede de destino.

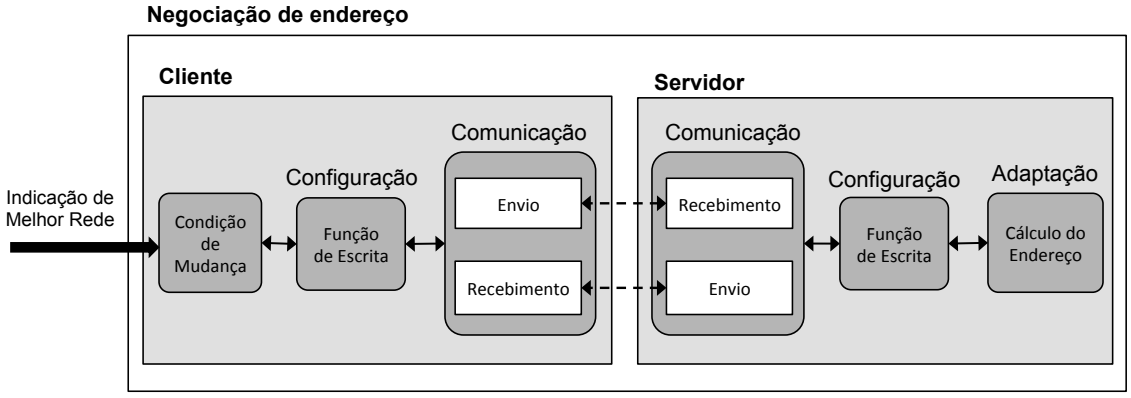


Figura 7.6: Arquitetura do sistema de negociação de endereço.

O componente de *Configuração*, formado por uma *Função de escrita* é responsável pela edição dos arquivos de configuração do sistema de endereçamento. O objetivo deste componente é efetuar as edições dos arquivos de configuração a fim de definir um novo endereço de acordo com as caraterísticas da rede de acesso, possibilitando ao dispositivo comunicação naquela rede. O componente de *Comunicação* é formado pelos elementos de envio e recebimento. Esses elementos são responsáveis pela troca de mensagens entre os módulos *Cliente e Servidor*, que atribui um novo endereço ao dispositivo em transição pela rede de acesso.

O módulo *Servidor* também possui um componente de *Comunicação* e outro de *Configuração* com as mesmas funcionalidades do módulo cliente. Um novo componente é adicionado, o componente de *Adaptação*. O componente de *Adaptação* é o responsável pelo processamento dos endereços que serão distribuídos ao dispositivos que solicitarem o acesso á rede. A adaptação dos novos endereços é realizada através de uma operação de *Cálculo de endereço*, que considera as partes relacionadas ao endereço do dispositivo (HosID) e o endereço da rede (NetID). Deste modo, o servidor processa um novo endereço que será atribuído ao dispositivo em transição, possibilitando o acesso a rede com a manutenção da conectividade.

7.3 Análise e avaliação

O projeto da arquitetura possibilitou a implementação do sistema de gerência para que análises de seu funcionamento fossem realizadas. O sistema foi implementado como um módulo do simulador de redes *Network Simulator 2* (NS-2), utilizando a linguagem de programação C++. O uso do simulador possibilitou a realização de testes de funcionamento do sistema em diferentes tipos de redes. A Figura 7.7, ilustra o diagrama de classe elaborado para o desenvolvimento do sistema.

O diagrama apresenta uma visão em alto nível das principais relações entre as classes e os módulos do NS-2 e os componentes criados para o desenvolvimento do sistema de gerência de endereços dinâmicos em redes heterogêneas. A implementação envolveu a criação de uma classe derivada da classe *Agent* do NS-2, para possibilitar a troca de

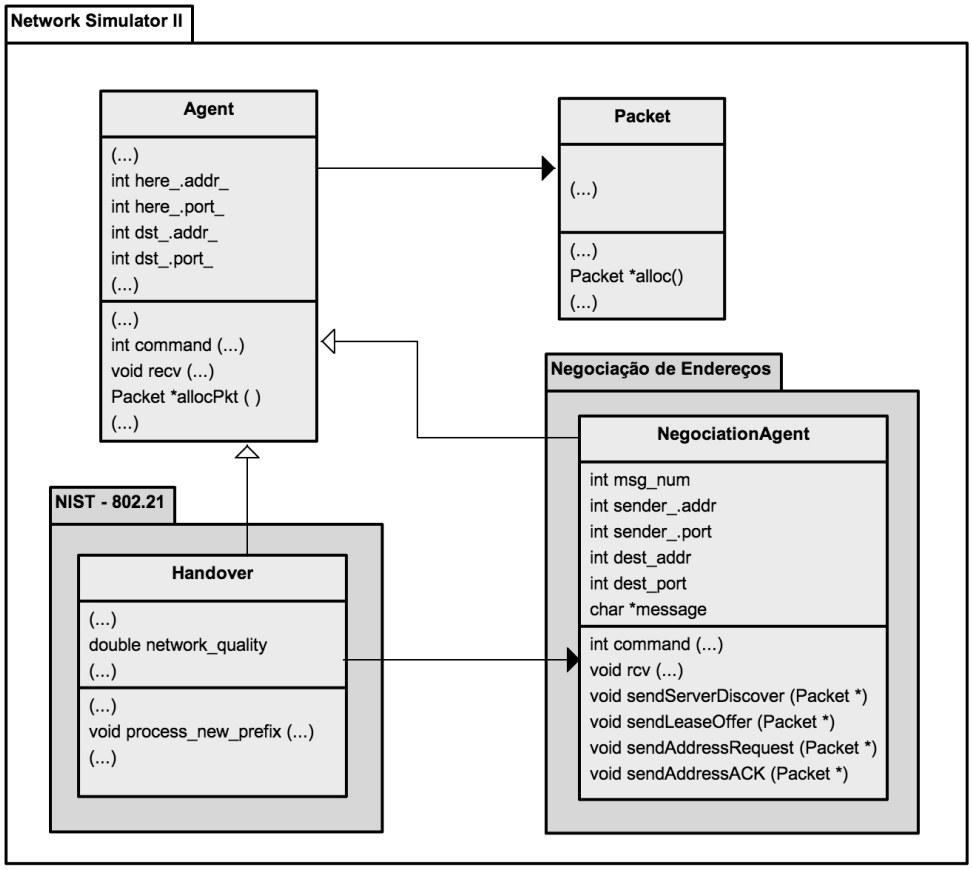


Figura 7.7: Diagram de classe da implementação do sistema de gerência de endereços

mensagens do processo de negociação de endereços. As funções que implementam essas mensagens realizam a alocação de pacotes com base na classe *Packet*, também pertencente ao NS-2. A classe *Handover*, que foi implementada pelo NIST [97, 98] é o componente que inicia o processo de negociação de endereços, enviando a condição de mudança ao módulo de negociação, logo que o processo de handover é iniciado. Diferentes métodos e funções foram implementadas para que o sistema de gerência realize o processo de negociação de endereços para dispositivos móveis em transição por redes de acesso heterogêneas sem fio.

7.3.1 Descrição dos cenários

A avaliação do sistema de gerência autonômica do serviço de endereçamento dinâmico em redes heterogêneas foi realizada considerando os três cenários distintos apresentados na Seção 6.3 e ilustrados na Figura 6.6. A Tabela 6.1 detalha os parâmetros utilizados em cada cenário. Assim como na Seção 6.3 também utilizaremos *i) BSR* para representar

o cenário 1, com baixa sobreposição de redes, *ii) MSR* para o cenário 2 com média sobreposição e *iii) ASR* para o cenário 3 com alta sobreposição de redes.

7.3.2 Discussão dos resultados

A avaliação do sistema de gerência foi realizada de acordo com os aspectos de eficácia e a eficiência. A métrica utilizada na avaliação da eficácia corresponde ao *Número de negociação de endereços*. Essa métrica verifica as negociações de endereçamento realizadas durante as transições dos usuários móveis de uma rede para outra. A avaliação da eficiência ocorre pela verificação do impacto que o sistema causa nas transmissões de dados da rede. As métricas utilizadas para essa avaliação são: *i) Tempo gasto para a realização das negociações de endereço*. Essa medida verifica se há uma sobrecarga na duração das negociações. *ii) Taxa de entrega* e a *iii) Latência*, que verificam a influência do processo de negociação de endereços nos fluxos de dados na rede.

Número de negociações de endereços

A Figura 7.8 ilustra o número de negociações de endereços ocorridos durante as simulações nos três cenários descritos. No cenário *BSR*, com baixa sobreposição de redes, o processo de negociação de endereços dos dispositivos móveis em transição teve o mesmo resultado, independentemente da velocidade dos dispositivos. Isso ocorre porque apenas duas redes sobrepostas existem no ambiente e por mais que haja variação da velocidade, os dispositivos só podem migrar sua conexão de uma rede para outra, independente de seu percurso.

No cenário *MSR*, devido ao maior número de redes sobrepostas, verificou-se que conforme a velocidade do dispositivo aumenta ocorre um acréscimo no número de negociação de endereços. Isso acontece porque o dispositivo móvel passa a detectar mais redes disponíveis em sua área de cobertura e sua velocidade de mobilidade faz com que a dissociação e associação às redes sejam frequentes, devido à constante entrada e saída da área de cobertura.

No cenário *ASR*, com baixa velocidade, mesmo que existam muitas redes sobrepostas

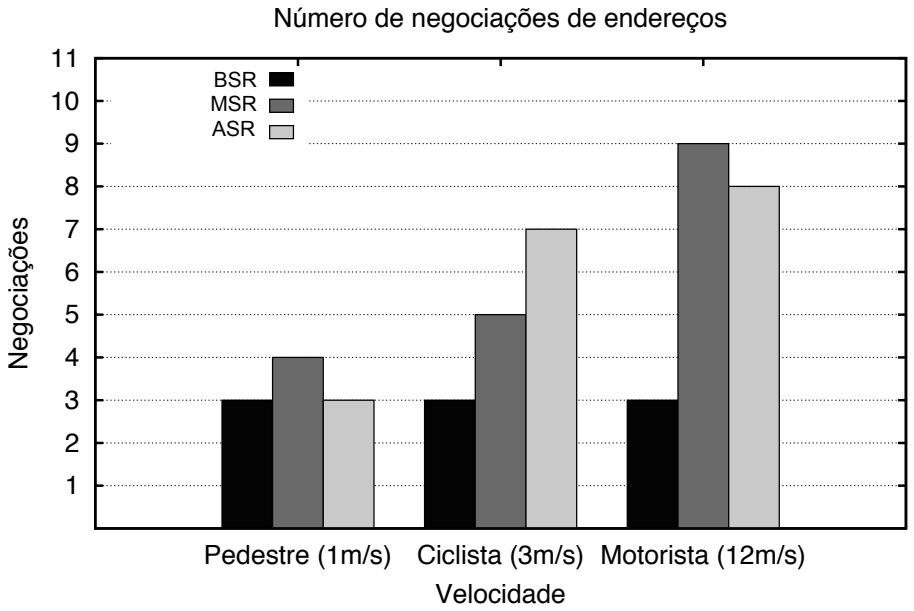


Figura 7.8: Avaliação do número de negociações de endereços

o número de negociações é baixo. Isso acontece porque o dispositivo não tem velocidade suficiente para se locomover por todas as áreas de cobertura das redes durante o tempo de simulação. Assim, com essa velocidade o dispositivo tem baixa mobilidade e realiza 3 negociações de endereços. Para o caso de velocidade de um ciclista o número de redes que o dispositivos consegue transitar aumenta, com isso também aumenta consideravelmente o número de negociações de endereços. Com a velocidade de um automóvel os resultados mostram que apesar da alta mobilidade em uma área de alta sobreposição de redes, os dispositivos permanece mais tempo conectado na mesma rede e assim realiza menos negociações do que se tivesse em uma área de média sobreposição. Isso mostra que a partir de um certo número de sobreposições de redes a velocidade já não tem forte influência no número de negociações de endereços.

Outro resultado obtido aponta a igualdade do número de negociações de endereçamento e o número de transições realizadas pelos dispositivos móveis. Esse resultado confirma que o processo de negociação de endereços ocorre toda vez que um dispositivos realiza a transição de uma rede para a outra, adaptando seu formato de endereço de acordo com as características da rede a qual irá se conectar. O gráfico da Figura 7.9 mostra os resultados obtidos para todos o cenários avaliados.

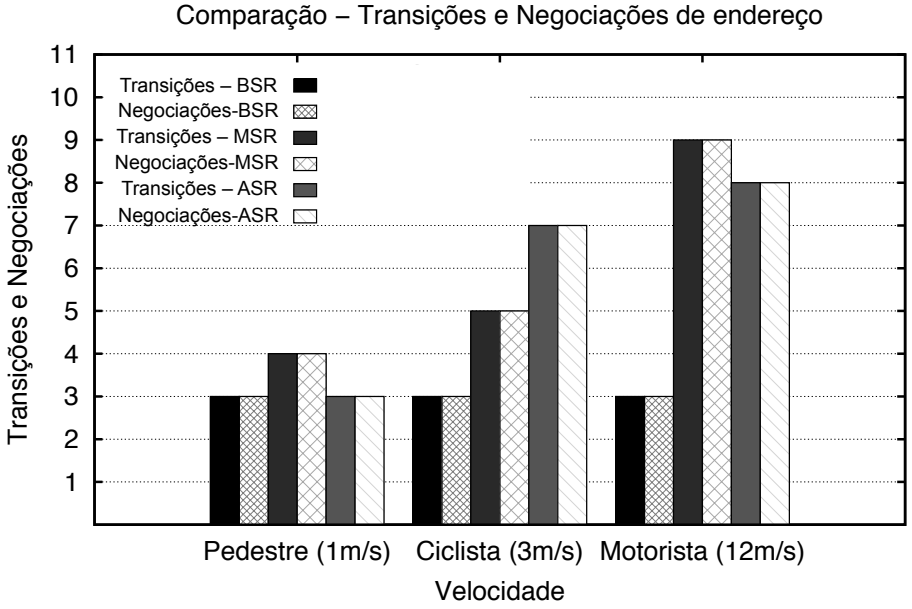


Figura 7.9: Comparação do número de transições × negociações de endereços

Tempo gasto para a realização das negociações de endereço

A avaliação do tempo gasto para a realização das negociações de endereço foi verificada sob dois aspectos. O primeiro, ilustrado na Figura 7.10, analisa o tempo gasto para negociação de endereços nos diferentes cenários de sobreposição de redes. Nesta análise é verificado que com baixa sobreposição de redes o tempo gasto para negociação de endereços oscilou e chegou perto de 0.9 segundos. Para o caso de média sobreposição os valores do tempo se mantiveram mais estáveis. Já para ambientes de alta sobreposição houve um pico próximo a 1 segundo. No entanto, foi possível verificar que o processo de negociação de endereços em redes heterogêneas não chegou a 1 segundo em nenhum dos cenários avaliados, o que mostra que a negociação de endereços não causa impacto significativo no tempo de transição das comunicações na rede.

A segunda avaliação verifica o tempo gasto para a realização das negociações de endereço dos dispositivos móveis em diferentes velocidades de mobilidade. A Figura 7.11 mostra os resultados desta avaliação. Como observado em velocidades de pedestre o tempo de negociação de endereços teve algumas oscilações devido à migração da conexão para redes de diferentes tecnologias, contudo o tempo não atingiu 0.9 segundos. No caso de um ciclista os valores do tempo foram mais estáveis, e permaneceram em sua grande

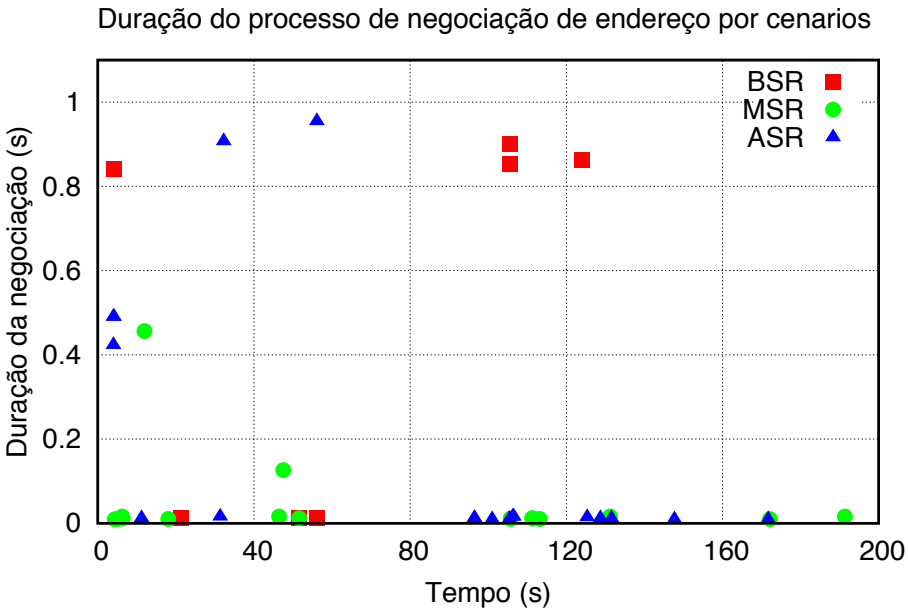


Figura 7.10: Avaliação do tempo de negociação em diferentes cenários

maioria abaixo de 0.2 segundos. Já para o motorista teve um pico próximo a 0.9 segundo no tempo de negociação de endereços, contudo em sua grande maioria seus valores ficaram bem abaixo de 0.2 segundos.

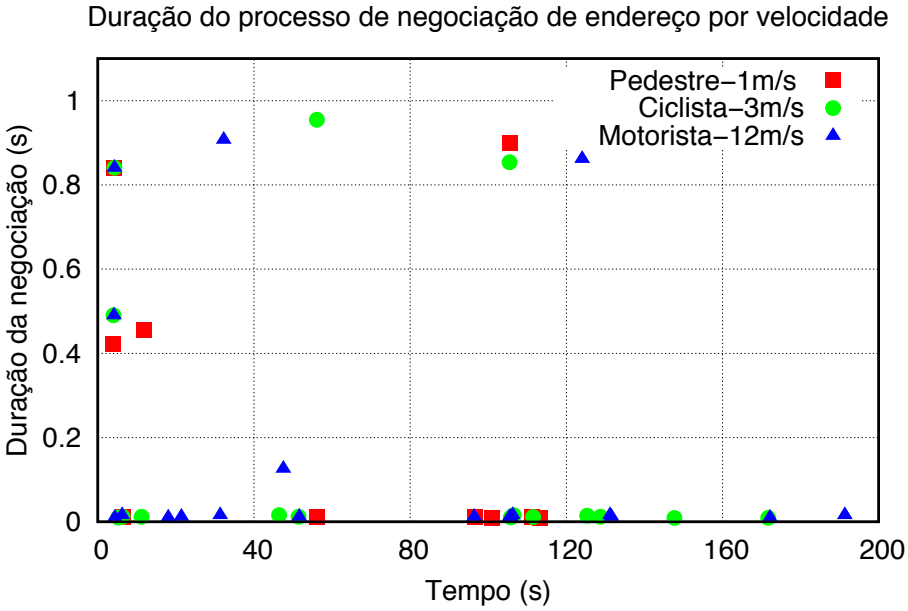


Figura 7.11: Avaliação do tempo de negociação em diferentes velocidades

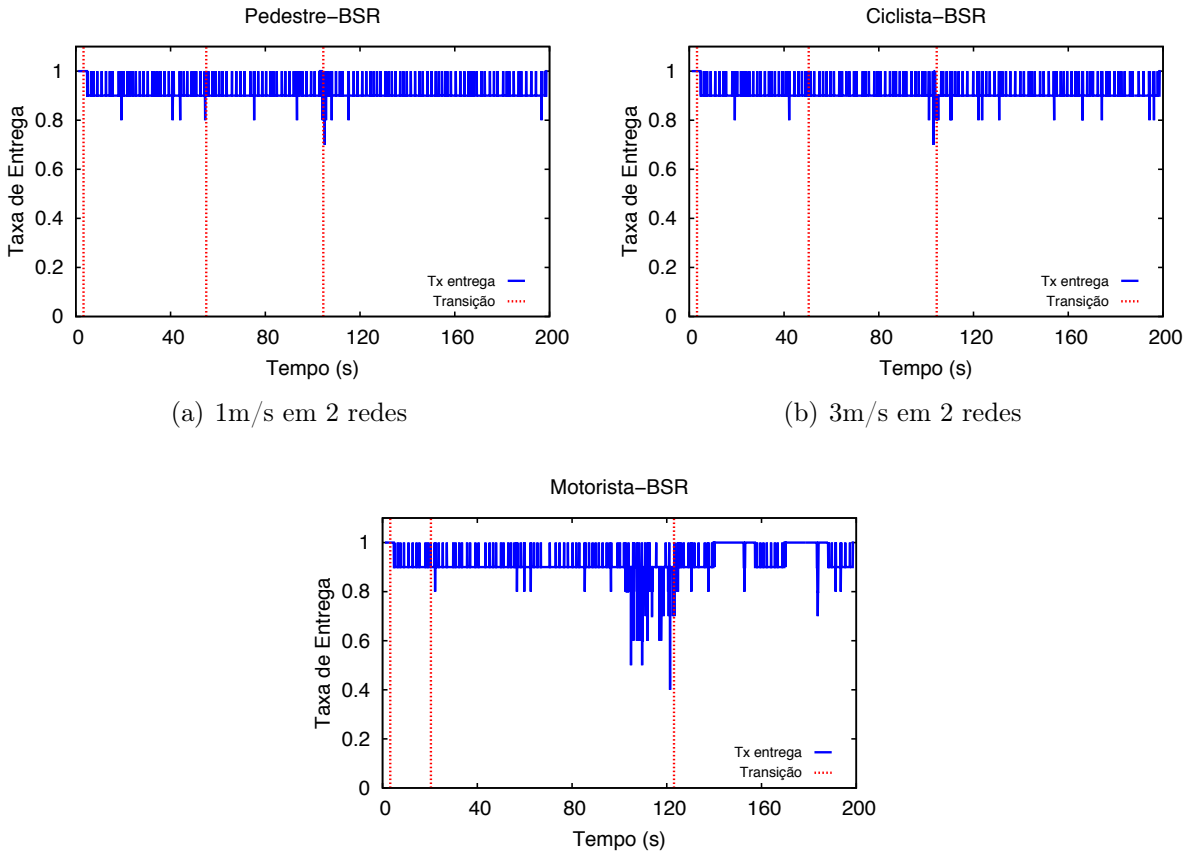
Taxa de entrega

A *Taxa de entrega* representa uma das métricas utilizadas para verificação do impacto que o processo de negociação de endereços causa na rede. A análise da taxa de entrega, Figura 7.12, verifica as condições da rede antes, durante e depois da negociação de endereço realizada pelo sistema apresentado. O momento de transição de uma rede para outra e consequentemente a negociação de endereços é representada pelas linhas pontilhadas nos gráficos.

Em cenários de *BSR e MSR* a taxa de entrega possui valores similares, ilustrados nas Figuras 7.12(a) e 7.12(b). Nestes cenários, são similares as variações antes e após o processo de negociação. Esse resultado foi observado independente da velocidade do dispositivo móvel. Na Figura 7.12(c) a variação é maior depois do processo de negociação de endereço, o que pode ser explicado pela característica da rede para a qual o dispositivo migrou. Esse comportamento mostra que a variação da taxa de entrega é influenciada pela característica da rede a qual o dispositivo se conecta e não pelo processo de negociação de endereço.

Em cenários de *MSR*, Figura 7.13, nota-se que as variações da taxa de entrega ocorrem próximas aos processos negociação de endereço. Contudo, em nenhum momento o processo de negociação de endereços influencia essa métrica, que foi afetada devido à migração de uma rede para outra, como nos casos anteriores. Para mobilidade de pedestre, Figura 7.13(a), a taxa de entrega oscilou de acordo com as condições das redes. A medida que o dispositivo migrou para uma rede mais estável seu valor de taxa de entrega também se estabilizou. Para mobilidade de ciclista, Figura 7.13(b), a taxa de entrega se manteve constante, independente das transições realizadas, com apenas alguns instantes de variações. Já para dispositivos com alta mobilidade, Figura 7.13(c), as variações da taxa de entrega foram as maiores observadas. Isso ocorre porque a alta mobilidade influencia no número de transições para diferentes redes e cada rede possui diferentes condições e características de funcionamento, afetando os valores da taxa de entrega.

No cenário *ASR* é possível notar através da Figura 7.14 que quanto maior a velocidade, mais negociações ocorrem, e consequentemente a taxa de entrega tem maior variação.



(a) 1m/s em 2 redes

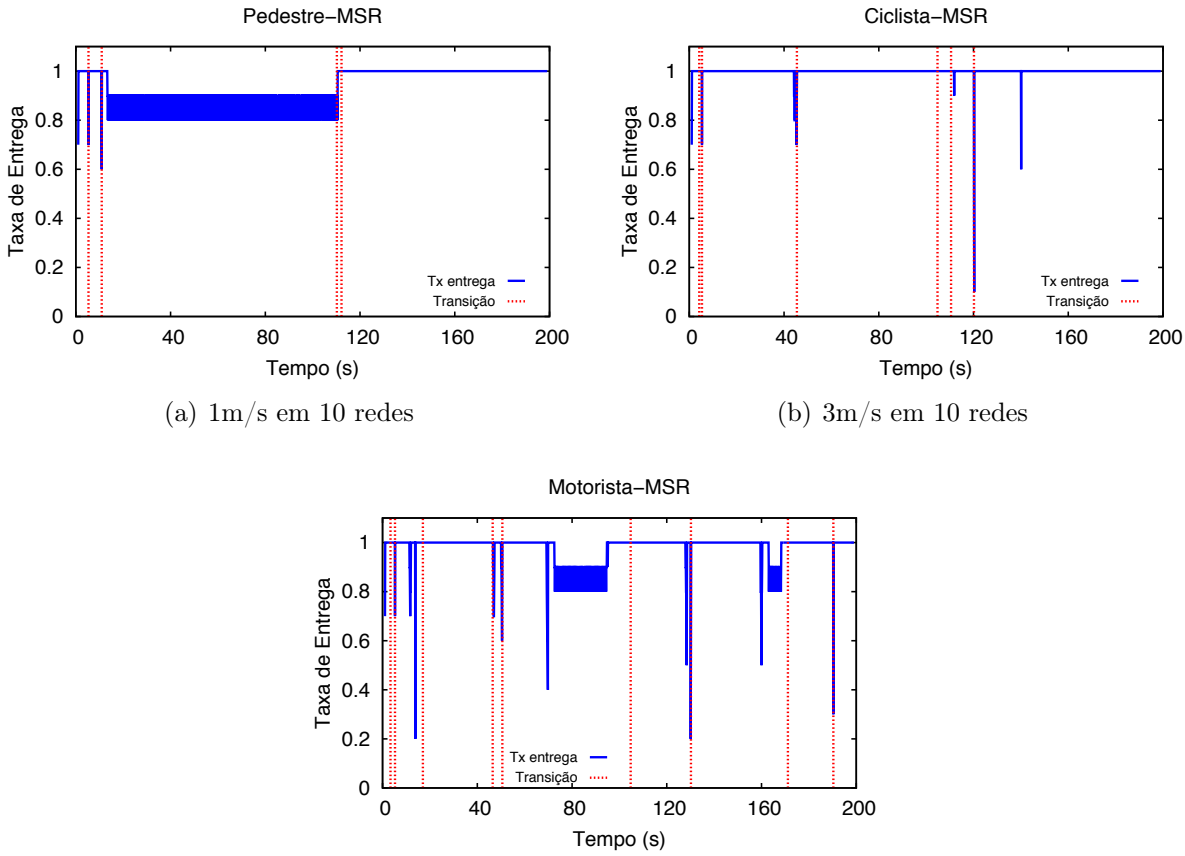
(b) 3m/s em 2 redes

(c) 12m/s em 2 redes

Figura 7.12: Avaliação da taxa de entrega no cenário 1

Para velocidades de pedestre, Figuras 7.14(a), existe uma certa estabilidade da taxa de entrega do dispositivo, que é afetada à medida que sua conexão migra de uma rede para outra de tecnologia de comunicação diferente. No caso do ciclista, Figuras 7.14(b), o mesmo comportamento foi verificado, contudo maiores variações ocorrem em razão do aumento das transições causadas pela velocidade do dispositivo em alta sobreposição de redes. Para o motorista, Figura 7.14(c), as variações da taxa de entrega foram superiores para o cenário *ASR*. A velocidade de mobilidade dos dispositivos faz com sejam realizadas mais transições e consequentemente mais alterações da taxa de entrega.

Ao se comparar a taxa de entrega e a duração do processo de negociação de endereço nota-se que a redução da taxa de entrega não é diretamente relacionada ao processo de negociação, mas sim pelas características da rede à qual se conecta. Isso ocorre devido à maior troca de informações entre o dispositivo e as redes, como os eventos *Link Detected, Link Up e Link Down*, que são realizados à medida que novas redes são detectadas na



(a) 1m/s em 10 redes

(b) 3m/s em 10 redes

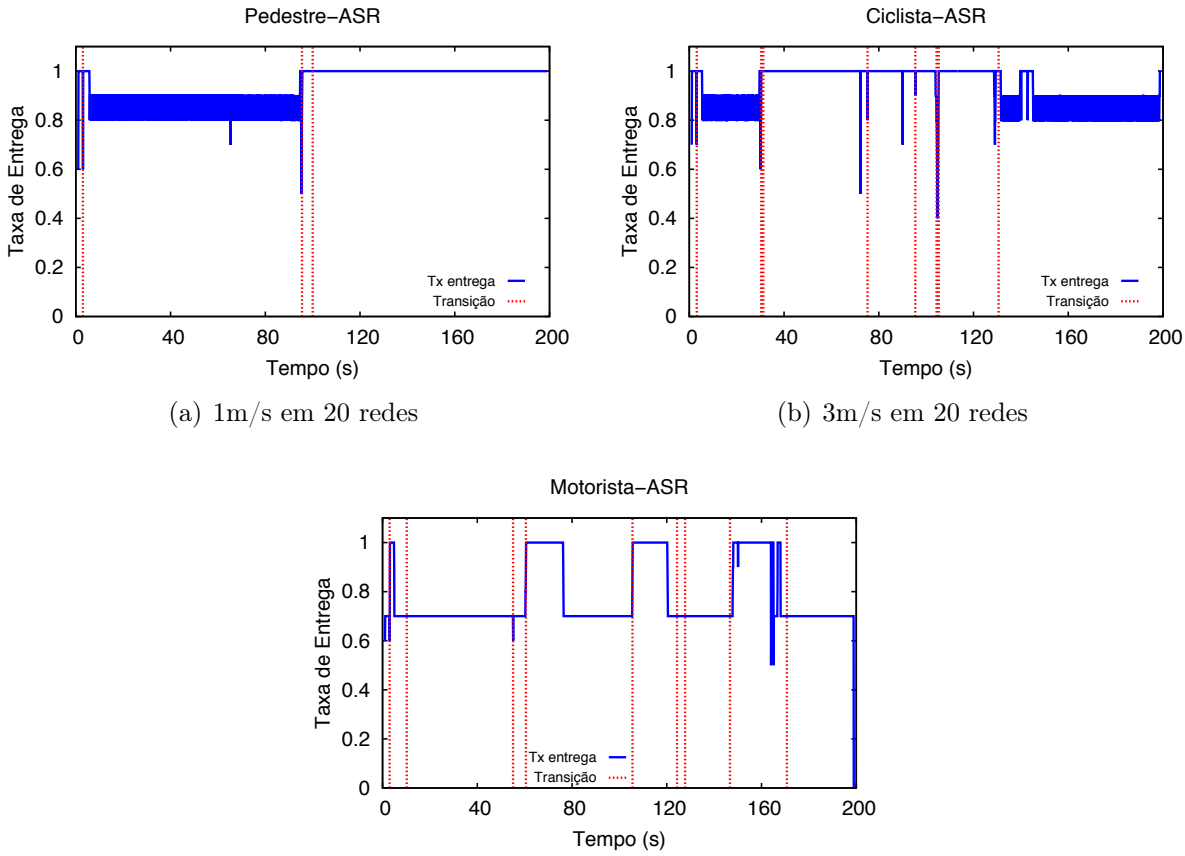
(c) 12m/s em 10 redes

Figura 7.13: Avaliação da taxa de entrega no cenário 2

mesma área de cobertura. Esses eventos iniciam o processo de avaliação das condições da rede para uma possível transição do acesso para a melhor rede disponível. Os resultados desta análise da eficiência do sistema de endereçamento mostram que a taxa de entrega não é diretamente influenciada pelo processo de negociação de endereços e sim pelas características da rede a qual é feita a transição de conexão.

Latência

A *Latência* é outra métrica utilizada para a análise da eficiência e verificação do impacto do processo de negociação nos fluxos de dados da rede. No cenário *BSR* ilustrado na Figura 7.15 a latência se manteve com poucas variações após a transição de uma rede para outra. Nos casos de velocidade de um pedestre, Figura 7.15(a) e ciclista, Figura 7.15(b) a latência foi mantida em aproximadamente 0.5s. Os resultados foram bem parecidos



(a) 1m/s em 20 redes

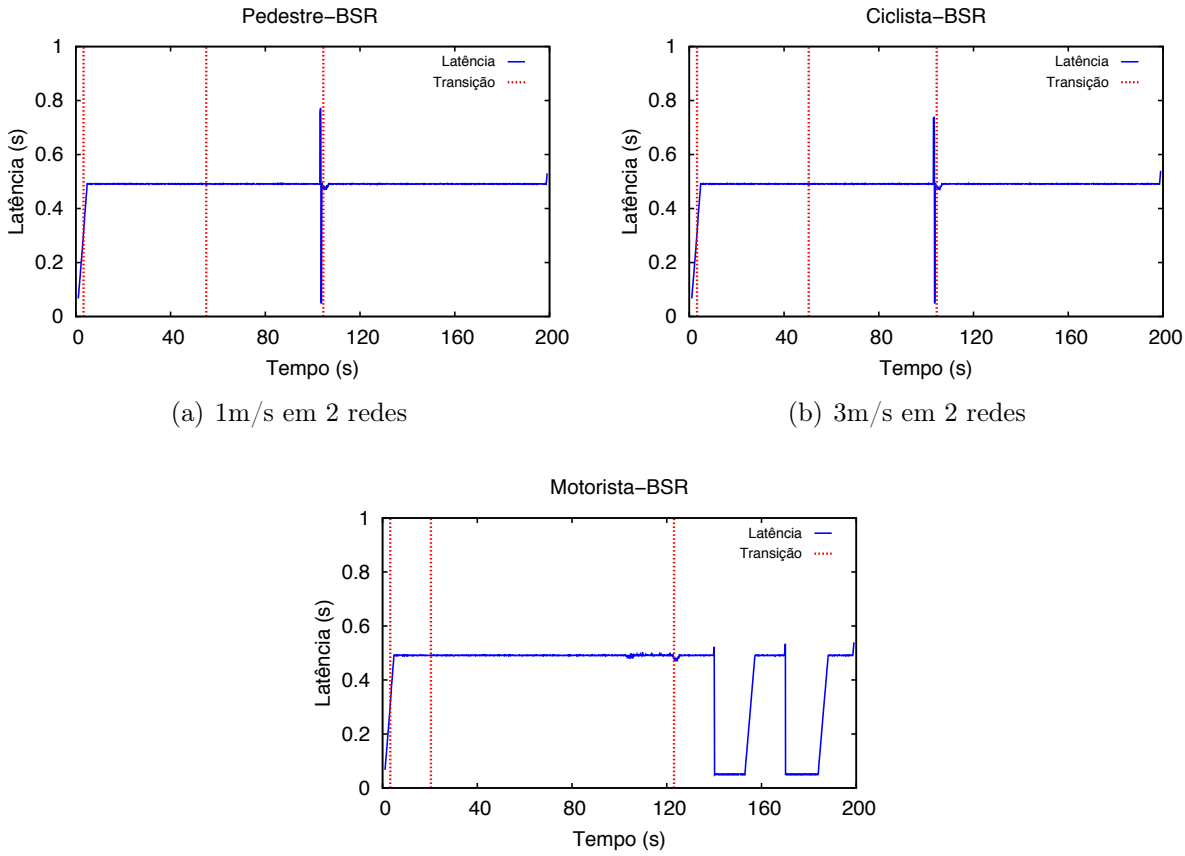
(b) 3m/s em 20 redes

(c) 12m/s em 20 redes

Figura 7.14: Avaliação da taxa de entrega no cenário 3

devido à proximidade da velocidade do dispositivos, causando pequeno impacto na rede. Já nos casos de velocidade de um motorista Figura 7.15(c) a latência oscilou mais devido à transição e manutenção de conexão para uma rede com diferentes condições, como por exemplo, maior vazão. A medida que o dispositivo se conecta em redes com condições diferentes das anteriores passa a ficar sujeito à sua característica.

No cenário *MSR*, ilustrado na Figura 7.16 a latência também teve variações em relação as condições da nova rede para à qual foi feita a transição de conexão. A Figura 7.16(a) mostra o caso de um pedestre que teve variação dos resultados à medida que migra sua conexão de um rede para outra de diferente tecnologia de comunicação. Contudo, em momentos que a transição foi feita entre redes de mesma tecnologia o valor da latência se manteve estável, como ilustrado na Figura 7.16(b) em que um ciclista transita por redes de mesma tecnologia. Em casos de alta mobilidade do dispositivo, ilustrado pela Figura 7.16(c), a velocidade do dispositivo móvel tem forte influência na variação dos resultados,



(a) 1m/s em 2 redes

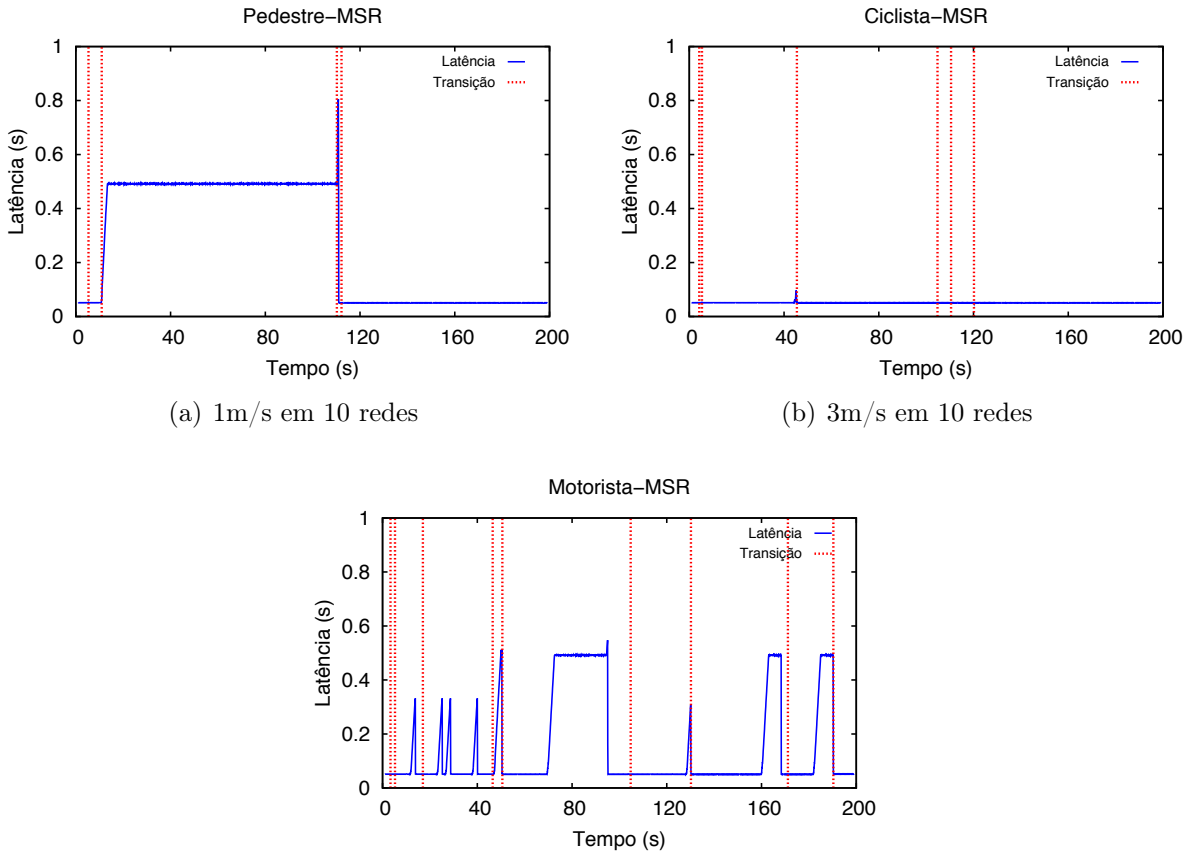
(b) 3m/s em 2 redes

(c) 12m/s em 2 redes

Figura 7.15: Avaliação da latência no cenário 1

que oscilam constantemente independente das transições realizadas.

O cenário *ASR* tem a latência afetada pela transição de uma rede para outra, similarmente ao que acontece com a taxa de entrega, onde a tecnologia da rede determina suas características e condições de funcionamento. Essa variação teve um acréscimo à mediada que a velocidade do dispositivo aumentava. A Figura 7.17(a) que representa a mobilidade de um pedestre, ilustra uma variação na latência à medida que o dispositivo migra sua conexão de uma rede para outra de diferente tecnologia de comunicação. Devido sua baixa mobilidade, a permanência na mesma rede após à migração diminui o numero de negociações de endereço e reduz a variação de latência. A Figura 7.17(b) mostra um comportamento similar a da Figura 7.17(a). Contudo, em razão da maior mobilidade o dispositivo realiza mais transições entre as redes e sua variação da latência é maior. Já em situações de alta mobilidade, Figura 7.17(c), o número de transições de uma rede para outra é maior e consequentemente a variação na latência também.



(a) 1m/s em 10 redes

(b) 3m/s em 10 redes

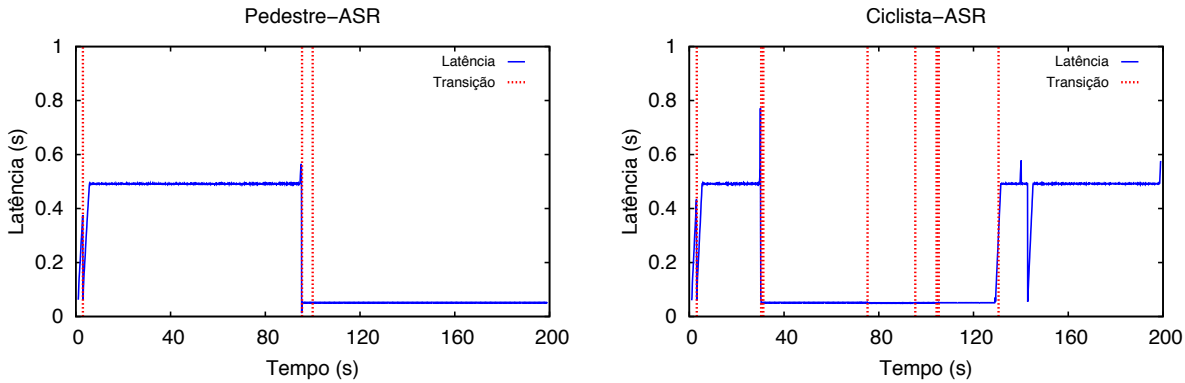
(c) 12m/s em 10 redes

Figura 7.16: Avaliação da latência no cenário 2

Os resultados da avaliação da eficiência do sistema de gerência mostram que o processo de negociação de endereçamento não causa impacto no fluxo de dados das redes. A *Taxa de entrega* e a *Latência* não sofrem influências da execução do sistema de gerência autonômica de endereçamento dinâmico. Os resultados indicam que essas métricas são afetadas apenas pelas características de cada rede e não pelo processo realizado na adaptação do endereço dos dispositivos móveis, em transição pelas redes de acesso heterogêneas.

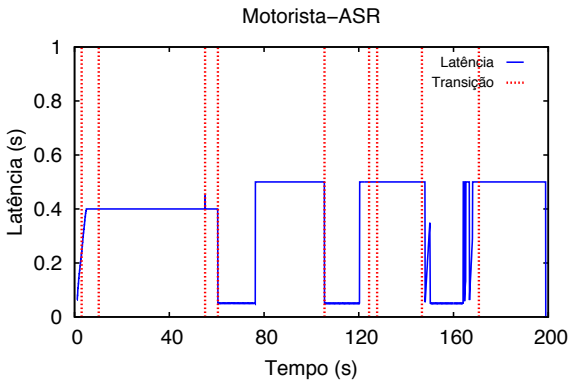
7.4 Resumo

Esse capítulo apresentou uma estratégia de gerência autonômica do serviço de endereçamento dinâmico em redes de acesso heterogêneas. Foram discutidos os fundamentos do processo de gerência do serviço de endereçamento e foi apresentado um sistema que utiliza princípios da computação autonômica para gerenciar os endereços dos dispositivos



(a) 1m/s em 20 redes

(b) 3m/s em 20 redes



(c) 12m/s em 20 redes

Figura 7.17: Avaliação da latência no cenário 3

em trânsito de uma rede para outra. Foi apresentado a arquitetura do sistema proposto, bem como uma análise e avaliação de sua eficácia e eficiência. Os resultados mostraram que o sistema não causou impacto nos fluxos de dados dos dispositivos da rede e seu funcionamento foi eficaz na garantia de conectividade contínua de dispositivos em trânsito de uma rede para outra independente da tecnologia de comunicação.

CAPÍTULO 8

CONCLUSÕES

Este capítulo resume as conclusões da teses e apresenta direções futuras. O objetivo é o de reforçar as contribuições alcançadas e apontar algumas direções para prosseguir com novas investigações. A Seção 8.1 discute os objetivos e resultados alcançados na tese, e a Seção 8.2 aponta direções para trabalhos futuros.

8.1 Objetivos e resultados

Essa tese abordou os desafios relacionados à manutenção de conectividade durante a transição dos dispositivos móveis por redes de acesso heterogêneas. As propostas existentes apresentam abordagens ineficientes sobre o gerenciamento da garantia de conectividade e impróprios sob o aspecto de segurança, visto que elas atuam de forma individualizada não condizentes com as futuras infra-estruturas de redes convergentes. Neste sentido, destaca-se a necessidade de supervisão e controle de modo autonômico e auto-organizável da transição em rede de acesso adequada e segura ao estabelecimento de conexão. Essas redes estão sujeitas às vulnerabilidades e ataques que podem ser explorados pela seleção equivocada da rede de acesso e de dispositivos móveis candidatos à conexão.

A mobilidade do usuário com manutenção de conectividade, independente da tecnologia de rede de acesso para à qual os dispositivos estiverem associados garante o suporte a diversos serviços que demandam por alta conectividade, como a computação em nuvem, que depende de uma infraestrutura robusta de comunicação. A conectividade contínua também permite que os usuários usufruam de recursos da internet durante seu trânsito de um local para o outro, além de possibilitar o acesso a um grande volume de dados com velocidade confiabilidade e facilidade, etc. Contudo, as adversidades de segurança como as vulnerabilidades e ataques específicos de cada tipo de rede podem ser proliferados por todo ambiente convergente, devido à integração de redes heterogêneas, afetando direta-

mente os usurários, seus dispositivos, serviços e a rede. O perfil nômade dos usuários móveis que transitam de uma rede para outra representa um fator decisivo na propagação e contaminação da rede por *vírus, worms, spywares, etc.* Por outro lado, redes completamente boicotadas por atacantes mal intencionados podem ser oferecidas aos usuários legítimos com alto índice de conectividade mas que são propícias a fraudes, ataques e roubo de dados confidenciais.

A concepção de uma abordagem segura de gerenciamento da seleção de melhor rede de acesso em ambientes heterogêneos, com suporte a mobilidade com manutenção de conectividade é fundamental para proporcionar a continuidade das comunicações, mesmo quando usuários móveis migrem de uma rede para outra. Nesta tese foi apresentada uma arquitetura para o gerenciamento de conectividade segura e contínua em redes de acesso heterogêneas. Essa arquitetura possui princípios autônomos e adaptativos para aferir indicadores de segurança da rede e dos dispositivos em transição de modo a oferecer uma migração entre redes, possibilitando a continuidade do acesso em ambientes heterogêneos.

A arquitetura apresentada contempla todas as fases de seleção e transição entre redes de acesso heterogêneas. O processo é iniciado com uma coleta de dados das condições das redes disponíveis, utilizando informações de contexto de diferentes critérios. Posteriormente mecanismos de inferência com base em abordagens multicritério são empregados para inferir a melhor escolha e estratégias de transição são aplicadas para efetivar a migração de acesso em diferentes redes com a manutenção da conectividade. A supervisão e controle do processo de transição é realizada de modo autonômico e adaptativo sem a necessidade de intervenção manual.

A arquitetura apresentada considera que a composição de métricas de segurança para a uma avaliação preliminar das condições da rede e dos dispositivos móveis são fundamentais para a escolha adequada da rede de acesso e dos dispositivos candidatos a conexão. O uso da quantificação das estratégias de segurança para avaliar as condições da redes permite a composição de indicadores importantes no processo de decisão. A decisão de acesso a partir desses indicadores pode evitar a conexão em redes inseguras e o comprometimento da continuidade dos serviços. Assim, a arquitetura de gerenciamento de

conectividade apresentada faz uso desta abordagem para garantir conectividade contínua, segura, confiável e com suporte a mobilidade dos dispositivos que transitam de uma rede para outra.

A consolidação do funcionamento da arquitetura projetada foi realizada através do desenvolvimento de serviços referentes aos seus módulos e componentes. A aferição da resiliência de conectividade de redes heterogêneas foi realizada para representar o indicador de segurança utilizado no processo de seleção da melhor rede de acesso. A análise e avaliação deste serviço utilizou dados de redes reais com topologias de conectividade dinâmicas e estáticas. Os resultados mostraram que a métrica utilizada para avaliação da resiliência da conectividade da rede pôde ser calculada de forma precisa e sua representação das condições de segurança da rede auxilia no gerenciamento de decisão de melhor acesso em ambientes de redes heterogêneos.

O serviço de decisão de melhor acesso em redes heterogêneas corresponde o módulo de decisão da arquitetura de gerenciamento de conectividade contínua e segura. Esse serviço utiliza estratégia multicritério para decidir o melhor acesso em ambientes de redes sobrepostas. As decisões são realizadas priorizando critérios e métricas relacionadas às condições de segurança das redes. Os resultados indicam uma redução do número de transições desnecessárias e uma decisão de migração de acesso entre redes seguras e com conectividade contínua.

A gerência do serviço de endereçamento em redes heterogêneas foi desenvolvida com o objetivo de controlar as negociações de troca de endereços dos dispositivos que se conectam em redes de acesso distintas. Esse serviço garante que apesar das transições de uma rede para outra os fluxos de dados dos dispositivos não são interrompidos. Princípios da computação autonômica são utilizados para evitar a intervenção humana no gerenciamento da rede. Os resultados mostram que a negociação de endereços dos dispositivos móveis não causa impacto no processo de transição e nem no desempenho da rede.

Os resultados obtidos a partir de cada serviço referente aos módulos da arquitetura apresentada demonstram sua eficácia na manutenção da conectividade segura durante a transição em redes de acesso heterogêneas. O uso de indicadores de segurança no processo

de decisão de conexão garante uma transição mais confiável. A escolha de melhor rede utilizando uma estratégia de decisão multicritério combinando métricas de segurança, desempenho e QoS é mais justa e completa. A utilização do gerenciamento autonômico do serviços de endereçamento garante a manutenção da conectividade à dispositivos móveis em transição por redes heterogêneas.

8.2 Trabalhos futuros

Esta pesquisa levantou muitas questões que merecem mais investigação. Uma série de trabalhos futuros podem ser explorados para o aperfeiçoamento da arquitetura de gerenciamento de conectividade segura e contínua em redes heterogêneas. Uma lista não exaustiva de possibilidades de novas pesquisas é apresentada, de acordo com o conjunto de serviços pertinentes à arquitetura.

- **Indicadores de segurança de redes de acesso heterogêneas**. As questões relacionadas à segurança no processo de transição em redes de acesso heterogêneas ainda são pouco exploradas. Novos critérios e métricas de segurança devem ser discutidos como forma de avaliação das condições das redes e utilizadas na decisão e escolha do acesso. Estratégias que garantam proteção e defesa ao processo de decisão de acesso também representam desafios a serem superados. Os princípios como confidencialidade, integridade e disponibilidade dos serviços utilizados no momento das transições de uma rede para outra representam pontos a serem atacados.

- **Estratégias de decisão de melhor acesso em ambientes de redes heterogêneas**. Novos métodos e técnicas de decisão devem ser exploradas a fim de encontrar soluções eficientes e adequadas às características dos ambientes heterogêneos, que possuem alta dinamicidade. Um estudo das diferentes técnicas pode indicar a melhor estratégia para a tomada de decisão, bem como otimizar seu desempenho para que as escolhas sejam rápidas e eficazes. Abordagens heurísticas também podem ser aplicadas para maximizar a eficiência do processo.

- **Gerenciamento de serviços relacionados à troca de mensagens em redes**

heterogêneas. Diferentes serviços relacionados a comunicação entre os dispositivos móveis e as estações provedoras de acesso podem ser investigados sob o aspecto de gerenciamento. O monitoramento e controle da conectividade dos dispositivos móveis em transição por redes heterogêneas deve ser explorado em novos trabalhos. Estratégias de gerência tanto dos dispositivos quanto das redes de acesso apresentam uma ampla gama de possibilidades.

- **Coleta de informações significativas das condições da rede**. Este serviço demanda por investigações de estratégias distribuídas e colaborativas de coleta de informações das condições das redes de acesso. Abordagens que consigam explorar a rede a fim de obter informações relevantes que possam ser utilizadas para auxiliar o processo de tomada de decisão de acesso na melhor rede são necessárias. Essas abordagens devem considerar o caráter dinâmico das redes bem como sua heterogeneidade de tecnologias de comunicação.

- **Execução de transições em redes heterogêneas**. Pesquisas experimentais podem ser realizadas a fim de aprofundar o conhecimento do processo de transição de acesso entre redes de diferentes tecnologias de comunicação. Estratégias que integrem o máximo de tecnologias de redes possíveis ampliarão o leque de possibilidades de uma manutenção de conectividade de dispositivos móveis. Trabalhos que tratem do controle das transições entre as redes também são promissores.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Subharthi Paul, Jianli Pan, and Raj Jain. Architectures for the future networks and the next generation internet: A survey. *Computer Communications*, 34(1):2–42, 2011.

[2] Marinho Pilla Barcellos. Desafios e tendências em segurança na internet do futuro. In *Workshop Futuro da Internet*. CPqD, 2009.

[3] Tomonori Aoyama. A new generation network: Beyond the internet and ngn. *IEEE Communications Magazine*, 47(5):82–87, 2009.

[4] J. Pan, S. Paul, and R. Jain. A survey of the research on future internet architectures. *IEEE Communications Magazine*, 49(7):26–36, 2011.

[5] B. Ahlgren, P.A. Aranda, P. Chemouil, S. Oueslati, L.M. Correia, H. Karl, M. Sollner, and A. Welin. Content, connectivity, and cloud: ingredients for the network of the future. *IEEE Communications Magazine*, 49(7):62–70, 2011.

[6] Daniel F. Macedo, Aldri Luiz dos Santos, and Guy Pujolle. From tcp/ip to convergent networks: challenges and taxonomy. *IEEE Communications Surveys Tutorials*, 10(4):40–55, 2008.

[7] R. Berezdivin, R. Breinig, and R. Topp. Next-generation wireless communications concepts and technologies. *IEEE Communications Magazine*, 40(3):108–116, 2002.

[8] R. Kuhne, G. Huitema, and G. Carle. Charging and billing in modern communications networks - a comprehensive survey of the state of the art and future requirements. *IEEE Communications Surveys Tutorials*, 14(1):170–192, 2012.

[9] Z. Ahmed, H. Jamal, R. Mehboob, S. Khan, and M. Shahbaz. Secure cognitive mobile hotspot. *IEEE Transactions on Consumer Electronics*, 56(2):606–612, 2010.

[10] M.R. Wigan and R. Clarke. Big data's big unintended consequences. *IEEE Computer*, 46(6):46–53, 2013.

[11] V.P. Kafle, H. Otsuki, and M. Inoue. An id/locator split architecture for future networks. *IEEE Communications Magazine*, 48(2):138–144, 2010.

[12] Lusheng Wang and Geng Sheng. Mathematical modeling for network selection in heterogeneous wireless networks – a tutorial. *IEEE Communications Surveys & Tutorials*, 15(01):271–292, 2013.

[13] Peng Lin, Jin Zhang, Yanjiao Chen, and Qian Zhang. Macro-femto heterogeneous network deployment and management: From business models to technical solutions. *IEEE Wireless Communications*, 18(3):64–70, 2011.

[14] Malamati Louta and Paolo Bellavista. Bringing always best connectivity vision a step closer: challenges and perspectives. *IEEE Communications Magazine*, 51(2):158–166, 2013.

[15] Daojing He, Chun Chen, Jiajun Bu, S. Chan, and Yan Zhang. Security and efficiency in roaming services for wireless networks: challenges, approaches, and prospects. *IEEE Communications Magazine*, 51(2):142–150, 2013.

[16] Robson Melo, Aldri Santos, Michele Nogueira, and Deep Medhi. *Anais 31 Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, chapter Modelagem e projeto de redes sem fio heterogêneas, resilientes e sobreviventes, pages 1–50. Sociedade Brasileira de Computação (SBC), 2013.

[17] Haoming Li, J. Hajipour, A. Attar, and V.C.M. Leung. Efficient hetnet implementation using broadband wireless access with fiber-connected massively distributed antennas architecture. *IEEE Wireless Communications*, 18(2):72–78, 2011.

[18] D. Lopez Perez, I. Guvenc, G. De la Roche, M. Kountouris, T.Q.S. Quek, and Jie Zhang. Enhanced intercell interference coordination challenges in heterogeneous networks. *IEEE Wireless Communications*, 18(3):22–30, 2011.

[19] A. Prasad, O. Tirkkonen, P. Lunden, O.N.C. Yilmaz, L. Dalsgaard, and C. Wijting. Energy-efficient inter-frequency small cell discovery techniques for lte-advanced heterogeneous network deployments. *IEEE Communications Magazine*, 51(5):72–81, 2013.

[20] Weisi Guo, Siyi Wang, Xiaoli Chu, Jie Zhang, Jiming Chen, and Hui Song. Automated small-cell deployment for heterogeneous cellular networks. *IEEE Communications Magazine*, 51(5):46–53, 2013.

[21] H Raza. A brief survey of radio access network backhaul evolution: part i. *IEEE Communications Magazine*, 49(6):164–171, 2011.

[22] H. Raza. A brief survey of radio access network backhaul evolution: part ii. *IEEE Communications Magazine*, 51(5):170–177, 2013.

[23] Mugen Peng, Yang Liu, Dongyan Wei, Wenbo Wang, and Hsiao-Hwa Chen. Hierarchical cooperative relay based heterogeneous networks. *IEEE Wireless Communications*, 18(3):48–56, 2011.

[24] Shu ping Yeh, S. Talwar, Geng Wu, N. Himayat, and K. Johnsson. Capacity and coverage enhancement in heterogeneous networks. *IEEE Wireless Communications*, 18(3):32–38, 2011.

[25] S. Buljore, H. Harada, S. Filin, P. Houze, K. Tsagkaris, O. Holland, K. Nolte, T. Farnham, and V. Ivanov. Architecture and enablers for optimized radio resource usage in heterogeneous wireless access networks: The ieee 1900.4 working group. *IEEE Communications Magazine*, 47(1):122–129, 2009.

[26] A. Ghosh, N. Mangalvedhe, R. Ratasuk, B. Mondal, M. Cudak, E. Visotsky, T.A. Thomas, J.G. Andrews, P. Xia, H-S Jo, H.S. Dhillon, and T.D. Novlan. Heterogeneous cellular networks: From theory to practice. *IEEE Communications Magazine*, 50(6):54–64, 2012.

[27] Sina Lashgari and Amir Salman Avestimehr. Timely throughput of heterogeneous wireless networks: Fundamental limits and algorithms. *CoRR*, abs/1201.5173, 2012.

[28] Ping Yu, Xiaoxing Ma, Jiannong Cao, and Jian Lu. Application mobility in pervasive computing: A survey. *Pervasive and Mobile Computing*, 9(1):2–17, 2013.

[29] Sam Malek, George Edwards, Yuriy Brun, Hossein Tajalli, Joshua Garcia, Ivo Krka, Nenad Medvidovic, Marija Mikic-Rakic, and Gaurav S. Sukhatme. An architecture-driven software mobility framework. *Journal of Systems and Software*, 83(6):972–989, 2010.

[30] Jiannong Cao, Weigang Wu, and Xuan Liu. Seamless mobility support for adaptive applications in heterogeneous wireless networks. In *Ubiquitous Intelligence Computing and 7th International Conference on Autonomic Trusted Computing (UIC/ATC), 2010 7th International Conference on*, 2010.

[31] K.S. Munasinghe and A. Jamalipour. Group mobility management for vehicular area networks roaming between heterogeneous networks. In *Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd*, 2010.

[32] Bruno Miguel Sousa, Kostas Pentikousis, and Marilia Curado. Multihoming management for future networks. *Mobile Networks and Applications*, 16(4):505–517, 2011.

[33] Ping Zhang, A. Durresi, and L. Barolli. Policy based mobility support in heterogeneous networks. In *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, 2010.

[34] P. Dini, J. Nin Guerrero, J. Mangues Bafalluy, L.L. Dai, and S. Addepalli. Interworking scheme using optimized sip mobility for multihomed mobile nodes in wireless heterogeneous networks. In *Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st*, 2010.

[35] Shin Hun Kang and Jae Hyun Kim. Qos-aware path selection for multi-homed mobile terminals in heterogeneous wireless networks. In *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*, 2010.

[36] Yannan Yuan, Yuliang Tang, and Congren Lin. A novel mobility prediction mechanism in heterogeneous networks. In *Communications and Mobile Computing (CMC), 2010 International Conference on*, volume 3, 2010.

[37] T. Sivakami and S. Shanmugavel. An overview of mobility management and integration methods for heterogeneous networks. In *Advanced Computing (ICoAC), 2011 Third International Conference on*, 2011.

[38] Wei Ren, Qing Zhao, and A. Swami. Connectivity of heterogeneous wireless networks. *IEEE Transactions on Information Theory*, 57(7):4315–4332, 2011.

[39] A. Sen, S. Murthy, and S. Banerjee. Region-based connectivity - a new paradigm for design of fault-tolerant networks. In *High Performance Switching and Routing, 2009. HPSR 2009. International Conference on*, 2009.

[40] A. Sgora and D.D. Vergados. Handoff prioritization and decision schemes in wireless cellular networks: a survey. *IEEE Communications Surveys Tutorial*, 11(4):57–77, 2009.

[41] S. Fernandes and A. Karmouch. Vertical mobility management architectures in wireless networks: A comprehensive survey and future directions. *IEEE Communications Surveys Tutorials*, 14(1):45–63, 2012.

[42] N. Nasser, A. Hasswa, and H. Hassanein. Handoffs in fourth generation heterogeneous networks. *IEEE Communications Magazine*, 44(10):96–193, 2006.

[43] Johann Márquez Barja, Carlos T. Calafate, Juan Carlos Cano, and Pietro Manzoni. An overview of vertical handover techniques: Algorithms, protocols and tools. *Computer Communications*, 34(8):985–997, 2011.

[44] Xiaohuan Yan, Y. Ahmet Sekercioglu, and Sathya Narayanan. A survey of vertical handover decision algorithms in fourth generation heterogeneous wireless networks. *Computer Networks*, 54(11):1848–1863, 2010.

[45] F. Hashim, K.S. Munasinghe, and A Jamalipour. On the negative selection and the danger theory inspired security for heterogeneous networks. *IEEE Wireless Communications*, 19(3):74–84, 2012.

[46] F. Hashim, K.S. Munasinghe, and A. Jamalipour. Biologically inspired anomaly detection and security control frameworks for complex heterogeneous networks. *IEEE Transactions on Network and Service Management*, 7(4):268–281, 2010.

[47] J. Schonwalder, M. Fouquet, G.D. Rodosek, and I. Hochstatter. Future internet = content + services + management. *IEEE Communications Magazine*, 47(7):27–33, 2009.

[48] Shih Jung Wu. A new integrated mobile architecture for heterogeneous wireless networks. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on*, 2010.

[49] Shih Jung Wu and Che Yu Yang. Hip - based handover mechanism under mih architecture in heterogeneous wireless networks. In *Networked Computing and Advanced Information Management (NCM), 2011 7th International Conference on*, 2011.

[50] D.E. Charilas and A.D. Panagopoulous. Multiaccess radio network enviroments. *IEEE Vehicular Technology Magazine*, 5(4):40–49, 2010.

[51] K. Taniuchi, Y. Ohba, V. Fajardo, S. Das, M. Tauil, Y.H. Cheng, A. Dutta, D. Baker, M. Yajnik, and D. Famolari. Ieee 802.21: Media independent handover: Features, applicability, and realization. *IEEE Communications Magazine*, 47(1):112–120, 2009.

[52] G. Lampropoulos, A.K. Salkintzis, and N. Passas. Media-independent handover

for seamless service provision in heterogeneous networks. *IEEE Communications Magazine*, 46(1):64–71, 2008.

[53] IEEE. Ieee 802.21. `http://www.ieee802.org/21/`, Útimo Acesso: Maio 2013.

[54] 3GPP. Architecture enhancements for non-3gpp accesses. `http://www.3gpp.org/ftp/Specs/html-info/23402.htm`, Útimo Acesso: Maio 2013.

[55] 3GPP. Access network discovery and selection function (andsf) management object (mo). `http://www.3gpp.org/ftp/Specs/html-info/24312.htm`, Útimo Acesso: Maio 2013.

[56] IEEE. Ieee 1900.4 working group on architectural building blocks enabling network-device distributed decision making for optimized radio resource usage in heterogeneous wireless access networks. `http://grouper.ieee.org/groups/dyspan/4/index.htm`, Útimo Acesso: Junho 2013.

[57] E. Gustafsson and A. Jonsson. Always best connected. *IEEE Wireless Communications*, 10(1):49–55, 2003.

[58] Ramona Trestian, Olga Ormond, and Gabriel-Miro Muntean. Game theory-based network selection: Solutions and challenges. *IEEE Communications Surveys Tutorials*, 14(4):1212–1231, 2012.

[59] Meriem Kassar, Brigitte Kervella, and Guy Pujolle. An overview of vertical handover decision strategies in heterogeneous wireless networks. *Computer Communications*, 31(10):2607–2620, 2008.

[60] K. Radhika and A.V.G. Reddy. Network selection in heterogeneous wireless networks based on fuzzy multiple criteria decision making. In *3rd International Conference on Electronics Computer Technology (ICECT), 2011.*, volume 6, pages 136–139, 2011.

[61] B. Bakmaz, Z. BojkoviC, and M. Bakmaz. Traffic parameters influences on network

selection in heterogeneous wireless environment. In *19th International Conference on Systems, Signals and Image Processing (IWSSIP), 2012*, pages 292–295, 2012.

[62] F. Moety, M. Ibrahim, S. Lahoud, and K. Khawam. Distributed heuristic algorithms for rat selection in wireless heterogeneous networks. In *IEEE Wireless Communications and Networking Conference (WCNC), 2012*, pages 2220–2224, 2012.

[63] Ying Wang and Ke Zhang. Decision tree based unsupervised learning to network selection in heterogeneous wireless networks. In *IEEE Consumer Communications and Networking Conference (CCNC), 2011*, pages 1108–1109, 2011.

[64] Joon-Myung Kang, Hong-Taek Ju, and James Won-Ki Hong. *Autonomic Management of Mobile Multimedia Services*, chapter Towards Autonomic Handover Decision Management in 4G Networks, pages 145–157. Springer Berlin Heidelberg, 2006.

[65] Joon-Myung Kang. *Autonomic Management for Personalized Handover Decisions in Heterogeneous Wireless Networks.* PhD thesis, Pohang University of Science and Technology, 2011.

[66] SuKyoung Lee, K. Sriram, Kyungsoo Kim, Yoon Hyuk Kim, and N. Golmie. Vertical handoff decision algorithms for providing optimized performance in heterogeneous wireless networks. *IEEE Transactions on Vehicular Technology*, 58(2):865–881, 2009.

[67] Wenhui Zhang. Handover decision using fuzzy madm in heterogeneous networks. In *IEEE WCNC-Wireless Communications and Networking Conference, 2004.*, 2004.

[68] Hani Alquhayz, Ali Al Bayatti, and Amelia Platt. Security management system for 4g heterogeneous networks. In *Proceedings of the World Congress on Engineering 2012*, 2012.

[69] G. Mapp, M. Aiash, A. Lasebae, and Raphael Phan. Security models for heterogeneous networking. In *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on*, 2010.

[70] Jiannong Cao, Chisheng Zhang, Jun Zhang, Yueming Deng, Xin Xiao, Miao Xiong, Jie Zhou, Yang Zou, Gang Yao, Wei Feng, Liang Yang, and Yao Yu. Shawk: Platform for secure integration of heterogeneous advanced wireless networks. In *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, 2012.

[71] Shaman. `http://www.ist-world.org/ProjectDetails.aspx?ProjectId=505370da4fd74e4c8a1ffd674da657f1`, Útimo Acesso: Junho 2013.

[72] Hyeyeon Kwon, Kyung Yul Cheon, and Aesoon Park. Analysis of wlan to umts handover. In *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, 2007.

[73] Nist. `http://www.nist.gov/itl/antd/emntg/ssm_seamlessandsecure.cfm`, Útimo Acesso: Julho 2013.

[74] Seqomo. `http://www.tkn.tu-berlin.de/research/SeQoMo/`, Útimo Acesso: Julho 2013.

[75] Secricom. `http://www.secricom.eu/eu-projects`, Útimo Acesso: Julho 2013.

[76] Odtone - open dot twenty one - an open-source multiple-plaftorm ieee 802.21 mihf implementation. `http://hng.av.it.pt/projects/odtone`, Útimo Acesso: Julho 2013.

[77] H. Redwan and Ki-Hyung Kim. Survey of security requirements, attacks and network integration in wireless mesh networks. In *NTMS '08 New Technologies, Mobility and Security, 2008.*, pages 1–15, 2008.

[78] Jacob Holm, Kristian de Lichtenberg, and Mikkel Thorup. Poly-logarithmic deterministic fully-dynamic algorithms for connectivity, minimum spanning tree, 2-edge, and biconnectivity. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, 1998.

[79] Jaime Cohen, Luiz A. Rodrigues, and Elias Procópio Duarte, Jr. A parallel implementation of gomory-hu's cut tree algorithm. *Symposium on Computer Architecture and High Performance Computing*, 0:124–131, 2012.

[80] Ariel Tseitlin. The antifragile organization. *Communications of the ACM*, 56(8):40–44, 2013.

[81] Markus J. and D. M'Raïhi. Mix-based electronic payments. In *Proceedings of the Selected Areas in Cryptography*, pages 157–173, 1998.

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

[83] Chih-Wei Hsu, Jian-Pan Li, and Sheng-Tzong Cheng. Connection manager using fahp of mcdm techniques in heterogeneous network. In *IEEE 11th International Conference on Hybrid Intelligent Systems (HIS)*, pages 10–15, 2011.

[84] Huazhong Zhang, Peipei Chen, and Shulan Gong. Weighted spanning tree clustering routing algorithm based on leach. In *IEEE 2nd International Conference on Future Computer and Communication (ICFCC)*, volume 2, pages 223–227, 2011.

[85] M.Q. Khan and S.H. Andresen. A semi and fully distributed handover algorithm for heterogeneous networks using miis. In *IEEE Symposium on Computers and Communications (ISCC)*, pages 145–150, 2012.

[86] M. B. Shah, P. S. Tamhankar, S.N. Merchant, and U.B. Desai. A realistic weighted clustering algorithm for data gathering in single hop cell phone based sensor network. In *IEEE GLOBECOM (GC Wkshps)*, pages 1253–1257, 2011.

[87] R. E. Gomory and T. C. Hu. Multi-terminal network flows. *Journal of the Society for Industrial and Applied Mathematics*, 9(4):551–570, 1961.

[88] Meshnet. Mesh testbed is an experimental wireless mesh network. `http://moment.cs.ucsb.edu/meshnet/`, Último acesso: Julho 2013.

[89] Lemon. Library for efficient modeling and optimization in networks. `http://lemon.cs.elte.hu/trac/lemon`, Último acesso: Julho 2013.

[90] Christophe Crespelle and Fabien Tarissan. Evaluation of a new method for measuring the internet degree distribution: Simulation results. *Computer Communications*, 34(5):635–648, 2011.

[91] Martin L. Puterman. *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. Wiley-Interscience, 1994.

[92] Jerônimo Pellegrini and Jacques Wainer. Processos de decisão de markov: um tutorial. *Revista de Informática Teórica e Alicada (RITA)*, pages 133–179, 2007.

[93] B. Malakooti and I Thomas. A distributed composite multiple criteria routing using distance vector. In *IEEE International Conference on Networking, Sensing and Control (ICNSC '06)*, 2006.

[94] THOMAS L. SAATY. *The analytic hierarchy process*. McGraw Hill, 1980.

[95] Behnam Vahdani, AmirHajiKarim Jabbari, Vahid Roshanaei, and Mostafa Zandieh. Extension of the electre method for decision-making problems with interval weights and data. *The International Journal of Advanced Manufacturing Technology*, 2010.

[96] Xiaoting Wang and Evangelos Triantaphyllou. Ranking irregularities when evaluating alternatives by using some electre. *Omega*, pages 45–63, 2008.

[97] Hugo Marques, José Ribeiro, Paulo Marques, and Jonathan Rodriguez. Simulation of 802.21 handovers using ns-2. *Journal of Computer Systems, Networks, and Communications - Special issue on lightweight mobile and wireless systems: technologies, architectures, and services*, 2010.

[98] NIST. The network simulator ns-2. nist add-on. ieee 802.21 model. Technical report, National Institute of Standards and Technology (NIST), 2006.

[99] Salumu Munga. Mih infrastructure support to ns-3. `http://code.nsnam.org/salumu/ns-3-mih/`, Último acesso: Junho 2014.

[100] G. Bouabene, C. Jelger, C. Tschudin, S. Schmid, A Keller, and M. May. The autonomic network architecture (ana). *IEEE Journal on Selected Areas in Communications*, 28(1):4–14, 2010.

[101] Georgios Aristomenopoulos, Timotheos Kastrinogiannis, Zhaojun Li, and Symeon Papavassiliou. An autonomic qos-centric architecture for integrated heterogeneous wireless networks. *Mobile Networks and Applications*, 16(4):490–504, 2011.

[102] Ralph Droms. Rfc2131: Dynamic host configuration protocol. Network Working Group, 1997.

[103] Zeina Jrad, Francine Krief, Lahcene Dehni, and Younes Bennani. Artificial intelligence techniques in the dynamic negotiation of qos: A user interface for the internet new generation. In *Proceedings of the First IFIP TC6 International Conference on Autonomic Networking*, pages 146–158, 2006.

[104] Jon Postel. Rfc791: Internet protocol. Defense Advanced Research Projects Agency Information Processing Techniques Office, 1981.

[105] Ming-Ming Xiao, Shun zheng Yu, and Yu Wang. Automatic network protocol automaton extraction. In *Third International Conference on Network and System Security (NSS 09)*, pages 336–343, 2009.

ROBSON GOMES DE MELO

GERENCIAMENTO DE CONECTIVIDADE SEGURA E CONTÍNUA EM REDES DE ACESSO HETEROGÊNEAS

Tese apresentada como requisito parcial à obtenção do grau de Doutor. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.

Orientador: Prof. Dr. Aldri Luiz dos Santos
Coorientadora: Profa. Dr. Michele Nogueira

CURITIBA

2014