Gerenciamento de handovers em next generation networks com agregação de contexto

Roberto Sadao Yokoyama

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura:

Gerenciamento de handovers em next generation networks com agregação de contexto

Roberto Sadao Yokoyama

Orientador: ***Prof. Dr. Edson dos Santos Moreira***

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências - Ciências de Computação e Matemática Computacional.

USP – São Carlos
Junho/2009

Dedico este trabalho a meus pais,

Joaquim e Helena.

Agradecimentos

Aos meus pais, minha irmã e a toda a minha família pelo incentivo e auxílio nos estudos para a conquista deste trabalho.

À minha querida companheira Rafaela, pelo seu amor, apoio e paciência que teve comigo.

Ao meu orientador, Edson Moreira, pela amizade, confiança, ideias e atenção em todos os momentos do mestrado.

Aos professores do ICMC-USP que ajudaram no desenvolvimento deste trabalho e pelos ensinamentos.

A todos os amigos que me apoiaram durante o trabalho, em particular ao Roberto Rigolin e Bruno Kimura pelas sugestões, ajuda nos esclarecimentos e soluções dos diversos problemas do projeto.

Aos funcionários do ICMC-USP.

À FAPESP pelo apoio financeiro.

Por fim, a todas as pessoas que, direta ou indiretamente, contribuíram na realização do trabalho.

A todos os meus sinceros agradecimentos. Obrigado!

Resumo

Em NGN (*Next Generation Networks*), os usuários podem se conectar em diferentes tecnologias de rede e desejam, além de uma comunicação transparente, novos serviços personalizados. Neste sentido, este trabalho explora informações de contexto em NGN. O principal objetivo é capturar as informações de contexto envolvidas no momento da utilização da rede sem fio, na escolha do novo ponto de acesso e no procedimento do *handover*. Este contexto capturado é aplicado para serviços cientes de contexto. A proposta é validada por meio de dois cenários, o primeiro é um *mashup* que exibe as redes sem fio disponíveis de um determinado local e o segundo um protótipo gerenciador de conexões para atender as preferências do usuário. Adicionalmente, são realizadas duas avaliações do impacto do uso de contexto em *handovers.* Para tanto, foi implantado um *testbed* NGN com o protocolo *Mobile IP*.

Palavras chaves: NGN, 4G, *handover*, serviços cientes de contexto e *handovers* cientes de contexto.

Abstract

In the NGN (Next Generation Networks) users can connect their Internet devices to different network technologies. In addition to a seamless communication, users desire new and personalized services. In this sense, this thesis exploits the context-aware information in NGN environments. The main propose is to capture the context information about the time involved by the use of wireless link for selecting the target access point and on the *handover* procedure. This context information is applied to the context-aware services. The propose is validated through two scenarios: the first is a mashup that shows the availability of wireless networks in a particular location, and the second is a prototype of a connection manager to attend user´s preferences. In addition, two evaluations are accomplished on the impact by the use of context information over *handovers*. Thus, an NGN *testbed* is deployed with Mobile IP protocol.

Keywords: NGN, 4G, *handover*, context-aware services and context-aware *handovers*.

Lista de Ilustrações

Figura 1 - Rota de Conectividade (imagem adaptada a partir do Google maps1)..... 3
Figura 2 - Sinais de redes Wi-Fi coletados por um sensor de espectro (Carvalio Jr. et al., 2009)..... 3
Figura 3 - Evolução das redes e dos protocolos (adaptado de Vidales, et al., 2007) 5
Figura 4 - Exemplo do ambiente NGN..... 10
Figura 5 - Funcionamento do Mobile IP (Adaptado de Heissenhuber et al., 2002): (A) Roteamento normal de pacotes entre o NM e o CN; (B) O NM registra-se com seu HA; (C) Roteamento triangular e (D) Otimização de rota..... 13
Figura 6 - Media independent *handover* framework..... 16
Figura 7 - Canais sem sobreposição em APs 802.11b/g (Carvalio Jr, 2009) 26
Figura 8 - Estrutura endereço Global Unicast (adaptado de Davies, 2008) 28
Figura 9 - *Testbed* Mobile IP versão 6 30
Figura 10 - Gráfico de dispersão da vazão e latência do *handover*. 31
Figura 11 - Arquitetura SOHand - lado cliente, *Broker* e lado provedor. 34
Figura 12 - Wireless Footprinting 38
Figura 13 - Fluxograma do gerenciador de conexões..... 41

Lista de Tabelas

Tabela 1 - Classificação dos *handovers* 11
Tabela 2 - Descrição das variáveis do algoritmo..... 22
Tabela 3 - Tecnologias de rede sem fio..... 25
Tabela 4 - Configuração dos nós do *testbed*..... 29
Tabela 5 - Fontes de contexto e exemplos de informações que podem ser captadas. 35
Tabela 6 - Descrição das variáveis e estruturas do algoritmo 39
Tabela 7 - Relação entre pesos e a preferência..... 40
Tabela 8 - Redes encontradas em determinado momento. 42
Tabela 9 - Pesos atribuídos aos parâmetros de cada rede. 42
Tabela 10 - Número do teste e tipo de configuração..... 44
Tabela 11 - Valores configurados na plataforma..... 44
Tabela 12 - Configurações dos APs no cenário..... 45
Tabela 13 - Configuração dos AP´s para cada teste 45
Tabela 14 - Resultados de cada Teste..... 46

Lista de Abreviaturas e Siglas

1G -Primeira Geração
2G -Segunda Geração
3G -Terceira Geração
4G -Quarta Geração
AAA -Authentication, Authorization e Accounting
ACK -Acknowledgment
AHP -Analytic Hierarchy Process
AMPS -Advanced Mobile Phone System
API -Application Programming Interface
AR -Access Router
ARP -Address Resolution Protocol
BA -Binding Acknowledgement
BDL -Base de Dados Local
BDC -Base de Dados Centralizada
BER -Bit Error Rate
BU -Binding Updates
CN -Correspondent Node
CoA -Care-of Address
CoT -Care-of Test
CoTI -Care-of Teste Initiate
CN -Correspondent Node
CSMA/CA -Carrier Sense Multiple Access/Collision Avoidance
CTS -Clear-To-Send
DHCP -Dynamic *Host* Configuration Protocol
DSSS -Direct Fequence Spread Spectrum
DCF -Distributed Coordination Function
EDCF -Enhanced Distributed Coordination Function
FC -Fontes de Contexto
FHSS -Frequency Hopping Spread Spectrum
FN -Foreign Network
GC -Gerenciador de Contexto
GH -Gerenciador de *Handover*
GN -Gerenciador de Negociação
GPRS -General packet radio service
GPS -Global Positioning System
GSM -Global System for Mobile Communcations
HA -Home Agent
HIP -*Host* Identity Protocol
HN -Home Network
HoT -Home Test
HoTI -Home Test Initiate
HR-DSSS -High Rate DSSS
IEEE -Institute of Electrical and Electronics Engineers
IP -Internet Protocol
ITU-T- International Telecommunication Union -Telecommunication

MAC -Media Access Control
MICS -Media Independent Command Service
MIES -Media Independent EventService
MIHF -Media Independent *Handover* Function
MIIS -Media Independent Information Service
MIMO -Multiple Input Multiple Output
MIPL -Mobile IP for Linux
MN -Mobile Node
MN -Módulo de Negociação
MPA -Media-independent Pre-Authentication
MSCTP -Mobile Stream Control Transmitioin Protocol
NA - Neighbour Advertisement
NGN - Next Generation Networks
NS -Neighbour Solicitation
OFDM -Ortogonais Frequency Division Multiplexing
PCF -Point Coordination Function
PDA´s -Personal Digital Assistants
PR -Pesos Relativos
QoS -Quality of Service
RA -Router Advertisement
RA -Roteadores de Acesso
RR -Return Routability
RS -Router Solution
RSSI -Received Signal Strength Indication
RTS -Ready-To-Send
SCTP - Stream Control Transmission Protocol
SIP -Session Initiation Protocol
SMS -Sort Message Service
SO -Sistema Operacional
SOHand - Service Oriented *Handover*
TCP -Transmission Control Protocol
TIPS -Transparent IP Sockets
TM -Terminais Móveis
UMTS -Universal Mobile Telecommunications System
VoIP - Voice over Internet Protocol
WPAN -Wireless Personal Area Network
WLAN -Wireless Local Area Network
WMANs -Wireless Metropolitan Area Networks
WWANs -Wireless Wide Area Networks
Wi-Fi - Wireless Fidelity
WiMAX - Worldwide Interoperability for Microwave Access
WEP -Wired Equivalent Privacy
WPA -Wi-Fi Protected Access

Sumário:

Agradecimentos ii
Resumo iii
Abstract iv
Lista de Ilustrações v
Lista de Tabelas vi
Lista de Abreviaturas e Siglas vii
1. Introdução 1
1.1. Motivação 2
1.2. Objetivo 4
1.3. Evolução das redes sem fio e convergência das tecnologias 4
1.4. Contexto em NGN 5
1.5. Ontologia para auxiliar serviços 6
1.6. Organização do trabalho 6
2. Gerenciamento de Mobilidade 8
2.1. Considerações Iniciais 8
2.2. Terminologias 8
2.3. Next Generation Networks 9
2.4. Classificação do handover 11
2.5. Protocolos de Gerenciamento de Mobilidade 12
2.6. Mobile IP versão 6 12
2.7. IEEE 802.21 - Protocolo para Gerenciamento de Handover 15
2.8. Considerações Finais 17
3. Handover Ciente de Contexto 18
3.1. Considerações iniciais 18
3.2. Classificação de Contexto 18
3.3. Trabalhos Relacionados 19
3.4. Algoritmo AHP 21
3.5. Considerações finais 22
4. Testbed NGN 24
4.1. Considerações iniciais 24
4.2. Classificação das tecnologias de rede sem fio 24
4.3. IEEE 802.11 24
4.3.1. Camada física 25
4.3.2. Camada de enlace de dados 26
4.3.3. Qualidade de Serviço, Segurança e Gerenciamento 27
4.4. Protocolo IPv6 27
4.5. Testbed 29
4.6. Avaliação de Desempenho do MIPv6 30
4.7. Considerações finais 31
5. Serviços com Contexto em NGN 32
5.1. Considerações Iniciais 32
5.2. Uma breve descrição da arquitetura SOHand 32

5.2.1 Componentes da Arquitetura SOHand 33
5.2.2 As Fontes de Contexto e Gerenciador de Contexto 34
5.2.3. Procedimento de conexão 36
5.3. Validação dos conceitos por meio de *Mashup* e *Handovers* por Preferência. 36
5.3.1. Cenário do *Mashup* com o Google Maps 37
5.3.2. Cenário das preferências do usuário 38
5.4. Formalização das informações contextuais. 47
5.5. Considerações finais 48
6. Avaliação de *Handovers* com Contexto 49
6.1. Considerações iniciais 49
6.2. Impacto da captura de contexto 49
6.3. Análise do Custo/Benefício do *handover* 51
6.4. Considerações finais 53
7. Conclusões 54
7.1. Principais resultados e contribuições 55
7.2. Trabalhos Futuros 56
Referências 57

1. Introdução

O aumento da oferta de acesso a Internet pelas redes de telefonia móvel, a popularização das redes sem fio locais e a expectativa das tecnologias sem fio para acesso metropolitano fazem com que o cenário de provimento reúna tecnologias de rede sem fio heterogêneas.

Seguindo a tendência dessa oferta de diversas tecnologias de acesso, alguns dispositivos móveis (Celulares, *SmartPhones*, etc), vêm incorporando mais de uma interface à rede, como por exemplo Wi-Fi (IEEE 802.11) e Bluetooth (IEEE 802.15.1). Além disso, as capacidades de armazenamento e processamento vêm aumentando nos últimos anos, possibilitando a integração de câmeras digitais e GPS (*Global Positioning System*).

Por essas razões, da combinação do aumento da oferta das redes e o crescimento do segmento de dispositivos móveis, surge o cenário em que o usuário pode acessar sob demanda a rede de sua opção. Assim, no aspecto de serviços, o modelo de negócios passa a ser **centrado no usuário** (Frattasi et al., 2006; Quoc-Thinh, et al., 2008). Um dos desafios que se apresenta é explorar as informações relacionadas à escolha da próxima rede e, desta forma, auxiliar na transição ou explorar novas oportunidades de negócios.

Considerando ainda a perspectiva do modelo centrado no usuário, esse pode trocar de rede pelos seguintes motivos (Moreira et al., 2007): pode ser **imperativo** (quando o usuário se afasta do ponto de acesso e a única opção é realizar a transição da rede para manter a conexão); pela **conveniência** (quando o usuário entrar em um aeroporto e quiser usar os serviços fornecidos por sua rede interna: mapas, horários de vôos, etc.); por **incentivos** (quando é oferecido ao usuário algum tipo de benefício para conectar a uma rede específica) e pela **preferência** (quando um usuário decide trocar para um determinado ponto de acesso com base em uma boa experiência anterior: preço, segurança, etc.).

Neste sentido, conhecer o contexto envolvido no uso da rede, no motivo que leva à troca, à seleção de outra rede, etc., pode ser de interesse para outras entidades (provedores de acesso, provedores de serviços, etc.) para aperfeiçoarem serviços e o relacionamento com o usuário. Portanto, a principal proposta deste trabalho é capturar as informações de contexto do **usuário**, do **ambiente**, do **dispositivo móvel**, da **rede** e das **aplicações**, essencialmente as

envolvidas no uso da rede e no procedimento da escolha do ponto de acesso, com a finalidade de serem utilizadas por outras entidades.

1.1. Motivação

Diversas entidades podem ter interesse nas informações envolvidas na utilização, na escolha e no procedimento de troca do ponto acesso a rede. O acesso pode ser melhorado em algumas áreas correlacionando dados da rede (e.g. qualidade do sinal) e o posicionamento geográfico do usuário, os serviços podem ser personalizados para dispositivos ou localização do usuário, administradores de rede podem capturar informações da rede sem fio para mitigar interferências de rádio, ataques, intrusões etc. Para ilustrar as possibilidades de explorar as informações contextuais envolvidas em ambientes com diversas redes sem fio disponíveis são descritos dois cenários, o primeiro aborda um serviço de acesso à rede e o segundo o gerenciamento do espectro em redes sem fio.

Cenário 1 - Rota de Conectividade. Um serviço centralizado para disponibilizar informações de contexto, por exemplo, um *Broker*, rotas de conectividade entre diferentes redes poderiam ser traçadas sem o contato, a priori, com provedores dessas redes. Essas rotas seriam baseadas nas preferências do usuário e na experiência de outros clientes que passaram pela mesma região utilizando as redes e cujos *feedbacks* são armazenados no *Broker*. O cliente, então, poderia consultar um percurso até o seu destino que passasse por redes de provedores que oferecessem segurança, boa conectividade, melhor QoS ou preço. A Figura 1 é um exemplo do possível serviço, que disponibiliza a rota em um mapa, baseada na preferência do usuário. Nesse exemplo, o usuário deseja ir do Ponto A ao B com conectividade em redes seguras.

Cenário 2 - Gerenciamento do espectro em redes sem fio.

O aumento do uso de redes Wi-Fi em residências, empresas, universidades e condomínios, torna necessário que o administrador de redes gerencie a camada física da comunicação sem fio, ou seja, o espectro de rádio frequência e as interferências em seu meio. Esse último é agravado devido à ocupação do espectro ser limitada às normas de agências reguladoras. Assim, a faixa de espectro não regulado, em alguns casos, pode ficar saturada, por exemplo, a frequência de 2,4GHz.

No futuro, diferentes tecnologias de rede sem fio emergentes, como o Wi-MAX (IEEE 802.16), tendem a piorar o problema da interferência e, consequentemente, afetar a disponibilidade dos serviços. Logo, em uma primeira instância é necessário o gerenciamento

dinâmico do espectro de radio frequência, principalmente em locais com grande concentração de redes sem fio e também em locais com muitos usuários buscando acesso. Para tanto, poderia ser criada uma plataforma para captura de informações do espectro de Wi-Fi e a análise das informações poderia levar a identificação das fontes de interferência. Essa análise poderia ser realizada com o auxílio de gráficos com as redes disponíveis, a qualidade do sinal e canais de utilização em função do tempo, como ilustrado na Figura 2 (Carvalio Jr. et al., 2009).

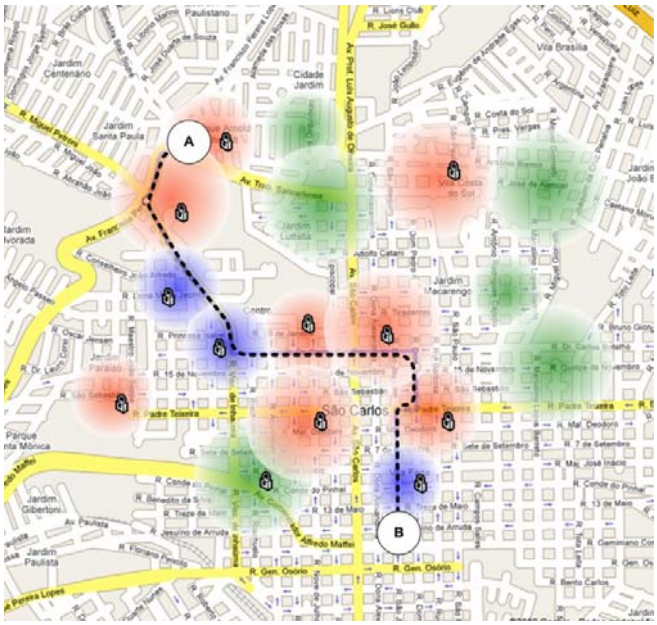

Figura 1 - Rota de Conectividade (imagem adaptada a partir do Google Maps)

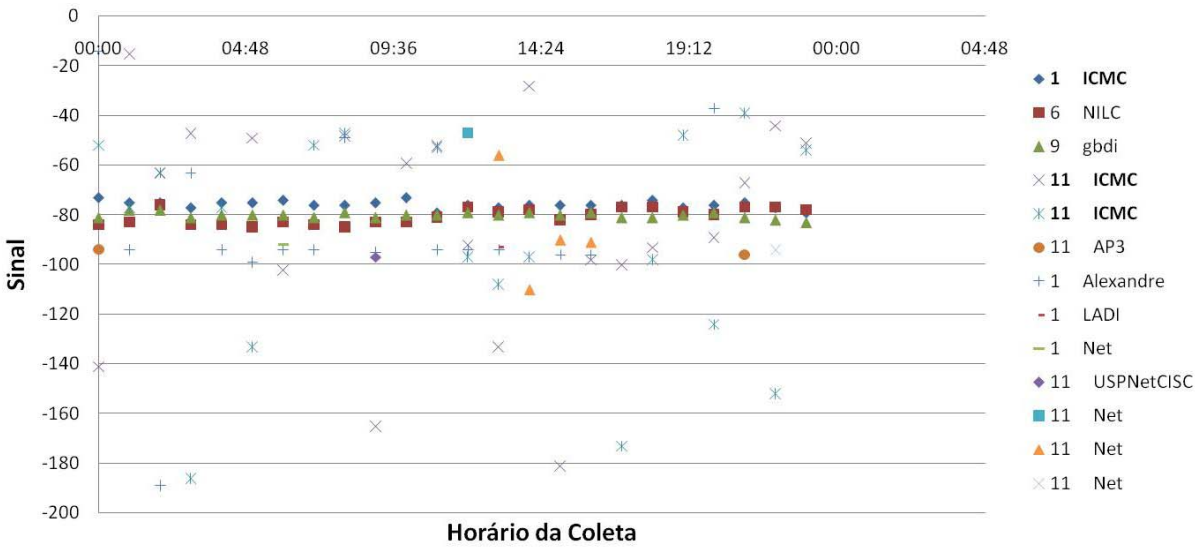

Figura 2 - Sinais de redes Wi-Fi coletados por um sensor de espectro (Carvalio Jr. et al., 2009)

1.2. Objetivo

O objetivo principal deste trabalho é explorar informações de contexto envolvidas na utilização da rede sem fio, na escolha de um novo ponto de acesso e informação do procedimento de transição entre as redes. Para isso, foi implementada uma plataforma básica de aquisição de informações de contexto e como prova da viabilidade da proposta foram utilizados dois cenários, o primeiro um serviço que exibe as redes sem fio disponíveis de um determinado local e o segundo um protótipo de gerenciador de conexões para atender as preferências do usuário. Para avaliação da plataforma foi implantando um *testbed* com Mobile IP. Adicionalmente, as informações contextuais foram padronizadas por meio de uma ontologia com vistas ao compartilhamento.

1.3. Evolução das redes sem fio e convergência das tecnologias

A telefonia celular passou por três gerações distintas. A primeira geração (1G) foi analógica e realizava somente comunicação de voz, sendo que o padrão mais comum foi o AMPS (*Advanced Mobile Phone System*). A segunda geração (2G) foi digital, com destaque para o padrão GSM (*Global System for Mobile Communcations*), que oferecia um serviço com qualidade de voz comparável à linha fixa e possibilitava perambulação (*roaming*) entre as operadoras. Adicionalmente, era suplementada com serviços de redirecionamento de ligações, secretária eletrônica e *Short Message Service* (SMS). Estas foram as razões do sucesso dos celulares 2G (Frattasi, et al., 2006).

A terceira geração (3G) já foi lançada em diversos países; e a ideia básica é oferecer altas taxas de transmissão, da ordem de 2Mbps, para serviços de Internet e multimídia (vídeo e voz simultâneos). O padrão desenvolvido foi o sistema UMTS (*Universal Mobile Telecommunications System*), porém, na prática, o aumento previsto de vazão não foi alcançado em virtude da dificuldade de gerenciar a mobilidade do usuário com rapidez suficiente, chegando a 2Mbps somente para usuários estacionários em recintos, 384 Kbps para pessoas andando a pé, e 144Kbps para conexões em automóveis (Tanenbaum, 2003).

A quarta geração (**4G**) ou **NGN** (ITU-T, 2009) é pautada pelo modelo de negócios centrado no usuário. Portanto, esta nova geração deverá oferecer: essencialmente alta qualidade de voz, vídeo com alta definição, elevada taxa de transmissão, a conexão mais apropriada entre as redes disponíveis, uma interface personalizada e amigável para o usuário levando em consideração a diversidade dos dispositivos móveis (tamanho da tela, memória,

autonomia de bateria, etc); serviços personalizados (perfis, preferências e informações de contexto) e uma arquitetura aberta que favoreça os interessados (operadoras, provedores de serviços, clientes etc.) e tenha como base o protocolo IP (Berndt, 2008).

Na Figura 3 é ilustrada a evolução das redes de computadores em função do tempo aproximado e grau de complexidade no gerenciamento. Inicialmente, as redes de computadores eram caracterizadas principalmente por terem terminais e roteadores estacionários, infraestrutura composta por cabos e comunicação fim-a-fim utilizando o endereçamento IP (*Internet Protocol*) fixo. Com o advento das tecnologias de comunicação sem fio, a infraestrutura deixou de ser exclusivamente por cabos e os terminais integralmente fixos e, posteriormente, criou-se a nova versão do protocolo IP, a versão 6. Nos últimos anos, incorporou-se aos protocolos IP o suporte à mobilidade, como o *Mobile* IPv6 (Jonhson, 2004).

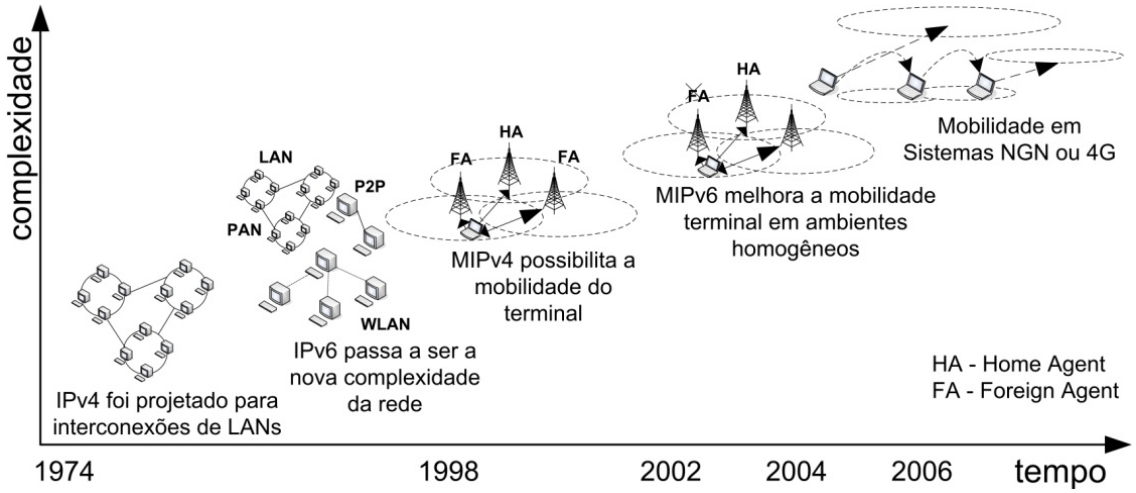

Figura 3: Evolução das redes e dos protocolos (adaptado de Vidales et al., 2007)

1.4. Contexto em NGN

O termo **contexto** é utilizado com vários significados em diferentes campos da computação. Uma das principais definições da literatura é realizada por Dey (Dey et al, 2001) e pode ser traduzido como: qualquer informação que pode ser usada para caracterizar a situação de uma entidade (e.g., pessoa, lugar ou objeto), que é considerada relevante para interação entre um usuário e uma aplicação, incluindo o usuário e a própria aplicação. Outras definições podem ser encontradas na literatura, por exemplo; Shilit (Shilit e Theimer, 1994), refere-se a contexto como localização, identifica pessoas próximas, objetos e mudanças desses objetos e Schmidt (Schmidt et al., 1999) refere-se a contexto como o conhecimento sobre o estado do usuário e seu dispositivo.

Contexto em NGN é, normalmente, utilizado para prover serviços cientes de contexto para o usuário. A ideia de serviço ciente de contexto faz parte da definição realizada por Dey (Dey et al, 2001) de Computação Ciente de Contexto, que pode ser entendida como: um sistema que utiliza contexto para prover informações relevantes e/ou serviços para o usuário, onde a relevância depende da tarefa do usuário. Assim, os trabalhos envolvendo contexto em NGN (Wei et al, 2006; Ahmed, 2006; Balasubramaniam e Indulska, 2004) fazem uso de informações contextuais da rede para prover QoS para o usuário, por exemplo, trocando o ponto de acesso atual por outro com melhor vazão, menor atraso e perda de pacotes.

1.5. Ontologia para auxiliar serviços

Ambientes NGN possibilitam a criação de novos serviços de telecomunicação por provedores de acesso e serviço, o que consequentemente, trazem o desafio de gerir o vasto conjunto de informações envolvidas no modelo de negócios. Pois, a cada troca de rede realizada pelo usuário, os provedores necessitam compartilhar informações, por exemplo, das preferências do usuário e de serviços personalizados. Todavia, a ausência de padronização e de um vocabulário comum dificulta o compartilhamento e comunicações entre os sistemas, uma vez que diversas variáveis podem mudar (e.g. segurança, QoS, preço, tecnologia da rede sem fio, etc.).

Nessas circunstâncias existe a demanda de uma ontologia para apoiar a tarefa de gerenciamento das informações (Vanni et al, 2006). Uma **ontologia** é a especificação explícita e formal de uma conceitualização compartilhada (Studer, 1998). Com isso, as informações teriam semântica e poderiam ser compartilhadas e exploradas por outras entidades como um dicionário detalhado e estruturado, cujo computador é capaz de processá-las.

1.6. Organização do trabalho

Esta dissertação está organizada da seguinte forma:

No capítulo 2, discorre-se sobre o estudo de Gerenciamento de Mobilidade. Inicialmente é realizada a definição das terminologias da área, depois são abordadas as NGN e os tipos de *handovers* envolvidos, uma visão dos protocolos de gerenciamento de mobilidade, uma descrição detalhada do Mobile IPv6, e no final, o protocolo de gerenciamento de *handovers* o IEEE 802.21.

O capítulo 3 aborda a Computação Ciente de Contexto em NGN. Discute-se sobre a classificação de informações contextuais, faz-se uma análise dos trabalhos relacionados e por fim, o detalhamento do algoritmo utilizado para seleção do ponto de acesso alvo.

No capítulo 4, é detalhado o *testbed* NGN. Descrevem-se as principais tecnologias envolvidas no projeto, a implantação e a configuração do *testbed* e, por último, apresenta-se uma avaliação de desempenho da rede.

No capítulo 5, são apresentados os Serviços com Contexto em NGN. Para tanto, é detalhada a especificação da arquitetura SOHand, são descritos os dois cenários usados para a validação do trabalho e os testes realizados dos serviços.

No capítulo 6, descreve-se uma Avaliação de *Handovers* com Contexto; foram avaliadas duas características, o impacto da captura de informações contextuais e o custo/benefício do *handover*.

No capítulo 7, finalmente, são apresentados as conclusões finais, as contribuições alcançadas e os possíveis trabalhos futuros.

2. Gerenciamento de Mobilidade

2.1. Considerações Iniciais

Neste Capítulo, inicialmente são abordadas as Terminologias relacionadas à Computação Móvel, cuja definição dos principais termos está de acordo com a ITU-T e a RFC 3753. Uma vez definidos os termos, é realizada uma discussão sobre NGN e os problemas envolvidos no evento *handover*, sendo esse classificado de várias formas.

Ainda no âmbito das NGN, existem algumas soluções propostas para o gerenciamento de mobilidade; e dentre as propostas é abordado em detalhes o protocolo MIPv6. Outro protocolo discutido é o IEEE 802.21, proposto para o gerenciamento de *handover*.

Na Seção 2.2 são definidos os termos de interesse para o trabalho; na Seção 2.3 é discorrido sobre as NGN; na Seção 2.4 são classificados e definidos os tipos de *handover*; na Seção 2.5 é apresentada uma visão geral dos protocolos de gerenciamento de mobilidade; na Seção 2.6 é descrito em detalhes o MIPv6; na Seção 2.7 discorre-se sobre o protocolo IEEE 802.21 e por fim, na Seção 2.8 são apresentadas as considerações finais.

2.2. Terminologias

Em uma visão ampla, a ITU-T(ITU-T, 2004) define **Mobilidade** como a capacidade de prestar serviços de rede independentes de mudanças que possam ocorrer na atividade do usuário. Assim, o usuário é capaz de trocar o seu ponto de acesso à rede, durante seu deslocamento geográfico, sem interromper o serviço atual ou sessão, ou seja, o que envolve *handovers*. Ainda, especifica que é **Mobilidade Terminal** quando o terminal acessa serviços em diferentes locais e em movimento, sendo identificado e localizado pelas redes, e **Mobilidade Pessoal** quando o usuário acessa os serviços de qualquer terminal utilizando um identificador pessoal.

Manner e Kojo (Manner e Kojo, 2004) classificam a mobilidade em **Macro-Mobilidade** e **Micro-Mobilidade**. Em linhas gerais, estão relacionadas a grandes áreas com diferentes domínios IP e pequenas áreas com mesmo domínio IP, respectivamente. Segundo Akyildiz (Akyildiz et al., 1999), o **Gerenciamento da Mobilidade** é aplicado à macro-mobilidade e divide-se em: **Gerenciamento do *Handover***, como um mecanismo que implementa a troca transparente e, adicionalmente, a escolha do próximo ponto de acesso; e

Gerenciamento de Localização, no sentido de atualizar o local (a rede) o qual o usuário se conectou após o *handover*, redirecionando o tráfego.

***Handover* ou handoff** é o processo no qual o nó móvel troca o ponto de conexão à rede ou quando ocorre uma tentativa (Manner e Kojo, 2004). Um **Nó Móvel** é um nó suscetível a transições de pontos de conexão à rede, podendo ou não realizar a funcionalidade de encaminhamento de pacotes, i.e., roteamento.

Finalizando os termos de interesse, tem-se os **Roteadores de Acesso**, que são roteadores de borda conectados a um ou mais pontos de acesso. Um Roteador de Acesso oferece conectividade para o Nó Móvel atuando como *gateway* da rede, sendo que a **Rede de Acesso** é uma rede composta por um ou mais Roteadores de Acesso. Com a finalidade de simplificar os termos, neste trabalho, adotou-se para a Mobilidade Terminal, puramente Mobilidade e Nó Móvel também é referenciado como Dispositivo Móvel.

2.3. *Next Generation Networks*

Na literatura, existe um conflito de nomenclaturas, no qual, normalmente, nos trabalhos relacionados à telefonia celular (Frattasi,et al ., 2006; Suk e Kai, 2003; Lee, et al., 2007; Vidales et al., 2005), são comuns as nomenclaturas de gerações (1G, 2G e 3G). Por outro lado, em trabalhos relacionados às redes de computadores, o cenário 4G é referido como NGN (Myoung, et. al., 2006; Han, et al., 2008; Moreira et al., 2007). Por isso, neste trabalho, entende-se que NGN e 4G tratam do mesmo paradigma. No entanto, esta pesquisa adota o termo de NGN porque possui uma definição da *International Telecommunication Union - Telecommunication* (ITU-T), realizada em uma de suas iniciativas globais de padronização a NGN-GSI (NGN-GSI, 2009).

A definição da ITU-T (ITU-T, 2009) para NGN pode ser traduzida como: uma rede de pacotes capaz de prover Serviços de Telecomunicações para os usuários e fazer uso de múltiplas tecnologias de banda larga, tecnologias de transporte com QoS, sendo que os serviços relacionados são independentes das tecnologias da infraestrutura. O usuário tem acesso irrestrito às redes e provedores de serviços concorrentes de acordo com a sua escolha e suporte à mobilidade generalizada, que permitirá prestação de serviços coerentes e ubíquos para os usuários.

As NGNs, segundo Suk (Suk e Kai, 2003), concentram seus desafios principalmente nos aspecto da **mobilidade do usuário**, **no sistema** e **nos serviços**. O problema da

mobilidade está na interoperabilidade dos dispositivos móveis com as redes e em controlar o acesso heterogêneas, e adicionalmente, em limitações dos recursos computacionais, consumo de energia e compatibilidade com sistemas legados. Ainda, as NGNs devem ser capazes de descobrir as redes disponíveis com tecnologias e protocolos distintos.

Com relação ao sistema, será necessária a identificação do usuário em redes diferentes e a atualização de sua localização, efetuar ***handovers* verticais** e **horizontais** (Tabela 1) com o mínimo de latência e perda de pacotes, integrar sistemas que utilizam IP com outros sistemas que não utilizam IP, garantir QoS fim-a-fim através de sistemas diferentes, tratar de problemas de segurança envolvidos no mecanismo de reconfiguração dinâmica e adaptação e ser tolerante as falhas.

Considerando os serviços, esses devem ser adequados para coletar, gerenciar e armazenar informações da conta do usuário, realizar de maneira eficiente a tarifação, prover mobilidade transparente sem necessidade de modificar os servidores existentes nos sistemas heterogêneos.

Um cenário de NGN é ilustrado na Figura 4 com diferentes tecnologias de redes (Wi-Fi, Bluetooth, Wi-Max, etc.) e suas coberturas, algumas possibilidades de *handover*, como por exemplo, de Wi-Max para GPRS, efetuados por dispositivos móveis como notebooks, celulares, PDA´s, etc. em diferentes ambientes (carro, casa, trem).

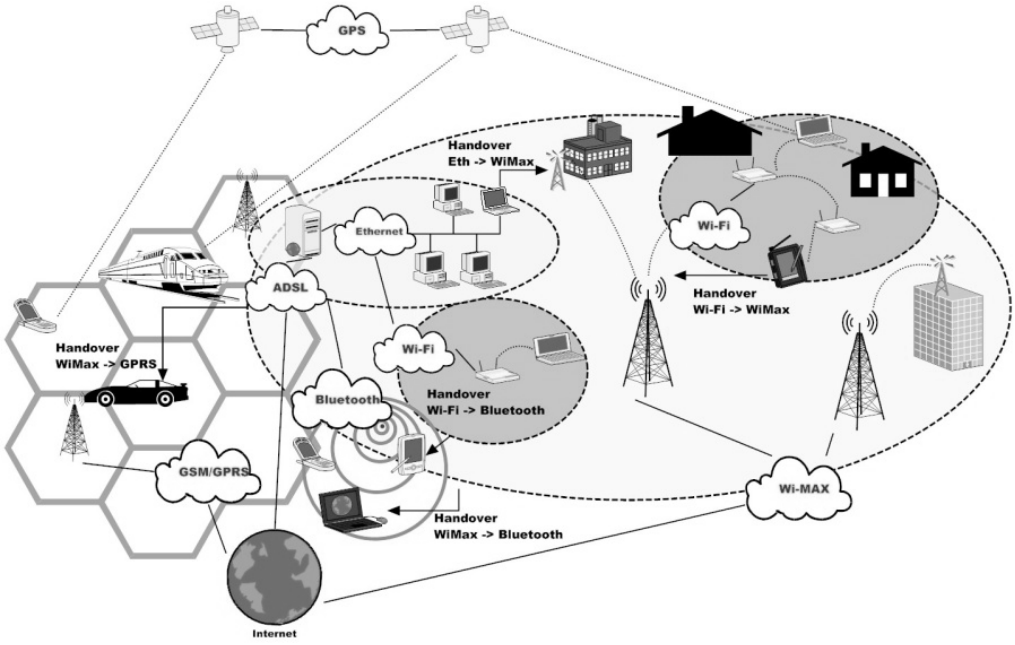

Figura 4: Exemplo do ambiente NGN

2.4. Classificação do *handover*

Na literatura são encontradas diversas classificações para um *handover* de acordo com a perspectiva, com a **camada,** com o **sistema**, com a **tecnologia,** a **decisão,** o **desempenho,** o **procedimento** e com a **conexão**. De forma sucinta, algumas são apresentadas na Tabela 1 e definidas com base na RFC 3753 (Manner e Kojo, 2004). Em complemento às classificações da Tabela 1, pode-se ainda ter uma perspectiva dos motivos pelos quais o usuário faz *handovers* (Moreira et. al.). Outra perspectiva está relacionada ao paradigma centrado no usuário, o ***handover* alternativo**, cujo objetivo principal é atender as preferências do usuário e melhorar a sua experiência durante a utilização do serviço.

Tabela 1: Classificação dos *handovers*

Perspectiva	Tipo	Definição
Camada	Enlace	Quando a transição do ponto de acesso é transparente para a camada 3, i.e., não ocorre novo endereçamento IP.
	Rede	Envolve o gerenciamento de mobilidade por meio de um protocolo com suporte a mobilidade, pois um novo endereço IP é atribuído para o Nó Móvel.
	Transporte	Abstrai a camada da rede, ou seja, é independe do conceito de rede de origem ou infraestrutura adicional, uma vez que o gerenciamento da mobilidade é realizado fim-a-fim.
	Aplicação	Uma aplicação gerencia a troca
Sistema	Intra-Sistema	São trocas sob o mesmo domínio, ou seja, quando ocorre entre o mesmo sistema.
	Inter-Sistema	Quando ocorrem transições entre domínios diferentes, requerendo o suporte de macro-mobilidade e envolve a atribuição de um novo endereço IP para o Nó Móvel.
Tecnologia	Horizontal ou Homogêneo	Caracterizado quando Nó Móvel é deslocado entre pontos de acesso de mesma tecnologia de comunicação.
	Vertical ou Heterogêneo	Caracterizado quando ocorrem transições entre tecnologias de comunicação distintas.
Decisão	Assistido pelo Nó Móvel	Informação e medidas obtidas do Nó Móvel são passadas para o Roteador de Acesso que decide sobre a execução *handover*.
	Assistido pela rede	Quando a Rede de Acesso recolhe informações que podem ser utilizadas pelo Nó Móvel na decisão do *handover*.
	Não assistido	Nenhuma informação para ajudar na decisão *handover* é trocada entre o Nó Móvel e o Roteador de Acesso.
Desempenho	*Smooth*	O objetivo principal é minimizar a perda de pacotes, sem preocupação com atrasos adicionais na transmissão.
	Fast	Visa principalmente minimizar a latência, sem se preocupar com a perda pacotes.

	Transparente	É considerado transparente, na prática, quando aplicações ou usuários não detectem quaisquer alterações no serviço e seja visto como uma degradação da qualidade.
Procedimento	Proativo	É caracterizado por ser uma troca planejada por meio da monitoração de parâmetros da rede, ou seja, feita antes da desconexão.
	Reativo	É uma transição inesperada, não são feitas indicações para auxiliar na passagem para nova rede.
Conexão	*Make-before-break* ou *soft handover*	Permite o Nó Móvel conectar ao mesmo tempo no próximo ponto de acesso e continuar com o original durante o *handover*.
	Break-before-make ou *hard handover*	Somente se conecta a um ponto de acesso por vez, ou seja, desconecta do ponto de acesso atual para depois de conectar ao próximo.

2.5. Protocolos de Gerenciamento de Mobilidade

Na literatura são encontradas algumas soluções para o gerenciamento de mobilidade. A seguir são apontadas as que foram consideradas mais significativas. Uma forma de classificar as soluções é pela camada na qual é implementada. Sendo assim, iniciando pela Camada de Rede, tem-se os protocolos Mobile IP versão 4 (Perkins et al., 2002), *Mobile IP* versão 6 (Johnson, 2004) e suas variações *Hierarchical* MIPv6 (Soliman et al., 2005) e *Fast* MIPv6 (Koodli et al., 2005).

Na Camada de Transporte tem-se os protocolos HIP (Moskowitz e Nicander, 2006) cuja proposta é a utilização de um *Host Identity* separando a identificação do *host* e o endereço IP; MSOCKS (Maltz e Bhagwat, 1998) propõe um *proxy* para manter as conexões; MSCTP (*Mobile Stream Control Transmitioin Protocol*) (Stewart et al., 2000) estende o SCTP para suporte a mobilidade e TIPS (*Transparent IP Sockets*) (Kimura e Guardia, 2008) faz uma adaptação da API *Berkeley Sockets* para prover mobilidade. Finalmente, para a Camada de Aplicação o mais significativo é protocolo SIP, *Session Initiation Protocol* (SIP) (Rosenberg et al., 2002) inicialmente projetado para transmissão multimídia, foi alterado para suportar mobilidade. Entre as soluções encontradas, o *Mobile* IP versão 6 é um dos mais referenciados na literatura, por isso, optou-se por sua utilização.

2.6. *Mobile IP* versão 6

O protocolo *Mobile* IPv6 (Johnson et al., 2004) foi desenvolvido para permitir Macro-Mobilidade. De forma que os **N**ós **M**óveis (NM) ou Terminais Móveis (TM) se deslocam de uma rede para outra em sistemas homogêneos e heterogêneos (Vidales et al., 2007). Os dois principais cenários especificados pelo MIPv6 são:

Primeiro, quando o NM está conectado à sua ***H**ome **N**etwork* (HN) (onde o dispositivo móvel é registrado como uma entidade local), os pacotes entre os ***C**orrespondent **N**ode* (CN) (ou seja, os nós que se comunicam com o NM) e o NM são entregues usando roteamento normal do IP, como ilustrado na Figura 5 (A).

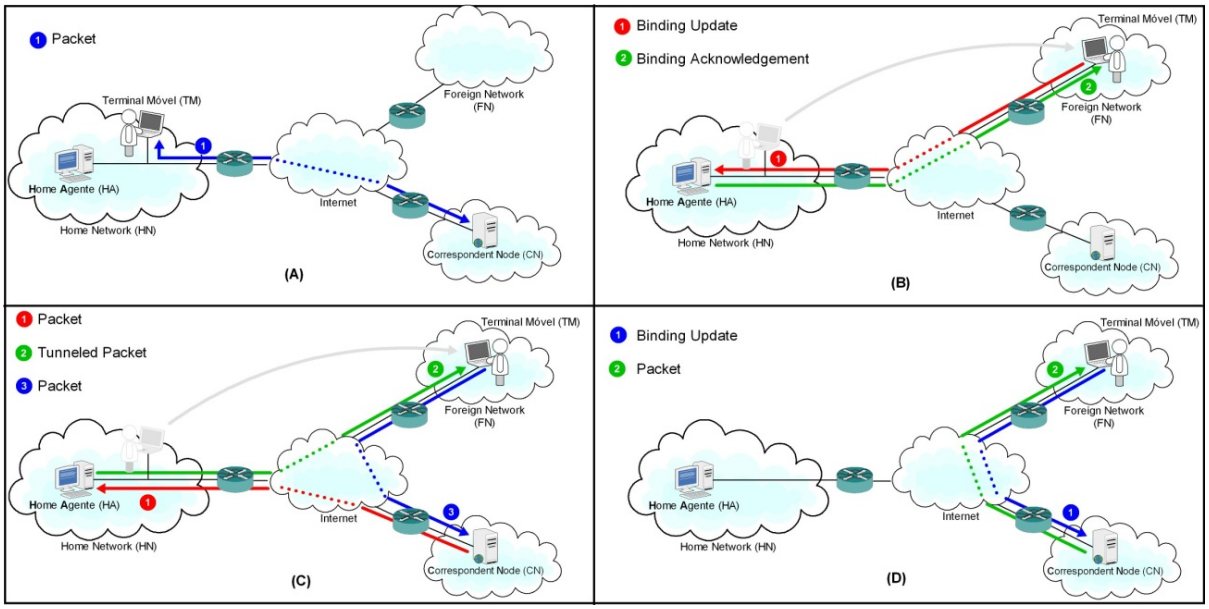

Figura 5: Funcionamento do *Mobile* IP (Adaptado de Heissenhuber ., 2002): (A) Roteamento normal de pacotes entre o NM e o CN; (B) O NM registra-se com seu HA; (C) Roteamento triangular e (D) Otimização de rota.

O segundo cenário pode ser observado na Figura 5 (B), e ocorre quando o NM está ligado a uma *Foreign Network* (FN) (rede externa/visitada/estrangeira), ou seja, não ligada à sua HN. Neste caso, a comunicação entre NM e CN pode acontecer de dois modos: tunelamento bidirecional - Figura 5 (C) ou otimização de rota - Figura 5 (D).

No tunelamento, um túnel bidirecional é criado entre o NM, e o ***H**ome **A**gent* (HA), que é um roteador que suporta encaminhamento de pacotes para os nós registrados. O HA encapsula os pacotes e os roteia para o NM usando seu ***C**are-**o**f **A**ddress* (CoA), atribuído ao NM por uma autoridade local da FN que utiliza um mecanismo de autoconfiguração

Para que seja possível saber onde o NM se encontra, uma associação (*binding*) entre *Home Address* e *CoA* deve ser realizada. O *Home Address* é constituído de um prefixo válido no *link* de sua HN. É por meio deste endereço que um CN irá se comunicar com o TM, independente de onde este estiver. Esta associação do *CoA* é feita pelo NM, no HA pelo procedimento de *Binding Registration* (Figura 5 - B), onde o NM envia mensagens ***B**inding **U**pdates* (BU) para o HA, que responde com uma mensagem ***B**inding **A**cknowledgement* (BA) (6NET, 2005; Martins et al., 2003).

Este modo de comunicação entre o NM e CN, não requer que o CN tenha suporte ao MIPv6 e que o NM tenha se registrado com o CN. Os pacotes são roteados do CN para o HA e do HA são tunelados para o TM. Depois, o TM responde para o HA pelo túnel que, por sua vez, responde para o CN; cada pacote interceptado é tunelado para o *CoA* do NM, como ilustrado na Figura 5 (C) (Martins, 2003).

No caso da otimização de rota, MIPv6 define o procedimento para evitar o problema do roteamento triangular causado pelo uso de túneis bidirecionais. Este mecanismo permite que os TM enviem mensagens BU também para os CN, não só para o HA, a fim de informar sobre a localização atual do TM (ou seja, CoA do TM). Depois que o CN está ciente da localização real do TM, a comunicação é direta entre CN e TM, eliminando o congestionamento no *Home Network*, pois ignora o HA. Entretanto, o CN deve ter suporte ao MIPv6 e o TM deve se registrar com o CN (Heissenhuber e Fritsche, 2002).

O seguintes passos são especificados pelo procedimento do *handover* no MIPv6:

1) **Detecção do movimento**, quando o TM percebe que o atual roteador de acesso não é mais alcançável (*unreachable*), ou um novo e diferente roteador de acesso está disponível;
2) **Router Discover,** é realizado pelo recebimento de mensagem *Advertisement* enviada pelo novo roteador de acesso (AR –*Access Router* da FN).
3) **Address Configuration**, o TM auto-configura um endereço IPv6 para ser usado na nova rede. Este processo pode ser feito de maneira *Stateful* ou *Stateless*.
4) **Duplicate Address Detection**, um TM que entra em uma nova rede deve assegurar que o CoA obtido pelo *Address Configuration* é único.
5) **Register New CoA**, informa o HA da sua nova localização, por meio das mensagens BU e BA. Os pacotes enviados do TM para o CN, durante o processo de registro, são perdidos.
6) **Binding Update Completion**, este estágio refere-se ao TM informar todos os CNs da sua nova localização. Além de enviar as mensagens BU para o CN, existe um procedimento adicional conhecido como teste *Return Routability* (RR) que é utilizado para evitar BU maliciosos enviados por terceiros. Em linhas gerais, RR usa o *Home Test* (HoT) e um *Care-of Test* (CoT). O CN aplica dois testes no TM via o HA e otimização de rota, respectivamente. O TM responde os dois testes com mensagens BUs enviadas para o CN. Se os testes são respondidos corretamente, CN valida o TM.

2.7. IEEE 802.21 - Protocolo para Gerenciamento de *Handover*

A fim de prover um melhoramento no gerenciamento do *handover*, surgiu o protocolo IEEE 802.21, um *framework* para otimizar o *handover* entre redes com tecnologias de acesso heterogêneas, definindo comandos e eventos que disparam o assistente no processo de decisão, utilizando trocas de informações do terminal móvel e da infraestrutura da rede. O padrão IEEE 802.21 oferece mecanismos para informar quais são as redes vizinhas disponíveis, a fim de ajudar o terminal móvel selecionar uma delas. O objetivo é realizar um *handover* mais inteligente e permitir que fabricantes e operadoras desenvolvam suas próprias estratégias e políticas de *handover*. Para isto, implementa uma camada intermediária MIHF (*Media Independent Handover Function*), que consiste de funções que residem entre as camadas 2 e 3 do modelo OSI, conforme Figura 6. Ela apresenta uma interface homogênea independente da tecnologia de acesso. Esta interface é responsável pela comunicação entre as camadas superiores e inferiores. Dutta (Dutta et al., 2007) descreve os três diferentes serviços definidos pelo MIHF, a saber: *Media Independent EventService* (MIES), *Media Independent Command Service* (MICS) e *Media Independent Information Service* (MIIS).

• ***Media Independent Event Service*** (MIES) oferece serviços para a camada superior comunicando eventos locais ou remotos. Evento local assume a posição dentro da pilha de protocolos locais no terminal móvel, enquanto eventos remotos assumem a posição em outro MIHF na rede. Suporta os eventos de transferência, filtragem e classificação de mudanças dinâmicas de características do link de acesso. Alguns dos eventos mais comuns são: "*Link Up," "Link Down," "Link Parameters Change," "Link Going Down" e "Handover Imminent,*" etc. As camadas superiores obtêm notificações sobre certos eventos e fazem uso do serviço de comandos para controlar os links e trocar para um novo ponto de acesso.

• ***Media Independent Command Service*** (MICS) permite que as camadas superiores controlem as funções das camadas inferiores, por meio de primitivas. Os comandos MICS são usados para coletar informações sobre o estado do link conectado, bem como para desempenhar mobilidade nas camadas superiores e decisão de conectividade nas camadas inferiores, de forma local ou remota. Alguns exemplos de comandos são: *"MIH Poll", "MIH Scan", "MIH Configure"* e *"MIH Switch"*. As instruções de um dispositivo MHI são

pesquisar os links conectados para aprender seus estados recentes, fazer uma varredura para descobrir novos links, configurar os novos links e trocar entre os links disponíveis.

• ***Media Independent Information Service*** (MIIS) oferece um mecanismo que permite à entidade descobrir e obter informações sobre as características e serviços providos pelas redes vizinhas, incluindo tipo de rede, parceria de *roaming*, canal utilizado, endereço MAC, mecanismos de segurança e outras informações sobre serviços de camadas superiores que ajudam na decisão de *handover* eficaz. Em alguns casos, as informações podem não estar disponíveis nas camadas inferiores ou serem insuficientes para tomada de decisão inteligente, podendo ser consultados os serviços das camadas superiores para ajudar na decisão de mobilidade. A MIIS especifica uma forma comum de representar a informação utilizando um formato padrão como XML (*eXtensible Markup Language*) e TLV (*Type-Length-Value*).

Lee (Lee et al., 2007) implementa o padrão IEEE 802.21 baseado na plataforma Linux e realiza um experimento de *handovers* entre redes 802.11 (Wi-Fi) e 802.16 (WiMAX). O MIHF do terminal móvel está ligado ao MjSIP e ao driver da interface. Para avaliar a o desempenho utiliza-se comunicações de vídeo e áudio baseados no SIP. Como resultado, apresenta dois gráficos, um do *handover* não assistido pelo 802.21 com 14.5s de latência e outro assistido pelo 802.21 com um melhoramento significativo, porém com flutuações da vazão.

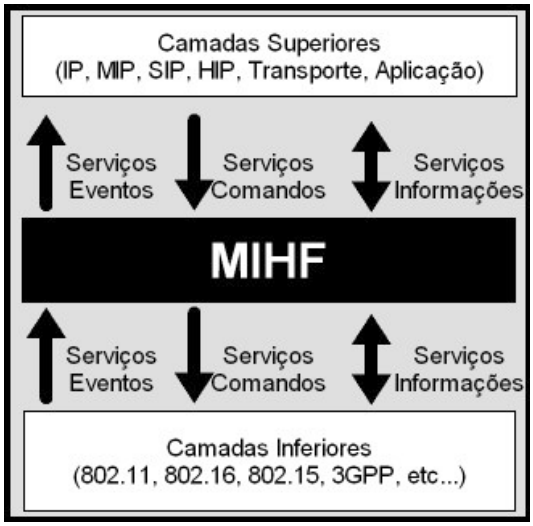

Figura 6-Media *independent handover framework*

O trabalho de Dutta (Dutta et al., 2007), apresenta uma solução com MPA (*Media-independent Pre-Authentication*) e o 802.21 para serem utilizados juntos a fim de melhorar a

performance do *handover* em redes de acesso heterogêneas; implementa um *testbed* e realiza diversas comparações de *handovers* assistidos e não assistidos. O *testbed* utiliza o MPA com SIP *Mobility* (Rosenberg e Schulzrinne, 2000) e o MIPv6 como protocolos de gerenciamento de mobilidade. A configuração é feita pelo protocolo DHCP e o agente de autenticação é o servidor PANA (Dutta et al., 2007). Os resultados obtidos dos experimentos validam a proposta de utilizar a MPA assistida pelo *framework* IEEE 802.21, podendo prover uma convergência para um *handover* transparente em diferentes cenários reduzindo a perda de pacotes e atrasos para níveis aceitáveis de tráfego streaming e VoIP.

2.8. Considerações Finais

Uma revisão das NGN foi apresentada neste Capítulo. O protocolo MIPv6 foi apresentado em detalhes, pois é de interesse ao trabalho. Na literatura, as pesquisas tentam resolver o problema do gerenciamento de mobilidade e *handover*. Uma das possibilidades é agregar contexto a estas soluções; neste sentido, o padrão 802.21 tem-se mostrado promissor. Outra possibilidade é explorar o evento *handover* e as informações contextuais envolvidas para prestações de novos serviços.

3. *Handover* Ciente de Contexto

3.1. Considerações iniciais

O *handover* ciente de contexto está relacionado ao gerenciamento do *handover*. Essa mudança passa a ser apoiada pela computação ciente de contexto, ou seja, o dispositivo captura o contexto e, por meio dessas informações, realiza decisões sem a interferência explícita do usuário. As decisões, nesses casos, envolvem a escolha do novo ponto de acesso, visando trazer benefícios para o usuário, por exemplo, melhor QoS.

Neste sentido, é importante a definição de contexto e sua classificação. A ideia de contexto utilizada neste trabalho é compreendida na definição realizada por Dey (Dey, 2001). Porém, as informações de contexto da rede difere das propostas normalmente encontradas na literatura, como discutido na seção 3.2.

Além de classificar as informações de contexto, outro problema é aplicar o contexto em NGN. Uma vez capturadas as informações, o dispositivo tem que decidir a ação a ser realizada com base em diversos dados, e por isso, é necessário um algoritmo de decisão. Por meio da revisão bibliográfica dos trabalhos relacionados encontrou-se o AHP (*Analytic Hierarchy Process*) já descrito na seção 3.4.

Na Seção 3.3 é realizada uma discussão sobre os trabalhos relacionados e por fim, na Seção 3.5 são apresentadas as considerações finais do Capítulo.

3.2. Classificação de Contexto

Essa discussão não tem a pretensão de relatar exaustivamente as classificações da literatura, pois o assunto ainda está em aberto, mas abordar alguns trabalhos importantes que direcionem a classificação das informações utilizadas neste trabalho.

Além da discussão sobre a definição do que é contexto, na literatura encontram-se diversas formas para classificar instâncias de contexto, como o trabalho de Prekop (Prekop, 2003) que apresenta uma distinção de dimensões de contexto chamadas de externas e internas. Hofer (Hofer et al., 2002) apresenta tais dimensões como contexto físico e lógico. E Gu (Gu et al, 2005) classifica como contexto direto e indireto, dependendo da forma como a informação de contexto é obtida.

A dimensão externa, física ou direta, refere-se ao contexto que pode ser medido por sensores. Por exemplo, localização, luz, som, movimento, toque, temperatura ou pressão do ar. Gu (Gu et al., 2005) estende a dimensão externa, sendo aquelas obtidas por sensores ou definidas pelo usuário; um exemplo seria configuração de uma preferência.

A dimensão interna, lógica ou indireta é aquela principalmente capturada pelo monitoramento do usuário, ou inferidas por meio das informações obtidas na dimensão externa. Por exemplo, a tarefa, estado emocional, estado atual do usuário. A inferência pode ser pela localização do usuário na casa e com informações complementares, como chuveiro ligado e a porta fechada, isto pode significar que a atividade do usuário é "estar no banho".

Outra classificação de contexto é proposta por Dey (Dey e Abowd, 2001), com três distinções chamadas entidades: local (e.g. salas, prédios), pessoas (e.g. individual, grupos) e coisas (e.g. objetos pessoais, computadores), sendo que cada entidade possui atributos. Esses são divididos em quatro categorias: identidade (cada entidade tem um identificador único), localização (uma posição geográfica da entidade, proximidade, etc.), estado (ou atividade, significando uma propriedade intrínseca de uma entidade, por exemplo, temperatura, iluminação de uma sala, processos sendo executados no dispositivo etc.) e tempo (usado para marcar uma situação, ordens dos eventos, etc.).

Entre as diversas classificações, para este trabalho, foi definido um limite lógico que estabelecesse o espaço da informação do contexto. Esse limite é baseado na classificação proposta por Moreira (Moreira, 2007), na qual o contexto pode ser classificado como, **Usuário**, **Aplicação**, **Dispositivo**, **Rede** e **Ambiente**.

3.3. Trabalhos Relacionados

O *handover* ciente de contexto é uma das estratégias de decisão do *handover*. Na literatura foram encontrados os trabalhos de (Balasubramaniam e Indulska 2004) e (Ahmed, et al., 2006), que adaptam o AHP para decisão do *handover*. O AHP foi proposto por (Saaty, 1990) para problemas relacionados à tomada de decisão de forma geral.

Em (Balasubramaniam e Indulska 2004), o procedimento do *handover* é realizado por dois componentes. Um Repositório de Contexto instalado na infraestrutura da rede e um Gerenciador de Adaptação instalado no dispositivo móvel. O repositório de contexto é responsável por coletar, gerenciar e avaliar informações contextuais de diferentes pontos da rede. O gerenciador de adaptação decide sobre mudanças de contexto e executa o *handover*. O

resultado mostrou a necessidade de um mecanismo de decisão com base em mudança de contexto.

Em outro trabalho, (Ahmed et al., 2006) estabelece que para cada tipo de serviço em execução no dispositivo móvel é executado o algoritmo de seleção. A decisão é realizada em cinco estágios, dois de pré-configuração (entrada do usuário e mapeamento os valores limites de acordo com preferências) e três em tempo real (atribuição da pontuação para cada rede disponível, calcular a classificação de cada rede e gerenciar a sessão). A proposta foi simulada e demonstrou que a decisão do algoritmo funcionou corretamente.

Os dois trabalhos utilizam AHP ajustados para arquiteturas específicas e também diferem nos objetivos e parâmetros. Para Ahmed (Ahmed et al., 2006), os objetivos são definidos em termos de Menor Custo, Interface de Preferência e Melhor Qualidade (maximizando vazão, minimizando atraso, *jitter* e *bit error rate* – BER) e Balasubramaniam (Balasubramaniam e Indulska, 2004) aplica o algoritmo para atender a necessidade de QoS da perspectiva do usuário, visando maximizar *i)* as preferências do dispositivo do usuário e *ii)* vazão da aplicação e minimizar *iii) jitter*, atraso e perda de pacotes e *iv)* flutuação da vazão.

Uma abordagem similar a Balasubramaniam (Balasubramaniam e Indulska, 2004) é apresentada por Wei (Wei et al., 2006). Wei faz uso de um algoritmo de decisão implementando por meio de condicionais (*if...elseif...else*). Ainda, o trabalho utiliza alguns nós da rede como repositório de contexto, e esses são requisitados pelos dispositivos móveis no momento antecedente ao *handover*. Os parâmetros considerados na decisão são: localização, velocidade, trajetória e QoS requeridos pela aplicação. O principal resultado é a prova conceitual que os *handovers* são mais eficientes com relação à QoS quando utilizam informações contextuais.

As propostas de Balasubramaniam (Balasubramaniam e Indulska, 2004) e Wei (Wei et al., 2006), dependem de que alguns recursos sejam implantados em nós da rede, restringindo a solução. Pode-se também considerar a existência da sobrecarga (*overhead*) ocasionada pela troca de informações entre os nós e entre o dispositivo e o nó. Em ambientes NGN com redes heterogêneas, a oferta de diferentes provedores e com expectativa do acesso sob demanda, soluções que exigem infraestrutura homogênea podem torná-las inexequíveis

Os três trabalhos (Balasubramaniam e Indulska, 2004; Ahmed et al., 2006; Wei et al., 2006) apresentam em comum parâmetros relacionados à QoS necessária para a aplicação. Entretanto, o paradigma centrado no usuário abrange também os anseios, experiências e sentimentos do usuário (*user expierence*) durante a utilização da rede. Neste sentido, outras

informações, por exemplo, provedor de preferência e se a rede segura ou não, tornam-se parâmetros relevantes para seleção do ponto de acesso e desta forma são considerados nesta proposta. Por fim, cada trabalho relacionado define e classifica contexto da forma mais conveniente para suas pesquisas.

3.4. Algoritmo AHP

A descrição do algoritmo AHP tem com base os trabalhos relacionados da Seção 3.3. O AHP foi adaptado para o problema de decisão do *handover*, pois originalmente o AHP não foi proposto para utilizar informações contextuais em NGN. O AHP é um método para auxiliar em decisões complexas. Para tanto, realiza um procedimento para hierarquizar o problema e relacionar elementos com objetivos e critérios para avaliar soluções.

A adaptação proposta por Balasubramaniam e Ahmed (Balasubramaniam e Indulska, 2004; Ahmed, 2006) estabelece que a seleção da rede deve satisfazer um conjunto de objetivos. Por exemplo:

Objetivo 1) Maximizar vazão

Objetivo 2) Minimizar atraso

Objetivo 3) Minimizar perda de pacotes

Desta forma, o AHP para decisão da rede é calculado em três passos, sendo que as variáveis das equações estão descritas na Tabela 2:

1) Calcula os pesos dos objetivos utilizando a matriz A de comparação por pares de objetivo (eq. 3.1.). A dimensão da matriz A depende do número de objetivos *n.* Sendo *PR* a Pontuação Relativa em uma escala linear de 1 a 9. Então, a matriz *A* é normalizada dividindo cada elemento pela soma individual de sua coluna. A_{norm} é mostrada na eq.3.2. Por fim, a média de cada linha define os pesos *W* de cada objetivo (e.q. 3.3).
2) Calcula os pesos de cada rede disponível. Este passo determina a importância do objetivo corresponde para cada rede, diferente do passo 1 em que a importância do objetivo corresponde ao usuário. O cálculo é realizado utilizando as equações 3.1., 3.2 e 3.3. Então, E_{xn} para *x* números de redes e *n* números de objetivos são calculados similarmente ao passo 1.
3) Este último passo define a classificação final (F_x) de cada rede, determinada pelo cálculo da equação 3.4. Consiste na soma dos produtos dos pesos das redes (E_{xn})

por pesos dos objetivos individuais (W_n). A rede com maior pontuação é selecionada.

A rede selecionada é aquela que obtiver maior valor de F_x. O principal problema para se utilizar o algoritmo é encontrar uma função que linearize a *PR* entre 1 e 9 para um determinado objetivo. Pawar (Pawar et al., 2008) propôs uma simplificação, adotando pesos fixos entre 0 e 1 para os objetivos do usuário, calculando apenas os valores dos pesos das redes disponíveis.

$$A = \begin{bmatrix} 1 & PR_{12} & \cdots & PR_{1n} \\ \frac{1}{PR_{12}} & 1 & \cdots & PR_{2n} \\ \vdots & \vdots & \cdots & PR_{3n} \\ \frac{1}{PR_{1n}} & \frac{1}{PR_{2n}} & \cdots & 1 \end{bmatrix} \quad (3.1)$$

$$A_{norm} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \quad (3.2)$$

$$Wi = \frac{a_{i1} + a_{i2} + \cdots + a_{in}}{n} \quad (3.3)$$

$$F_x = \sum_{1}^{xn} E_{xn}(W_n) \quad (3.4)$$

Tabela 2 - Descrição das variáveis do algoritmo

Variáveis e Estruturas	Descrição
x	Número de redes.
n	O número de objetivos.
PR	Peso Relativo atribuído a cada objetivo.
E_{xn}	Peso final de cada rede.
A	Matriz de comparação por pares.
A_{norm}	Matriz A normalizada.
W	Peso final de cada objetivo.
F_x	Peso final de cada rede *x*.

3.5. Considerações finais

A definição de contexto utilizada neste trabalho é bem aceita pela comunidade científica. A classificação das informações de contexto foi definida do ponto de vista desta

pesquisa, seguindo a proposta de Moreira (Moreira et al., 2007). O objetivo principal do Capítulo foi discutir o uso de contexto em NGN, especificamente para serviços, como a escolha do ponto de acesso.

Nos trabalhos relacionados, seus autores não discutem as formas de captura do contexto, e entende-se que eles assumem que tais informações são disponibilizadas por algum serviço. Pois, existem diversos problemas para a obtenção de medidas de atraso, jitter, perda de pacotes e a vazão da rede em tempo real. Algumas delas são: *i)* se forem medidas por conexões fim-a-fim a partir do dispositivo móvel, as redes visitadas têm que ser modificadas para captura dos valores; *ii)* no caso da utilização de monitores na infraestrutura, esses devem estar presentes em cada ponto de acesso; *iii)* existe o *overhead* gerado pelas medições; *iv)* o gerenciamento das informações quando necessitarem trafegar pela Internet.

Desta forma, o diferencial deste trabalho é abordagem prática, da captura, uso de contexto e implementação do AHP. Adicionalmente, é realizada uma avaliação do algoritmo.

4. *Testbed* NGN

4.1. Considerações iniciais

Para a avaliação dos protótipos utilizados como prova de conceito foi implantado um *testbed* com o protocolo MIPv6. A ideia do *testbed* é realizar os testes e também analisar o comportamento MIPv6 em ambientes não simulados.

A rede de teste possui três pontos de acesso Wi-Fi. Inicialmente, realizou-se um teste de desempenho do MIPv6, medindo a latência do *handover* horizontal. Em outra etapa foi utilizado para avaliar os impactos da captura de informações de contexto.

Este capítulo apresenta as tecnologias utilizadas para a implantação do *testbed* e sua avaliação de desempenho inicial. Na Seção 4.2 é apresentada uma classificação das tecnologias de rede sem fio. A Seção 4.3 aborda os tópicos tecnologia Wi-Fi de interesse para o *testbed*. Na Seção 4.4. é realizada uma breve descrição dos endereçamentos de IPv6 e o mecanismo de atribuição dinâmica de IP. Por fim, na Seção 4.5 é apresentado o detalhamento do *testbed* e resultados da avaliação.

4.2. Classificação das tecnologias de rede sem fio

Uma das formas de categorizar as redes sem fio é de acordo com sua área de cobertura. Essencialmente, são divididas em: *Wireless Personal Area Network* (WPAN), *Wireless Local Area Network* (WLAN), *Wireless Metropolitan Area Networks* (WMANs) e *Wireless Wide Area Networks* (WWANs), seguindo a ordem da menor para maior abrangência. Na Tabela 3 são apresentadas as principais tecnologias de rede e sua classificação conforme as áreas de cobertura, a aplicação típica para a rede, valores aproximados de alcance e da taxa de transferência de dados, frequência de operação e, por último, se alguns desses padrões mais atuais estão incorporando a capacidade de *handover*.

4.3. IEEE 802.11

O padrão da família IEEE 802.11 foi apresentado em 1997. Desde então, vem se popularizando e tornou-se conhecida como WLAN, ou ainda, redes Wi-Fi, de *Wireless Fidelity,* um consórcio que certifica, e desta forma, garante a interoperabilidade dos

dispositivos 802.11. A primeira versão do padrão atingia a vazão máxima de 2Mbps; os padrões subsequentes, o 802.11b atingia, 11Mbps, 802.11a e 802.11g chegaram a 54Mbps e o mais atual, o 802.11n, consegue vazões superiores a 108Mbps.

A rede WLAN possui dois modos de trabalho, o primeiro é infraestruturado com um AP e estações associadas, com as comunicações sempre conduzidas pelo AP. O segundo modo de trabalho é o descentralizado ou *Ad-Hoc* (não infraestruturado), em que estações comunicam-se diretamente. O padrão 802.11 especifica a camada física e a camada de enlace de dados, que serão abordadas nas Seções seguintes.

Tabela 3 - Tecnologias de rede sem fio

Tecnologia	**BLUETOOTH (IEEE 802.15.1)**	**Wi-Fi (IEEE 802.11g)**	**WiMAX (IEEE 802.16)**	**GSM/GPRS**
Classificação	WPAN	WLAN	WMAN	WWAN
Aplicação típica	Substituir cabos na interconexão de dispositivos	Acesso à Internet em redes locais	Provimento de Internet	Telefone, mensagem multimídia e acesso a Internet
Alcance aproximado	10 ou 100m	≅ 30m ambientes fechados ≅ 100m ambientes abertos	≅3-5Km	≅1-5Km em cidades
Taxa de transferência de dados	Max. 1MBit/s	Max. 54Mbit/s	Max.75Mbit/s	Max. 170Mbit/s
Frequência de operação	2.4GHz	2.4GHz	10-600 Ghz 2-11Ghz	900 Mhz 1800 Mhz 1900 Mhz
Capacidade de *handover*	Não	Não	Sim	Sim

4.3.1. Camada física

O primeiro padrão 802.11 especificou duas técnicas principais de transmissão, o *Frequency Hopping Spread Spectrum* (FHSS) e o *Direct Fequence Spread Spectrum* (DSSS), mas logo foi substituído pelo 802.11b que utiliza a técnica *High Rate DSSS* (HR-DSSS). Os padrões atuais, 802.11a e 802.11g passaram a usar *Ortogonais Frequency Division Multiplexing* (OFDM). O próximo padrão, 802.11n, acopla o mecanismo *Multiple Input Multiple Output* (MIMO) ao OFDM (Kuran, 2007).

As faixas de frequência utilizadas nos equipamentos 802.11 são: 2400-2483,5 MHz para os padrões 802.11b/g/n e 5725-5850 MHz para os padrões 802.11a/n. A frequência de 2,4 GHz é dividida em 14 canais, sendo que, a quantidade de canais é disponibilizada de acordo com a legislação do país. No Brasil estão disponíveis 11 canais de 22Mhz em

frequência não licenciada. Para o padrão 802.11a os canais são de 20Mhz e variam de 34 a 161. Os canais são utilizados para mitigar as interferências que ocorrem durante as transmissões. Uma interferência pode ocorrer quando dois sinais de rádio distintos são enviados ao mesmo tempo e na mesma frequência (Rappaport, 2009).

Normalmente, as interferências nas WLANs são interferências de mesmo canal, quando dois APs operam no mesmo canal. Outra forma pode ser por sobreposição de canais adjacentes, que ocorre quando dois APs utilizam canais próximos a ponto das frequências se sobreporem. Para evitar interferências, até 3 APs 802.11b/g, podem usar os canais 1,6 e 1, pois eles não se sobrepões, como ilustrado na Figura 7. O 802.11a tem a vantagem de utilizar uma banda menos saturada, não exposta a interferência de aparelhos de telefone sem fio e forno micro-ondas (Tanenbaum, 2003).

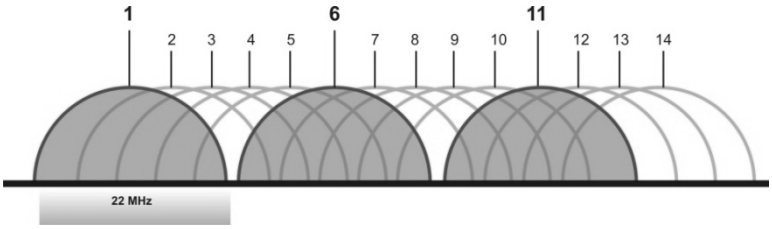

Figura 7 - Canais sem sobreposição em APs 802.11b/g (Carvalio Jr, 2009)

4.3.2. Camada de enlace de dados

A camada MAC (*Media Access Control*) admite dois modos de operação, o DCF (*Distributed Coordination Function*) e o PCF (*Point Coordination Function*). Contudo, PCF não é certificado pelo consórcio Wi-Fi, e como consequência, é pouco utilizado (Kuran, et al.,2007). O DCF utiliza o mecanismo CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*) para evitar colisões.

O CSMA/CA não garante a probabilidade de não ocorrer colisão, por isso foi introduzido um mecanismo de confirmação. Em linhas gerais, se uma estação quer transmitir dados, primeiro deve enviar um quadro RTS (*Ready-To-Send*) para a estação destino; se a estação destino não estiver transmitindo ela responde com um quadro CTS (*Clear-To-Send*); depois de receber a confirmação, a estação transmissora envia os dados. Por fim, a estação destino responde com um quadro ACK (*acknowledgment*) (Bernt, 2008).

4.3.3. Qualidade de Serviço, Segurança e Gerenciamento

Em 2005, o IEEE desenvolveu o 802.11e, que consiste em padronizar a QoS; duas técnicas foram introduzidas: o *Hybrid Coordination Function* (HCF) e o *Enhanced Distributed Coordination Function* (EDCF), uma com base no PCF e outra no DCF, respectivamente. As técnicas permitem priorizar pacotes; os com alta prioridade acessam mais rápido o canal do que os com baixa prioridade. São definidas quatro categorias: voz, vídeo, melhor esforço e tráfego em segundo plano, sendo voz o de maior prioridade e o tráfego de segundo plano a de menor prioridade (Bernet, 2008).

A fim de evitar escutas não autorizadas, a autenticação e a criptografia são tratadas na camada MAC com mecanismos de segurança. No início, havia somente método de criptografia *Wired Equivalent Privacy* (WEP), mas este apresentou problemas de segurança. Então, o consórcio Wi-Fi desenvolveu outro método de criptografia o Wi-Fi *Protected Access* (WPA). Por fim, uma versão melhorada do WPA também foi integrada ao padrão 802.11i, chamado de WPA2.

O padrão 802.11 original não foi desenvolvido pensando em mobilidade, ou seja, o usuário não pode efetuar transições sem perda de conexão entre as redes WLAN. Entretanto, o IEEE está projetando o 802.11s destinado a comunicação intra APs para suporte a redes *Mesh*, mas ainda não oferece uma solução para os *roamings* (Kuran et al., 2007).

4.4. Protocolo IPv6

Esta seção tem por objetivo abordar somente dois pontos de interesse sobre o protocolo IPv6, esses são relacionados à implantação do *testbed*. As classes de endereçamento e o mecanismo de atribuição dinâmica de IP.

O protocolo IPv6 permite mais de um endereço na mesma interface. Essa característica é utilizada por aplicações, normalmente de controle, que necessitam de endereços especiais (e.g. autoconfiguração de IP). O protocolo tem 3 tipos de endereços: *Unicast*, *Multicast* e *Anycast*. O endereço do tipo *broadcast* não existe; consequentemente, o protocolo ARP (*Address Resolution Protocol*) também deixou de ser utilizado. Uma descrição sucinta de cada tipo de endereço é dada a seguir (Silva e Faria, 2001):

Unicast: Identifica uma única interface. Desta forma, um pacote destinado a um endereço do tipo *Unicast* é enviado diretamente para a interface associada a esse endereço.

Anycast: Identifica um grupo de interfaces de *hosts* diferentes. Um pacote destinado a um endereço *anycast* é enviado para uma das interfaces identificadas pelo endereço.

Multicast: Identifica um grupo de interfaces ou um grupo de *host*, mas um pacote destinado a um endereço *multicast* é enviado para todas as interfaces do grupo. Um *host* pode pertencer a mais de um grupo *multicast*.

Considerando os três tipos citados, o tipo de endereçamento de interesse é *unicast*, que é divido em outras categorias, a saber:

- *Agregatable Global Unicast Address*
- *Loopback Address*
- *Unspecified Address*
- *NSAP Address*
- *IPX AddressSite-local Unicast Address*
- *Link-local Unicast Address*
- *IPv4-compatible IPv6 Address*

No *testbed* foram utilizados endereços *Agregatable Global Unicast Address.* É o globalmente da Internet e definido pelo prefixo do formato 001. Na Figura 8 é ilustrada a estrutura.

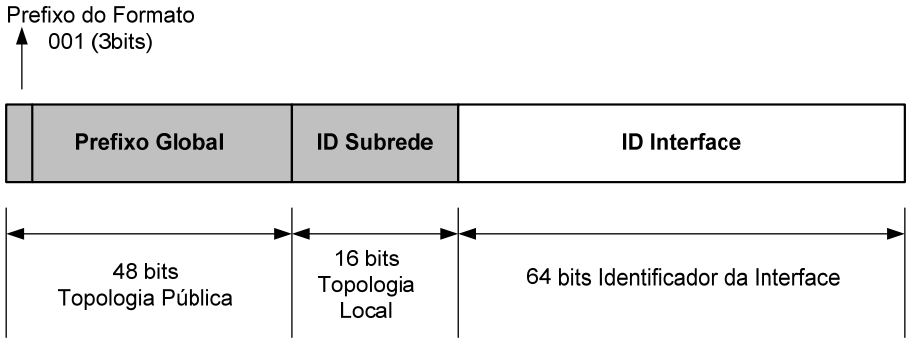

Figura 8 - Estrutura endereço *Global Unicast* (adaptado de Davies, 2008)

Uma vez definido o tipo de endereçamento a ser utilizado no *testbed*, o próximo tópico é o mecanismo de autoconfiguração de endereçamento; o IPv6 possui dois principais mecanismos:

- *Stateless* – A configuração é com base em mensagens de *Router Advertisement* (RA) recebidos.
- *Stateful* – É uma configuração por meio de protocolo de configuração de endereço, por exemplo, o DHCPv6.

Como a documentação do MIPv6 utilizava o mecanismo *Stateless*, decidiu-se utilizá-lo. Para esse funcionar, os *hosts* IPv6 devem ter endereços do tipo *link-local* (prefixo FE80::/10 + endereço MAC), que são automaticamente configurados no momento que o *host* é iniciado. Esse tipo de endereço habilita o *host* para se comunicar com vizinhos do mesmo enlace e também a configurar-se. Assim, ao receber um RA do roteador de seu enlace, automaticamente configura-se com um endereço *Global Unicast*.

O RA informa o prefixo da rede e o endereço do roteador, esses usados na configuração do *gateway*. Porém, para que o *host* seja capaz de utilizar as informações do RA é necessário que o prefixo de rede seja de 64 *bits*, caso contrário o *host* não poderá executar tal operação (Urtado e Alves Jr, 2009). No Linux o envio de RA pelo roteador é realizado pelo *software radvd* e deve-se configurar o arquivo *radvd.conf* com os prefixo(s) a ser(em) propagados por uma determinada interface.

4.5. *Testbed*

O *testbed* foi instalado conforme o diagrama da Figura 9. Para tanto, utilizou-se como a implementação a documentação de MIPL (*Mobile* IP for Linux) (MIPL, 2009). O protocolo MIPv6 foi instalado no Dispositivo Móvel (*Mobile* Node – MN), no Home Agent (HA) e no Correspondent Node (CN) e opcionalmente o mecanismo de otimização de rotas poderia ser ativado. Os Roteadores de Acesso (RA) foram configurados com protocolo IPv6. A configuração dos nós da rede é mostrada na Tabela 4, os AP utilizados foram os D-Link DIR-635, configurados no padrão IEEE 802.11g, SSIDs AP1, AP2 e AP3 e operando nos canais 1, 6 e 11, respectivamente; Sistema Operacional (SO) utilizado nos computadores foi o Debian 4.0 com kernel 2.6.16 compilado com o MIPv6.

Tabela 4 - Configuração dos nós do *testbed*

Função do Nó	Endereço IPv6	Processador	Memória RAM	Interface(s)
MN	2000:a::20/64	Core 2 Duo	1Gb	802.11g (Intel)
HA	2000:a::10/64	P4 3Ghz	1Gb	1Gbps (3Com)
CN	2000:e::1/64	QuadCore	4Gb	1Gbps (Nvidia)
RA-1	2000:a::1/64	P4 1.7Ghz	512Mb	100Mbps (3Com)
	2000:b::1/64			100Mbps (Encore)
RA-2	2000:b::2/64	P4 2Ghz	512Mb	100Mbps (3Com)
	2000:c::1/64			100Mbps (Encore)
	2000:d::1/64			100Mbps (Encore)
	2000:e::2/64			100Mbps (Encore)

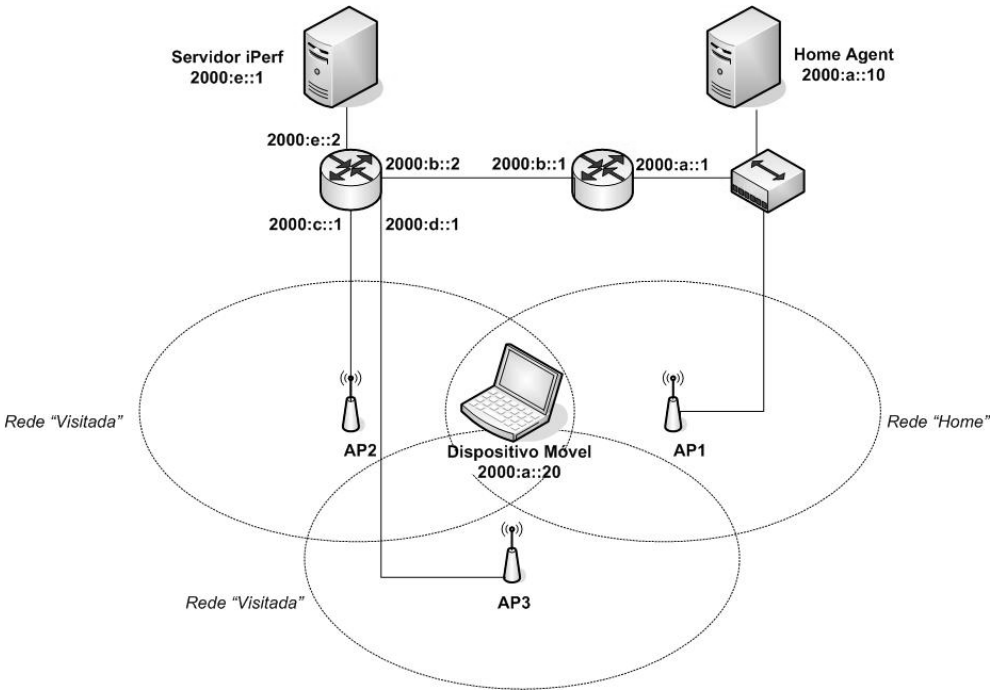

Figura 9 - *Testbed Mobile* IP versão 6

4.6. Avaliação de Desempenho do MIPv6

A finalidade da avaliação foi verificar o funcionamento da implementação do protocolo MIPv6 instalado e também o desempenho em *handovers* com a tecnologia IEEE 802.11 em ambientes não simulados. Para isso, foi utilizada a ferramenta iPerf (iPerf, 2009) que, em síntese, gera um fluxo TCP até ocupar a vazão máxima suportada pela rede.

O iPerf foi instalado em dois nós da rede; no MN o iPerf cliente e no CN o iPerf servidor. O MIPv6 foi configurado com o mecanismo de otimização de rotas. Um script (*shell script*) foi criado no MN para automatizar o procedimento do *handover* . O *script*, em linhas gerais, executava um laço de repetição de até 100 trocas de rede; para cada troca; iniciava uma conexão de 45s com iPerf servidor e após 8s saltava para outra rede, permanecendo até o fim da transmissão. Os valores de vazão retornados do iPerf a cada 0.5s foram redirecionados para um arquivo e plotados no gráfico da Figura 10.

No gráfico de dispersão apresentado na Figura 12 tem-se a vazão obtida em função do tempo. A concentração da vazão ficou no intervalo entre 18 a 20 Mbps, contudo, neste caso, o MIPv6 não influenciou na vazão, porque medidas realizadas com IPv4, obtiveram o mesmo valor na vazão. A latência do *handover* com *Mobile* IPv6 em redes 802.11g, representa a latência do ponto de vista da aplicação, ou seja, é o tempo total sem transmissão medido pelo iPerf. Aferiu-se que a média da latência é de aproximadamente 10.21s.

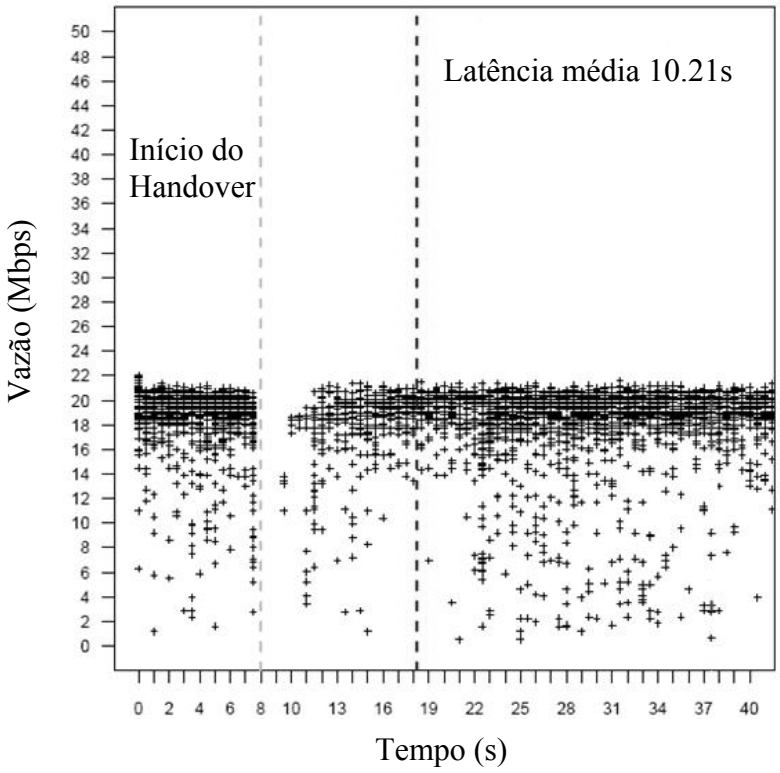

Figura 10 - Gráfico de dispersão da vazão e latência do *handover*.

4.7. Considerações finais

O protocolo MIPv6, até o fim deste trabalho, não é suportado nativamente pelos SO Windows e Linux, as versões mais recentes desses sistemas implementam até o IPv6. Para o Linux existem opções de MIP, tanto nas versões 4 e 6. A implementação mais recente, até o momento, é MIPL.

A instalação do MIPv6 exige a compilação do kernel do SO Linux e essa etapa demorou mais que o planejado devido às dificuldades encontradas. A implementação atual é somente para o kernel 2.6.16, essa versão do kernel é obsoleta e não possui drives para as interfaces de rede sem fio mais recentes. Outra dificuldade foi documentação para a compilação, que deixou de ser atualizada na versão do kernel 2.4.x e os módulos e arquivos de configuração não condiziam com a versão atual. Após ter sucesso na compilação, gastou-se um tempo para entender como configurava o MIPv6, devido também à falta de documentação atualizada. E ainda foi preciso estudar as classes de endereçamento IPv6, e principalmente, como implantava o mecanismo de atribuição de endereço *stateless*.

5. Serviços com Contexto em NGN

5.1. Considerações Iniciais

O objetivo principal deste trabalho foi explorar as informações contextuais relacionadas ao ambientes NGN. Para validar os conceitos, cogitaram-se dois cenários, o primeiro um ***Mashup*** para apontar no mapa as redes disponíveis em determinado local. *Mashup* pode ser entendido como uma página Web que combina informações e/ou funcionalidades de duas ou mais fontes da Internet, mas também pode ser visto como os usuários utilizam os sistemas existentes de forma inovadora (Wong e Hong, 2008).

O segundo cenário aborda o paradigma centrado no usuário, no qual ele pode escolher a rede a que irá se conectar. Um **Gerenciador de Conexões** verifica periodicamente as redes sem fio disponíveis e tenta automaticamente se conectar à rede que atenda as preferências do usuário.

Os dois cenários têm como base experimental a plataforma SOHand. Para se avaliar o gerenciador e os impactos da utilização de contexto em redes NGN foi implantado uma rede de teste com o protocolo de gerenciamento de mobilidade MIPv6.

Nas seções seguintes, serão descritas a arquitetura e a interação de seus módulos, os cenários e suas implementações. Na Seção 5.2 é realizada a descrição dos módulos da arquitetuta SOHand e suas interações; na Seção 5.3 são descritos os cenários que foram utilizados para validar os conceitos; na Seção 5.4 as informações de contexto são formalizadas por meio da linguagem OWL DL e por fim, na Seção 5.5 são apresentadas as considerações finais.

5.2. Uma breve descrição da arquitetura SOHand

A ideia central da arquitetura SOHand é disponibilizar uma plataforma abstrata (interfaces) para apoiar a prestação de serviços avançados de rede. A base do sistema é uma estrutura de informação versátil com suporte de uma ontologia compartilhada entre provedores e clientes. O cliente possui módulos capazes de capturar informações sobre, por exemplo, o usuário, a rede, os dispositivos, etc. O provedor de acesso pode ser classificado em categorias de serviço como tradicional (e.g., rede celular ou *hotspots* Wi-Fi) ou

comunitário (*e.g.*, redes *wireless mesh*). Em ambos, o usuário é beneficiado com a associação e correlação das informações contextuais para enriquecer a sua experiência durante o uso do ambiente de rede (Moreira, 2007)

SOHand além da habitual conexão com a Internet por meio de um provedor de acesso, apresenta o diferencial do gerenciamento de conectividade. Isso é feito por meio de uma abordagem centrada no usuário em detrimento à abordagem usual centrada no provedor. Dessa forma, a escolha do ponto de acesso passa a ser feita pelo usuário e embasada por informações contextuais.

Os serviços são facilidades (e.g. diretório de informação, uma operação, uma troca de mensagem, vídeo, voz, jogo) que um provedor de conteúdos oferece por meio de um serviço de acesso durante uma sessão com o usuário. Uma entidade pode oferecer acesso e conteúdo ao mesmo tempo. O usuário, durante o serviço, passa transparentemente pelas redes dos provedores de acesso e a conectividade é gerenciada por um mecanismo de suporte à mobilidade no cliente. Um *Broker*, além de centralizar as informações de contexto do cliente, pode atuar como intermediário na negociação AAA (*Authentication, Authorization e Accounting*) entre um cliente e um provedor e entre provedores. As informações do usuário, do dispositivo ou de qualquer serviço relacionado, podem ser utilizadas durante uma sessão para estruturar a segurança, a privacidade, a QoS, a tarifação e outras políticas.

5.2.1 Componentes da Arquitetura SOHand

A arquitetura SOHand é composta pelo **lado cliente,** pelo **lado provedor** e, eventualmente por um ***Broker***, conforme a Figura 11. No lado cliente existem diversas **Fontes de Contexto (FC)**. Cada fonte fornece informações que podem ser capturadas pelo dispositivo móvel. O **Gerenciador de Contexto (GC)** é responsável por: *1)* processar as informações de contexto das FC; *2)* armazená-las em uma **Base de Dados Local (BDL)**; e *3)* monitorar as condições da rede atual, do dispositivo e das preferências do usuário. O **Módulo de Negociação (MN)** utiliza os serviços disponibilizados por provedores de acesso, no ambiente de rede em questão, para negociar o acesso com base em políticas pré-definidas e em informações de contexto. O **Gerenciador de *Handover* (GH)** pode decidir qual é a melhor rede para a troca utilizando as preferências de preço e segurança definidas pelo usuário, por exemplo.

O provedor de acesso possui um **Gerenciador de Negociação (GN)** formado por dois módulos: *1)* o **Gerenciador de Políticas** que informa as políticas de acesso de acordo com a

posição geográfica do cliente; e *2*) o **AAA Local** que, apto a negociações, é responsável por autenticar, autorizar e tarifar o cliente. Porém, o *Broker* é o componente da arquitetura que disponibiliza informações de negociação de diferentes provedores e as centraliza em um **AAA Home**. Essas informações são utilizadas na negociação entre o cliente e provedor e entre provedores. Se um cliente não possui conta no provedor alvo, esse provedor irá consultar o *AAA Home* no *Broker* e obter as informações de conta do cliente fornecidas pelo seu provedor de origem. Além disso, o *Broker* possui uma **Base de Dados Centralizada (BDC)** das informações de contexto dos diversos clientes.

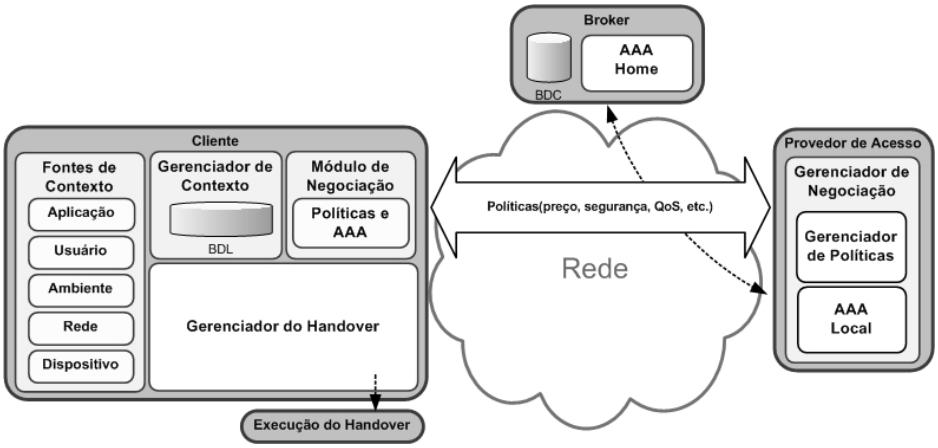

Figura 11 - Arquitetura SOHand - lado cliente, *Broker* e lado provedor.

5.2.2 As Fontes de Contexto (FC) e Gerenciador de Contexto (GC)

Normalmente, o *handover* é decidido com base na indicação da intensidade do sinal recebido (*Received Signal Strength Indication - RSSI*) (Pawar *et. al*, 2008) .Porém, realizar a decisão do próximo salto fazendo uso apenas do *RSSI* em ambientes NGN pode não ser suficiente. Esses ambientes serão compostos por diversos provedores de acesso (com políticas distintas) e existindo a necessidade de atender as preferências do usuário e os eventuais requisitos das aplicações. Em SOHand, um dos objetivos é atender tais exigências utilizando um conjunto de informações de contexto. As **FC** são apresentadas na Tabela 5, acompanhadas de uma breve descrição de como são obtidas e a motivação para recuperá-las.

O **GC** obtém as informações por meio dos métodos descritos na Tabela 1. Além disso, ele é responsável por: *a)* monitorar o movimento do usuário (utilizando um receptor GPS); *b)* as condições da rede em uso (qualidade do sinal, segurança e atividades de redes vizinhas) e do dispositivo (tempo de bateria e interfaces ativas); *c)* emparelhar as informações com as preferências do usuário (preço, segurança, economia de energia, etc.); e, se for necessário para

garantir a preferência do usuário, poderá *d)* responsável por iniciar o procedimento do *handover* ativando o módulo de **GH** (Figura 11). Todas as informações capturadas a partir **FC** são persistidas no dispositivo móvel no **BDL**.

Tabela 5 - Fontes de contexto e exemplos de informações que podem ser captadas.

Fontes de Contexto	Informações de Contexto relacionadas	Método de recuperação da informação	Motivação
Usuário	Localização Hora Data Preferências	A localização (coordenadas geográficas) do usuário, hora e data são obtidas por meio do receptor GPS. As preferências são configuradas pelo usuário, que ordena uma lista de provedores, e se deseja minizar ou maximizar segurança, preço e energia (sim/não), indicando quando o SOHand deve considerar essas preferências na seleção da rede. Todas as preferências serão fornecidas pelo usuário por meio de interface.	Localização é importante para o *handover* pró-ativo considerando as preferências do usuário e também para os LBS. Data e hora são informações que o provedor pode combinar com outras informações para personalizar os serviços, proporcionar QoS, etc. O usuário pode usar as preferências para criar perfis, por exemplo, de segurança para realizar uma operação financeira, escolhendo os provedores com maior nível de segurança, ou ainda, um perfil de economia de tarifas para selecionar o de menor custo.
Rede	IP/Prefixo Gateway DNS MAC Address do AP Modo de Operação Canal de operação SSID Segurança Qualidade do sinal Redes vizinhas	As informações de IP/Prefixo, Gateway e DNS são obtidas por meio de chamadas a API do Sistema Operacional (SO). As redes vizinhas e as demais informações são capturadas durante o processo de scan da interface (o protótipo utiliza o padrão IEEE 802.11g).	O IP/Prefixo, Gateway e DNS da rede atual podem ser armazenados e utilizados em uma conexão futura (na mesma rede) para pré-configurar a interface e eliminar o tempo de mecanismos de auto-configuração (e.g. DHCP) na camada de rede, assim reduzindo o tempo para o *handover*. As demais informações são aplicadas ao procedimento de seleção do próximo ponto de acesso.
Dispositivo	Interfaces de rede Tempo restante da bateria	Por meio de chamadas à API do SO são retornadas as informações do nível da bateria em mA e os nomes das interfaces que estão ativas.	As informações do nível da bateria e interfaces ativas podem ser associadas às preferências do usuário, por exemplo, um perfil de economia de energia, que como alternativa pode utilizar uma conexão via Bluetooth (IEEE 802.15).
Ambiente	Praça Universidade Restaurante Shopping, etc.	O ambiente pode ser recuperado por meio de algum serviço que mapeasse os locais e relacionasse com a posição geográfica obtida pelo GPS.	Relacionar o local com a disponibilidade de redes abre novas oportunidades de negócios. Pode-se inferir que o local não possue cobertura de um determinado provedor.
Aplicação	Navegador Web Player de vídeo E-mail (imap, pop) FTP, etc.	Informações da aplicação podem ser obtidas por meio de chamadas a API do SO.	Conhecer a aplicação que utiliza a rede é importante para proporcionar QoS, segurança e provionamente de recursos.

5.2.3. Procedimento de conexão

Existem, basicamente, quatro casos de uso do sistema: *a)* usuário parado desconectado querendo conectar-se; *b)* usuário parado conectado, que eventualmente pode realizar um *handover* por conveniência, por exemplo; *c)* usuário em movimento e desconectado por não ter uma rede disponível; e *d)* usuário em movimento, conectado. Esse último caso é o mais complexo, pois exige que para cada *handover* seja realizado o processo de descoberta, negociação e associação ao novo ponto de acesso.

Um serviço no lado provedor aguarda requisições de negociação independentemente da rede origem do cliente. O cliente conhece a forma de acessar os serviços de cada provedor e configura em ordem de preferência em seu perfil. Então, conecta-se ao provedor, informando a sua posição geográfica atual. O servidor verifica as políticas de acesso com base na localização do cliente e retorna as informações para negociação.

Contudo, o uso de uma nomenclatura específica por cada provedor para determinar seus parâmetros pode inviabilizar o procedimento de negociação. Dessa forma, um vocabulário comum e compartilhado entre as entidades, i.e., uma ontologia, mostra-se necessário.

Uma vez obtidas às informações dos provedores (preço, segurança, etc), elas são retornadas para o GH, que executa o algoritmo para decisão do *handover* para selecionar a melhor rede disponível de acordo com a preferência do usuário.

Depois de selecionado o novo provedor é iniciado o procedimento de AAA. O cliente passa as informações necessárias para o provedor (e.g., ID, rede de origem, método de autenticação suportado pelo dispositivo, plano de consumo, etc). Se o provedor não for capaz de resolver o procedimento AAA localmente, então ele deve consultar o AAA *Home* que centraliza as informações do usuário no *Broker*.

5.3. Validação dos conceitos por meio de *Mashup* e *Handovers* por Preferência.

A prova de conceito do *handover* baseado em contexto foi realizada por meio da implementação de dois cenários. No primeiro caso, a ideia foi criar um serviço que auxiliasse os usuários em futuras conexões na rede e também em pesquisas sobre a disponibilidade de redes sem fio em um determinado local. Para tanto, foi definido um conjunto de informações de contexto a ser capturado, armazenado e foi realizado o *mashup* com o Google Maps. O

serviço faz parte da implementação da ferramenta *Wireless Footprint* que está no âmbito do projeto SOHand.

O segundo cenário coleta um conjunto de informações das redes sem fio disponíveis e com base em configurações prévias, tenta encontrar uma melhor rede que atenda a preferência do usuário. Para tanto, foi utilizado o algoritmo de decisão AHP, fundamentado na decomposição do problema em uma hierarquia sendo que a avaliação dos elementos da hierarquia é feita em pares por meio de medidas estimadas de peso.

5.3.1. Cenário do *Mashup* com o Google Maps

Para demonstrar a possibilidade de provimento de serviços, um *mashup* combina a posição geográfica do usuário com o Google Maps, como mostra a Figura 12. Além do recurso visual (disponibilizado em um mapa), as redes disponíveis para acesso nas proximidades são exibidas com base nas informações das experiências de usuários anteriores.

O serviço foi implementado em um *Broker* acessível pela Internet, que disponibiliza na Web as informações coletadas durante a utilização das redes sem fio realizadas pelos usuários; esse serviço é chamado *Wireless Footprinting.* As informações obtidas são: posição geográfica, data/hora, tecnologia de acesso, MAC do ponto de acesso, canal de comunicação, qualidade do sinal e ruído.

No lado cliente, o módulo Gerenciador de Contexto (GC) foi implementado utilizando a linguagem Java. O dispositivo móvel utilizado foi um notebook, com SO Linux, e interface de rede Wi-Fi 802.11 b/g. As Fontes de Contexto, Rede e Dispositivo, foram capturadas a partir do diretório */proc* no Linux. Esse diretório é utilizado como interface para as estruturas de dados do Kernel que, nesse caso, contém variáveis que representam as fontes de contexto desejadas. A ferramenta é executada no dispositivo móvel em segundo plano (*backgroud*) acompanhando as mudanças de contexto. Essa funcionalidade foi implementada usando um dispositivo GPS que constantemente observa as coordenadas geográficas. O GPS foi manipulado por meio de um *daemon* chamado *gpsd* que acessa o dispositivo GPS.

Uma vez capturadas, as informações de contexto foram armazenadas em uma Base de Dados no *Broker* que implementa um SGBD PostGreSQL. A consulta às informações pode ser realizada por meio de coordenadas geográficas ou por uma seleção de um local listado.

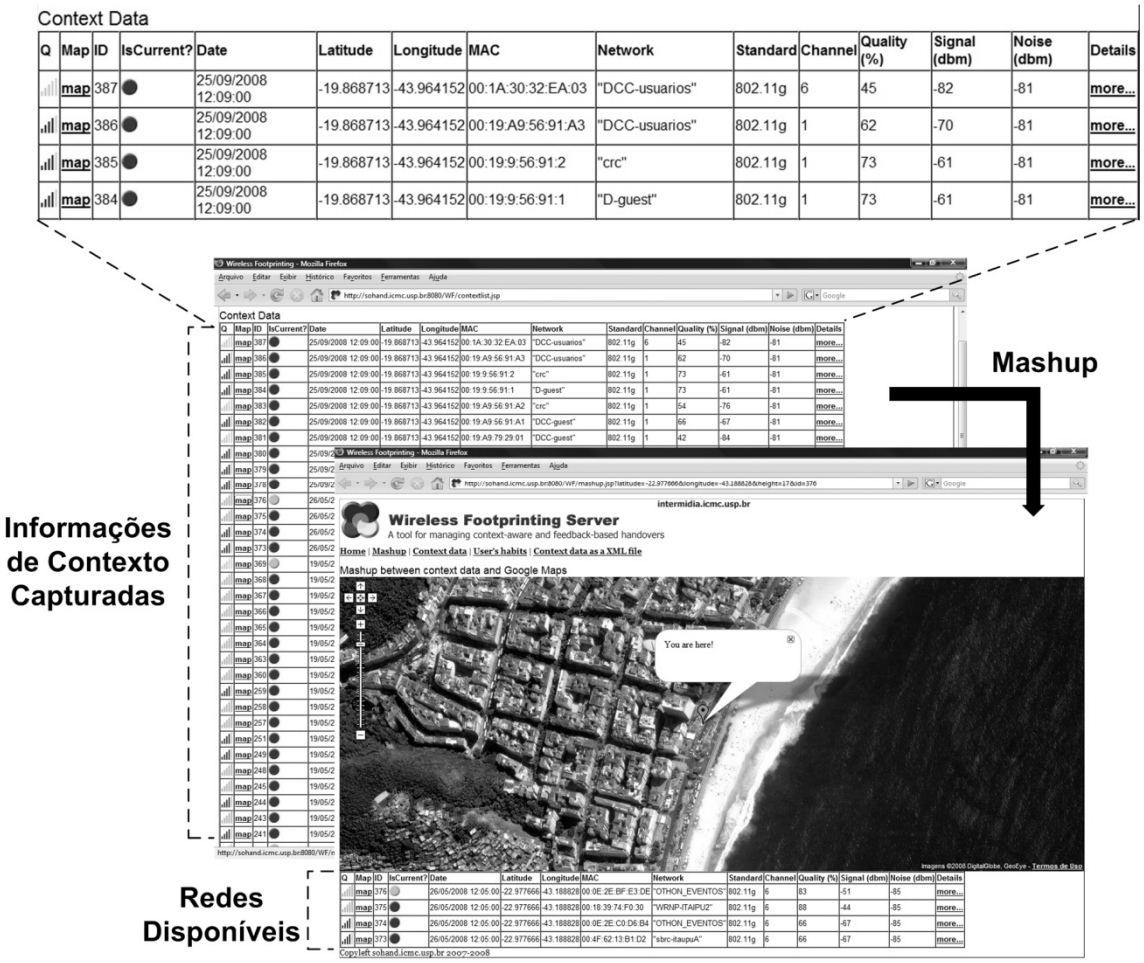

Figura 12 - *Wireless Footprinting*

5.3.2. Cenário das preferências do usuário

No cotidiano, alguns usuários podem estabelecer uma rotina, que pode ser também com relação à utilização das redes. Por exemplo, em casa, no trabalho e outros locais usualmente frequentados, o usuário, pela experiência da utilização, passa a ter suas redes preferenciais nesses locais. Contudo, a cada mudança de local é preciso, muitas vezes manualmente, realizar o reconhecimento das redes disponíveis e se conectar à rede desejada.

Neste sentido, foi planejado um gerenciador de conexões que utiliza informações contextuais da rede e do usuário para atender de forma automatizada a preferência do usuário. Por exemplo, um usuário poderia preferir uma rede que ofereça melhor segurança e QoS, tarifas mais baixas, ou determinadas tecnologias. Desta forma, o gerenciador analisa as características de cada rede e se conecta à que melhor atende as preferências do usuário.

Para validar este cenário foi implementado um protótipo do gerenciador que captura as informações de contexto das redes Wi-Fi e do usuário. A partir das informações obtidas, o

gerenciador executa a decisão do *handover* utilizando o algoritmo AHP adaptado para este cenário. O gerenciador foi avaliado em um *testbed* composto por três redes Wi-Fi.

A ideia é que os módulos desenvolvidos possam ser integrados na arquitetura SOHand. Os módulos são: **Gerenciador de Contexto** - captura e monitora as informações das redes sem fio disponíveis e das preferências do usuário; **Gerenciador de *Handover*** - executa o algoritmo AHP para seleção da nova rede e **Execução do *Handover*** - efetua troca, ou seja, faz a associação a outro ponto de acesso.

Neste trabalho, a captura de informações ficou limitada à infraestrutura da rede e às tecnologias (interfaces de rede) disponíveis nos dispositivos móveis. Assim, o gerenciador aceita três parâmetros de preferência: Rede Preferencial (SSID), Qualidade do Sinal e Segurança. É necessária uma pré-configuração do usuário, que consiste em informar o nome da rede de preferência e, se optar por redes protegidas (e.g. WEP, WPA, etc.), inserir chave de acesso.

Algoritmo para seleção da rede

O problema na seleção entre diferentes redes é avaliar um conjunto de informações contextuais e selecionar a rede desejada pelo usuário. Além disso, o número de redes e seus parâmetros podem variar com o local. Por isso, o problema foi dividido em duas etapas. A primeira seleciona um número fixo de redes elegíveis e na segunda aplica-se a ideia básica do algoritmo AHP às redes selecionadas. A descrição das variáveis e estruturas do algoritmo encontra-se na Tabela 6.

Tabela 6 - Descrição das variáveis e estruturas do algoritmo

Variáveis e Estruturas	Descrição
x	Número de redes elegíveis que se deseja utilizar.
n	O número de parâmetros.
C	Conjunto de parâmetros (e.g. c_1=SSID, c_2=Qualidade do sinal,..., c_n=Segurança).
L	Lista de todas as redes encontradas, cuja estrutura é uma matriz $L=[c_1, c_2, ..., c_n]$.
R	Lista de todas as redes elegíveis, possuí a mesma estrutura de L.
PR	Peso Relativo atribuído a cada parâmetro de contexto e cada rede.
v	Valor do parâmetro obtido pelo monitor de contexto.
E_{xn}	Importância de cada rede.
A	Matriz de comparação por pares.
W_i	Importância de cada parâmetro.
F_x	Pontuação final de cada rede x.

Os passos da primeira etapa seguindo as nomenclaturas da Tabela 6 são:

1. Obtenção de todas as redes disponíveis e ordenadas de forma decrescente pela qualidade de sinal e armazenmento no vetor L.

2. Realização de buscas pelos parâmetros de rede configurados pelo usuário na lista *L*, da seguinte forma:
    a. Repita até que número de redes em *L* <= *x*.
    b. Se parâmetro for encontrado, insira em *R*. Senão, passe para o próximo parâmetro.

Se parâmetro = *n*, então insira em *R* as redes de maior qualidade de sinal.

Após selecionadas as redes elegíveis, utilizou-se algoritmo AHP para seleção da rede com as seguintes adaptações para este cenário.

a) Seguindo a proposta de Pawar (Pawar, et al, 2008), os objetivos para atender as preferências do usuário têm valores fixos, cuja soma dos pesos $0<PR\leq1$. Um mapeamento dos pesos relacionados à preferência pode ser observado na Tabela 7.

Tabela 7 - Relação entre pesos e a preferência

Pesos	Tipo de Preferência
0	Nenhuma
0.33	Baixa
0.5	Média
1	Alta

b) Os parâmetros adotados são diferentes dos parâmetros utilizados nos trabalhos relacionados. Alguns deles não são possíveis de normalizar nos Pesos Relativos (*PR*) de 1 a 9, como realizado, em Ahmed (Ahmed, et al, 2006), para parâmetros como *vazão*, *jitter*, etc. Por exemplo, com relação a segurança, nesse caso, a rede pode ou não oferecer segurança, não tendo valores intermediários de *PR*. A solução foi tornar os *PR* fixos para cada parâmetro *c* das Redes *L*, sendo 9 para o melhor caso, 5 para o caso médio e 1 para o pior caso.

Por último, obtidos os valores dos objetivos da preferência e a pontuação relativa de cada rede, o *ranking* das redes é calculado por meio da soma do produto do objetivo pela pontuação relativa da rede seguindo o modelo AHP e acrescidos dez por cento a cada preferência que a rede atender.

Implementação

Os módulos do protótipo do gerenciador foram implementados na linguagem Java. O Gerenciador de Contexto foi importado da ferramenta WF, porém a funcionalidade do GPS não foi aproveitada devido à limitação do funcionamento do dispositivo em ambientes abertos. Com isso, o contexto atual é periodicamente verificado e comparado com o estado imediatamente anterior. Uma vez verificada a mudança de contexto, as informações são

passadas para o gerenciador de *handover*. Esse último executa o algoritmo de seleção do novo ponto de acesso com base nas preferências do usuário. Se a rede alvo for diferente da atual, então são enviados os parâmetros necessários ao módulo de execução para troca da rede, como ilustrado no diagrama da Figura 13.

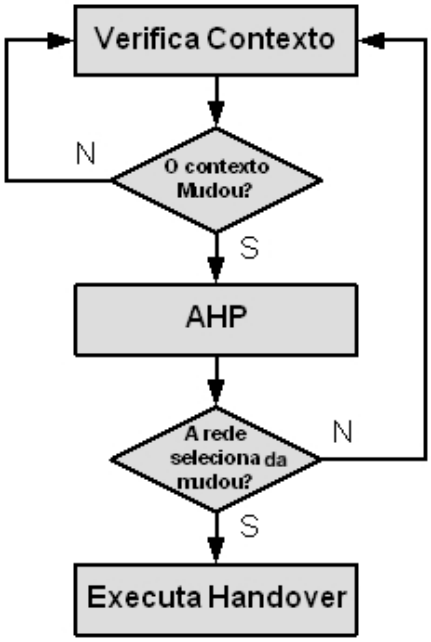

Figura 13 - Fluxograma do gerenciador de conexões

O módulo do Gerenciador do *Handover* executa o algoritmo de seleção descrito na Seção 5.3.2.1 para $x = 3$ (três redes) e os pesos são atribuídos conforme o valor v obtido e os seguintes critérios:

- SSID: Se for preferencial = 9, segundo com melhor qualidade do sinal = 5 e a última = 1;
- Qualidade do Sinal: A rede com melhor sinal = 9, a segunda com melhor =5 e a última = 1;
- Segurança: A rede que atender a preferência = 9, outros = 1;

Exemplo: Funcionamento do Gerenciador

Um exemplo ilustra o funcionamento do gerenciador,iniciando com pré-configuração das preferências do usuário para cada objetivo. As redes encontradas são descritas na Tabela 8. Após a primeira etapa são eleitas as três primeiras redes da Tabela 8. O algoritmo de seleção é executado e o ranking das redes é apresentado na Equação 5.1.

Pré-Configurações dos objetivos:

- Rede (SSID): 0.5 (Média) e SSID: AP1
- Qualidade do Sinal: 0.0 (Nenhuma)
- Segurança: 0.5 (Média) e WEP

A configuração do usuário expressa uma preferência igual entre a rede AP1 e uma rede com segurança, e nenhum interesse na qualidade do sinal. A melhor situação é encontrar a rede AP1 com segurança e a pior situação é não encontrar a rede AP1 e nenhuma rede segura. Outras situações intermediárias são encontrar a rede AP1 sem segurança ou não encontrar a rede AP1, mas outra com segurança. Nesses casos, a rede selecionada será aquela que possui um dos objetivos atendido.

Na Tabela 8 são exibidas quatro redes hipotéticas encontradas por meio do gerenciador de contexto que realiza uma varredura nos canais do IEEE 802.11. A lista é armazenada no vetor *L*.

Tabela 8 - Redes encontradas em determinado momento.

SSID	Qualidade do Sinal (%)	Segurança
AP1	100.0	Aberta
AP2	99.0	WEP
AP3	89.0	Aberta
AP4	78.0	WEP

Primeira etapa:

As redes, de acordo com a primeira etapa, são: AP1, AP2 e AP3.

- O AP1 foi selecionado porque é preferencial do usuário.
- O AP2 foi selecionado porque atende a preferência de segurança e está com melhor qualidade do sinal com relação a AP4.
- O AP3 foi selecionado por estar com melhor qualidade do sinal que o AP4.

Segunda etapa:

Na Tabela 9 estão as pontuações atribuídas aos parâmetros de cada rede.

Tabela 9 - Pesos atribuídos aos parâmetros de cada rede.

	SSID	Qualidade do Sinal	Segurança
AP1	9	9	1
AP2	5	5	9
AP3	1	1	1

A rede AP1 recebeu peso 9 no *SSID* porque é a configurada pelo usuário, peso 9 também na qualidade do sinal por ter o melhor sinal. A rede AP2 recebeu 5 no *SSID* e *Qualidade do Sinal*, por ter a segunda melhor qualidade de sinal e peso 9 na *Segurança* por ser a única rede segura. Como a rede AP3 não atende nenhuma das configurações do usuário, recebeu o menor peso em todos os parâmetros.

Para todos os parâmetros é realizado o cálculo da matriz A, normalizado e extraída a média de cada rede:

a) Para SSID e Qualidade do Sinal. Como os valores da pontuação são iguais, a Matriz A (eq.5.1) é a mesma para os dois parâmetros.

$$A=\begin{bmatrix} 1 & 9/5 & 9 \\ 5/9 & 1 & 5 \\ 1/9 & 1/5 & 1 \end{bmatrix} \Rightarrow A_{norm}=\begin{bmatrix} 0.6 & 0.6 & 0.6 \\ 0.3\overline{3} & 0.3\overline{3} & 0.3\overline{3} \\ 0.0\overline{6} & 0.0\overline{6} & 0.0\overline{6} \end{bmatrix} \Rightarrow A_{final}=\begin{bmatrix} 0.6 \\ 0.3\overline{3} \\ 0.0\overline{6} \end{bmatrix} \qquad eq.(5.1)$$

b) O cálculo da Matriz A é ilustrado na eq.5.2.

$$A=\begin{bmatrix} 1 & 5/9 & 1 \\ 9/5 & 1 & 9 \\ 1 & 1/9 & 1 \end{bmatrix} \Rightarrow A_{norm}=\begin{bmatrix} 0.263158 & 0.3\overline{3} & 0.\overline{09} \\ 0.473684 & 0.6 & 0.\overline{81} \\ 0.263158 & 0.0\overline{6} & 0.\overline{09} \end{bmatrix} \Rightarrow A_{final}=\begin{bmatrix} 0.229133 \\ 0.630622 \\ 0.140245 \end{bmatrix} \qquad eq.(5.2)$$

Depois do cálculo das Matrizes A para cada rede, o *ranking* das redes é obtido conforme eq. 5.3. Conforme os valores finais, a rede AP2 foi escolhida.

$$\begin{aligned} F_{AP1} &= 0.5\times 0.6\ \times 1.1 + 0\times 0.6\ \times 1\ + 0.5\times 0.229133\times 1\ \ = 0.444567 \\ F_{AP2} &= 0.5\times 0.3\overline{3}\times 1\ \ + 0\times 0.3\overline{3}\times 1\ + 0.5\times 0.630622\times 1.1 = 0.513509 \quad eq.(5.3) \\ F_{AP3} &= 0.5\times 0.0\overline{6}\times 1\ \ + 0\times 0.0\overline{6}\times 1 + 0.5\times 0.140245\times 1\ \ = 0.103456 \end{aligned}$$

Analisando o resultado, nesse caso, como a preferência é igual para SSID e Segurança (valores 0.5 para cada parâmetro) é possível inferir que a decisão mais adequada é a rede AP2 que oferece segurança.

Teste do gerenciador

Para a avaliação do gerenciador a ideia foi ponderar empiricamente a coerência da escolha da nova rede. Nesse sentido, o gerenciador de conexões foi avaliado variando-se as configurações, cujo objetivo foi observar se a decisão do algoritmo estava em conformidade

com a preferência definida pelo usuário. Para tanto, foram realizados sete testes diferentes cobrindo todas as possibilidades de configuração.

Na Tabela 10 estão numeradas por teste as possíveis preferências do usuário; para cada teste, foi executado um experimento. A Tabela 11 corresponde aos valores de configuração que o usuário faz no gerenciador de conexões. Por exemplo, no Teste 1 (coluna 2) o usuário configurou o peso do objetivo **Rede** com valor 1, **Qualidade do Sinal** com valor 0 e **Segurança** com valor 0. Como rede preferencial o **SSID** AP1 e o **Tipo de Segurança** Aberta.

Tabela 10 - Número do teste e tipo de configuração.

Teste	Descrição da preferência
1	Preferência por uma rede (SSID)
2	Preferência por melhor qualidade do sinal
3	Preferência por determinado tipo do segurança (aberto ou WEP)
4	Preferência por uma rede e qualidade de sinal
5	Preferência por uma rede e determinado tipo de segurança
6	Preferência por qualidade do sinal e determina tipo de segurança
7	Preferência considerando rede, qualidade do sinal e segurança

Tabela 11 - Valores configurados na plataforma.

Configuração	Teste 1	Teste 2	Teste 3	Teste 4	Teste 5	Teste 6	Teste 7
Rede	1	0	0	0.5	0.5	0	0.33
Qualidade Sinal	0	1	0	0.5	0	0.5	0.33
Segurança	0	0	1	0	0.5	0.5	0.33
SSID	AP1	AP1	AP1	AP3	AP2	AP3	AP2
Tipo de Segurança	Aberta	Aberta	WEP	Aberta	WEP	Aberta	WEP

Os testes foram executados no *testbed* NGN descrito no Capítulo 4. Contudo, as configurações da potência do sinal e tipo de segurança dos APs foram alteradas para os testes. O AP DIR-635 D-Link permite três modos da operação da potência do sinal: Alto, Médio e Baixo; e algumas configurações de segurança (chaves criptográficas): Nenhuma (Aberta), WEP 64bits, WEP 128bits, WPA, e WPA2. Desta forma, tentou-se elaborar um cenário que melhor atendesse os sete testes, pois não seria possível abordar exaustivamente todos os cenários. As configurações dos APs ficaram conforme a Tabela 12.

Tabela 12 - Configurações dos APs no cenário

	AP 1	AP 2	AP 3
Potência do Sinal	Baixa	Alta	Alta
Tipo de Segurança	Aberta	WEP	Aberta

Uma vez fixado o cenário inferiu-se, comparando a configuração de cada teste (Tabela 11) com o cenário (Tabela 12), a rede que atenderia a preferência do usuário. As redes inferidas são apresentadas na Tabela 13. As justificativas para as escolhas são:

1. Teste 1 – A configuração do usuário é para o SSID AP1, como no cenário existe a rede AP1 e a preferência é somente para rede, a escolha inferida é o AP 1.
2. Teste 2 – O usuário procura a rede com melhor qualidade de sinal, entretanto o cenário traz duas redes com potência do sinal alta (AP 2 e AP 3); neste caso, como a preferência de segurança é Aberta, a escolha inferida é o AP 3.
3. Teste 3 – No cenário, somente o AP 2 possui segurança, portanto, a escolha inferida é o AP2.
4. Teste 4 – Como o usuário se importa com a qualidade do sinal e a rede, e a configuração está para SSID AP3, comparando com o cenário que possui AP3 e potência do sinal alta, infere-se que a escolha é o AP 3.
5. Teste 5 – A configuração do usuário é para SSID AP2 e segurança WEP, no cenário a que atende essas preferências é o AP 2.
6. Teste 6 – No cenário os AP 2 e AP 3 possuem alta potência do sinal, mas a preferência é para tipo de segurança Aberta; assim, a escolha inferida é AP3.
7. Teste 7 – O último teste considera a preferência para os três objetivos. Neste caso, o AP 2 é o que atende a maioria, conforme a configuração, por isso, a rede inferida é AP2.

Tabela 13 - Configuração dos AP´s para cada teste

	Teste 1	Teste 2	Teste 3	Teste 4	Teste 5	Teste 6	Teste 7
Rede Inferida	AP1	AP3	AP2	AP3	AP2	AP3	AP2

Para cada experimento foram executados 40 *handovers.* A contagem dos acertos e erros foi por meio de registros gerados durante a execução do experimento. As informações armazenadas foram o contexto da rede, a rede de origem e a rede de destino. Após cada *handover* realizado pelo gerenciador para a rede alvo, outro era realizado para uma rede

aleatória diferente da rede inferida como preferencial. Desta maneira, garantiu-se que na próxima execução a rede de preferência estaria disponível. Os resultados obtidos estão sumariados na Tabela 14 em percentual de acertos e erros. Em cada teste foi contabilizado se a rede de destino decidida foi a rede de preferência inferida conforme Tabela 13.

Tabela 14 - Resultados de cada Teste

	Teste 1	**Teste 2**	**Teste 3**	**Teste 4**	**Teste 5**	**Teste 6**	**Teste 7**
Acertos	100%	40%	100%	42,5%	100%	50%	85 %
Erros	0%	60%	0%	57,5%	0%	50%	15%

É possível observar que nos Testes 2, 4 e 6 o desempenho foi insatisfatório, com acertos iguais ou inferiores a 50%. Ao investigar as causas do resultado, notou-se que os testes envolviam a qualidade do sinal. Analisando os valores obtidos chegou-se a duas conclusões:

I. Apesar dos esforços em tentar manter o ambiente controlado, o controle da potência do sinal dos APs, na prática, em ambientes fechados (e.g. no laboratório) com APs próximos, da ordem de metros, o controle de potência não foi eficiente. Assim, no cenário, o AP 1 que era para ter o menor valor de sinal não ocorreu em todas as execuções, influenciado, também, por interferências de outras fontes de rádio, uma vez que os valores obtidos são a relação sinal/ruído.

II. Oscilações da qualidade do sinal, mesmo com o dispositivo parado, mostraram-se inerentes às redes Wi-Fi. Como não foi realizada a normalização dos pontos (1 a 9) para os parâmetros da rede, em geral, o algoritmo apresentou um comportamento muito sensível às variações da qualidade do sinal. Contudo, o algoritmo escolhe a rede alvo corretamente, mas poderia ser tolerante às pequenas mudanças e tomar uma decisão mais "inteligente". Pois, em situações reais, o desempenho pode ser pior se consideramos os problemas envolvidos no procedimento de *handover*.

Apesar dos resultados apresentados nos testes 2, 4 e 6 terem sido prejudicados pelo difícil controle do cenário de experimentação, o gerenciador obteve bons resultados com relação às informações pouco dinâmicas. Portanto, o protótipo do gerenciador de conexões demonstrou a possibilidade de contexto para serviços relacionados à escolha do ponto de acesso, necessitando apenas de um ajuste no uso da qualidade do sinal.

5.4. Formalização das informações contextuais.

Nesta Seção são formalizadas as informações contextuais utilizadas na implementação. A finalidade é agregar a este trabalho, o conhecimento especializado representado por meio de ontologias.

Partindo-se da ontologia definida no escopo DOHand (Domínio de Ontologias para *Handovers*) (Vanni, et.al., 2006) e considerando um domínio Fontes de Contexto, foi especializada a classe Rede. A ideia é que essa classe, agora especializada com base na implementação, seja incorporada à ontologia definida em DOHand, a qual já possui os relacionamentos de classes desse domínio.

A classe Rede foi, então, formalizada utilizando a linguagem OWL DL (OWL, 2009) e modelada pela ferramenta *Protégé* (Protégé, 2009). Essa ferramenta permite gerar o código OWL de forma automática, como mostrado a seguir:

```
1 <?xml version="1.0"?>
2 <rdf:RDF
3    xmlns:xsp="http://www.owl-ontologies.com/2005/08/07/xsp.owl#"
4    xmlns="http://www.owl-ontologies.com/Ontology1245142736.owl#"
5    xmlns:swrlb="http://www.w3.org/2003/11/swrlb#"
6    xmlns:swrl="http://www.w3.org/2003/11/swrl#"
7    xmlns:protege="http://protege.stanford.edu/plugins/owl/protege#"
8    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
9    xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
10    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
11    xmlns:owl="http://www.w3.org/2002/07/owl#"
12  xml:base="http://www.owl-ontologies.com/Ontology1245142736.owl">
13  <owl:Ontology rdf:about=""/>
14  <owl:Class rdf:ID="Rede"/>
15  <owl:ObjectProperty rdf:ID="Seguranca"/>
17  <owl:ObjectProperty rdf:ID="Qualidade_do_sinal"/>
18  <owl:ObjectProperty rdf:ID="SSID"/>
19 </rdf:RDF>
```

As linhas 1 e 2 referem-se ao espaço de nomes XML e RDF. As declarações das linhas 3 a 12, com elementos de prefixos *owl, rdf, rdfs, xsd,* etc., são definições pertencentes aos vocabulários das linguagens OWL, RDF, RDFS e XML *Schemme*. A classe Rede é definida pelo construtor `owl:Class` (linha 14) e seus objetos por `owl:ObjectProperty` (linhas 15 a 18).

A principal contribuição desse formalismo é que a semântica embutida em cada termo, o qual pode possuir diferentes significados, faz com que sua interpretação seja relativa à circunstância em que está sendo empregado. Por exemplo, o temo Segurança poderia estar se referindo a vida do usuário, entretanto, neste caso, como o conceito é definido pela classe Rede, o termo refere-se à Segurança em Rede de Computadores.

5.5. Considerações finais

Este Capítulo abordou os cenários utilizados para validar o trabalho. O *mashup* descrito é realizado por meio da ferramenta *Wireless Footprinting*, a qual é parte de outro trabalho em desenvolvimento. A captura e a agregação de contexto no *mashup* implementadas pela ferramenta, mostram que é possível prover serviço ciente de contexto em NGN.

Neste Capítulo também foi apresentada a descrição de um Gerenciador de Conexões que utiliza informações contextuais para selecionar o ponto de acesso de acordo com preferência do usuário. Essa abordagem tem por finalidade provar conceitualmente o uso de contexto em NGN. Além disso, foi avaliado o algoritmo AHP em um cenário experimental não simulado, o qual se mostrou sensível a pequenas variações da qualidade do sinal. O problema poderia ser melhorado por meio de uma função para linearizar os pesos atribuídos ao objetivo *qualidade do sinal*.

Por último, é realizada uma iniciativa de formalização das informações contextuais utilizadas na implementação com a finalidade de colaborar com a ontologia DOHand em desenvolvimento.

6. Avaliação de *Handovers* com Contexto

6.1. Considerações iniciais

Neste Capítulo é apresentada a última etapa do trabalho, a avaliação dos impactos que são causados na rede quando se usa contexto, bem como a avaliação do custo/benefício da troca de rede. Nos dois casos são propostos modelos para estimar o impacto e o custo/benefício, ambos deduzidos a partir dos resultados obtidos nos experimentos.

Na Seção 6.2. é realizada a avaliação dos impactos sobre a tecnologia de rede Wi-Fi. Na Seção 6.3 é descrito o problema do custo/benefício com relação à vazão da rede e uma análise utilizando o MIPv6.

6.2. Impacto da captura de contexto

O objetivo do experimento foi avaliar o impacto na vazão provocado pela captura de informações contextuais da rede. O impacto pode variar de acordo com a tecnologia de rede utilizada. Desta forma, a ideia foi criar um modelo generalizado para estimar o custo da captura de contexto. Para isso, foi utilizado o *testbed* descrito no Capítulo 4 e analisado o impacto da captura sobre a tecnologia Wi-Fi. Essa, para descoberta das redes disponíveis, realiza uma varredura sobre os 11 canais de operação. Durante esse procedimento ocorre uma queda na transmissão de dados.

Após a varredura é executado um *handover* na Camada de Enlace (nível 2), ou seja, com IP fixo no dispositivo móvel. A vazão foi aferida utilizando o iPerf com o envio de fluxo TCP durante um período de 35s. No gráfico da Figura 14, é comparada a vazão com a varredura, e sem a varredura, ambos executam o *handover* no tempo 18s. Os valores foram obtidos a partir da média de 250 execuções de *handover*.

No tempo de 15s é iniciado o procedimento de varredura para a captura das redes sem fio que estão ativas ao redor do dispositivo móvel. Até o tempo de 17s a média da vazão diminui de 20.16 Mbps para 12.18 Mbps, uma perda de 39,58%. Prosseguindo, no tempo de 18s é executado o *handover*, cuja latência média foi de 12.824ms, sendo significativamente menor que a latência na camada IP. É possível perceber, pelo gráfico, que a varredura não tem influência na latência do *handover*.

Depois do *handover*, foi observada a influência do controle de congestionamento do protocolo TCP sobre a vazão. Em linhas gerais, o problema ocorre pela perda consecutiva de pacotes de confirmação – os *AKCs*. Essa perda é "entendida" pelo TCP como congestionamento na rede, o qual reage reduzindo a janela de transmissão pela metade até a conexão tornar-se estável. O aumento da janela de transmissão, por outro lado, é aditivo e é possível observar, na Figura 14, um retardo do período de *slow start* para a recuperação da vazão máxima da rede.

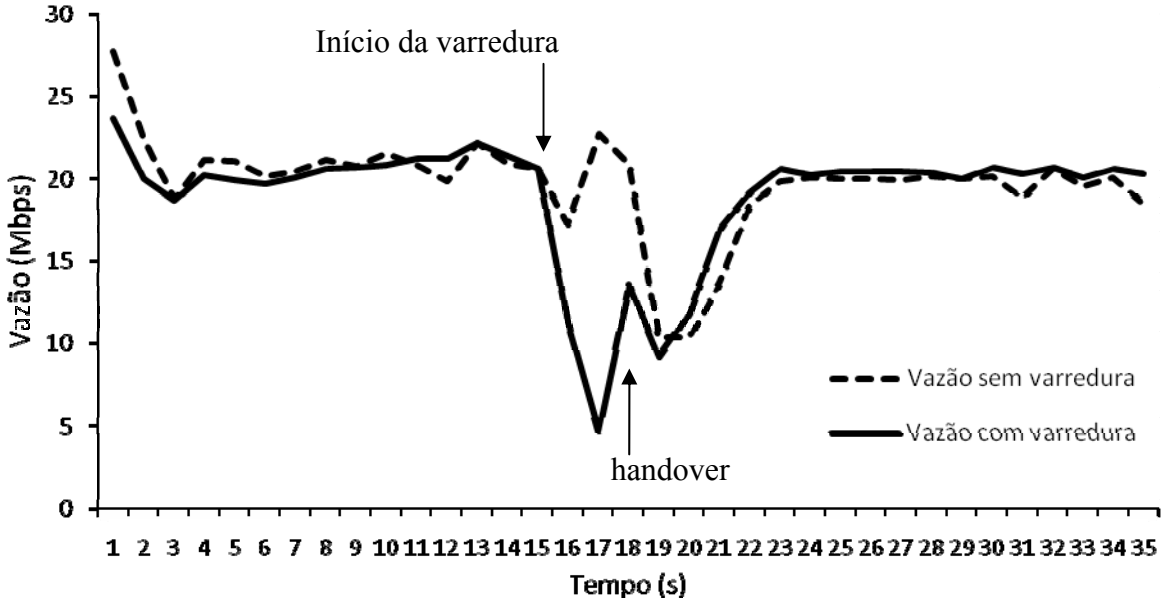

Figura 14 - Impacto do processo de captura de informações contextuais de rede.

Por meio dos dados obtidos é proposto o seguinte modelo para estimar o impacto da captura de informações contextuais:

$$\alpha = \frac{\overline{X}r \cdot t - n \cdot (\overline{X}r - \overline{X}s) \cdot \Delta ts}{\overline{X}r \cdot t}$$

Onde:

α : desempenho da rede
t : tempo total da transmissão em segundos
n : número de vezes que se captura o contexto durante t
$\overline{X}r$: média da vazão nominal da rede em Mbps
$\overline{X}s$: média da vazão durante a captura de contexto em Mbps
Δts : intervalo de tempo em segundos que se gasta para a captura de contexto

Utilizando os valores obtidos no experimento: t= 35s; n=1; $\overline{X}r$ = 20.16Mbps; $\overline{X}s$ = 12.18Mbps e Δts = 3s.

$$\alpha = \frac{20.16 * 35 - 1 * (20.16 - 12.18) * 3}{20.16 * 35} = 0.9660$$

Portanto, para n=1, uma captura de contexto a cada 35s, representa um impacto na rede de aproximadamente 4%. Se n=7, ou seja, uma captura a cada 5s, o impacto sobe para 23.75%.

6.3. Análise do Custo/Benefício do *handover*

A avaliação da relação custo/benefício do *handover* pode ser realizada sob diversas perspectivas. Por exemplo, a partir da segurança, da qualidade do sinal, da aplicação, da tarifa, etc. Contudo, essa avaliação analisa o desempenho da vazão e da latência.

Algumas propostas como em Balasubramaniam (Balasubramaniam e Indulska, 2004), Ahmed (Ahmed et al, 2006) e Wei (Wei et al, 2006) se baseiam principalmente na informação de vazão da rede para prover QoS, mas não analisam o impacto da latência do *handover* no custo/benefício da transição. Isso significa que, mesmo a rede destino tendo maior vazão, ela pode ter um custo/benefício ruim. Assim, nesse caso, não é atrativo fazer a mudança de rede se à quantidade de dados a ser transmitida for baixa e a latência do *handover* for alta. Por essa razão, para um bom custo/benefício, estabeleceu-se o seguinte critério:

$$T_A(d, \bar{x}_a) < T_H(d, \bar{x}_h) \quad eq.(6.1)$$

Sendo:

$$T_A(d, \bar{x}_a) = l + d \diagup \bar{x}_a \quad eq.(6.2)$$

$$T_H(d, \bar{x}_h) = d \diagup \bar{x}_h \quad eq.(6.3)$$

Onde:

d : quantidade de dados a ser transmitida em Mbits
l : latência do *handover* em segundos
$\bar{x}_a$: vazão média da rede alvo em Mbps
$\bar{x}_h$: vazão média da rede *home* em Mbps
T_A : tempo para a rede alvo transmitir d Mbits de dados
T_H : tempo para a rede home transmitir d Mbits de dados

Dados os critérios para um bom custo/benefício, avaliou-se uma situação que poderá ser típica em NGN: um usuário acessando uma rede *Visitada* (em *roaming*), num determinado

momento, e a rede *Home* torna-se disponível. Considerando a latência do *handover* com MIPv6 é importante analisar a relação custo/beneficio da troca para rede *Home*. Para tanto, foi utilizado o *testbed* adaptado para os dois AP´s. Além disso, para medir o *overhead* do roteamento triangular, o nó CN e o nó MN não foram preparados para utilizar o mecanismo de otimização de rotas.

Um *script* que periodicamente trocava entre a rede *Home* e a rede *Visitada* (alvo) foi utilizado para automatizar o experimento. A vazão foi obtida por meio da ferramenta iPerf, com transmissões de fluxo TCP durante 70s cada execução. A vazão média calculada a partir de 140 execuções é apresentada graficamente na Figura 15.

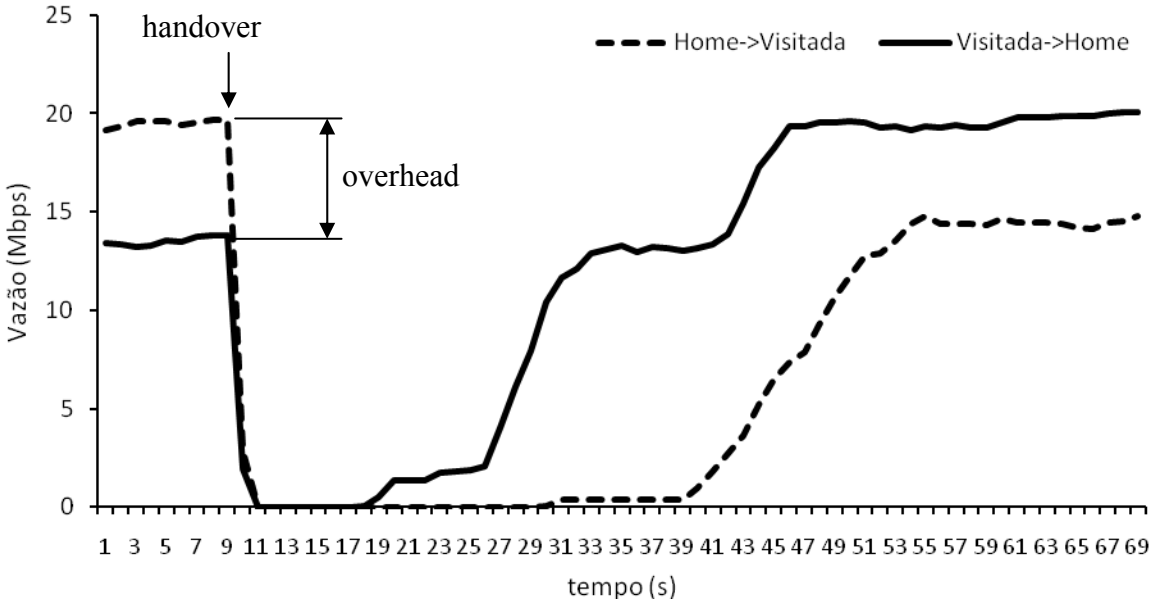

Figura 15 - *Handover* com MIPv6

Analisando os resultados, constata-se que o *overhead* do roteamento triangular do MIPv6 é de aproximadamente 30% para uma vazão média de 20 Mbps em uma rede Wi-Fi. Essa diferença pode ser visualizada no gráfico nos intervalos de 1 a 9s e de 55 a 68s. Outra constatação foi a latência do *handover* para cada caso: *i)* saindo da rede *Home* para a *Visitada* ser de no mínimo 18s, e no caso *ii)* a partir da rede *Visitada* para a *Home* ser de no mínimo 6s - uma diferença 3 vezes menor.

A justificativa para a diferença é que os três principais procedimentos responsáveis pela latência do MIPv6 (atribuição do IP, redirecionamento do *gateway* para túnel e *BU Home Agent*) não são realizados no caso *ii)*, pois o dispositivo móvel já possui o endereçamento da rede *Home,* o BU é e o acesso ao local e o *gateway* não é feito por tunelamento.

Para finalizar, o custo/benefício foi analisado sobre o *handover* partindo da rede *Visitada* para a rede *Home,* ou seja, saindo de uma rede que oferece menor vazão para uma com maior vazão. Os valores obtidos pelo experimento foram: $\bar{x}_h$ = 13.89 Mbps; $\bar{x}_a$ = 19.60 Mbps e l = 10.21s (latência média). Resolvendo a desigualdade da eq.6.1 temos:

$$T_A(d,\bar{x}_a) < T_H(d,\bar{x}_h) \Rightarrow l + d/\bar{x}_a < d/\bar{x}_h \Rightarrow d > \frac{l * \bar{x}_h}{1 - \bar{x}_h/\bar{x}_a} \therefore d > \frac{10.21 * 13.89}{1 - \frac{13.89}{19.60}} = 486.797 Mbits$$

Portanto, para o custo/benefício ser bom, o usuário teria que transmitir pelo menos 486.797 Mbits. Em outras palavras, após o *handover*, o usuário deve permanecer conectado na rede *Home* no mínimo 24.8366s utilizando a vazão máxima da rede. Como as redes Wi-Fi possuem altas taxas de transmissão se comparado a rede de telefonia celular, o tempo de permanência é baixo. Por outro lado, mas se consideramos vazões da ordem de Kbps e/ou altas latências, esse tempo pode se tornar expressivo.

6.4. Considerações finais

Neste capítulo se propôs dois modelos, o primeiro para estimar o impacto da captura de contexto e o segundo para ponderar o custo/benefício do *handover* com relação à vazão. Ambos utilizam a média, por isso se tem valores estimados. Para os valores serem exatos, há a necessidade de modelar uma função que descreva o comportamento da vazão, mas esta abordagem ficou fora do escopo do trabalho.

Além disso, os experimentos revelaram que *a)* o procedimento de varredura não influencia no *handover*; *b)* a latência do *handover* na Camada de Enlace é baixa se comparada à Camada de Rede, *c)* o overhead do MIPv6 é expressivo no desempenho e, nesse caso, um parâmetro da preferência do usuário poderia ser, possuir ou não o suporte à otimização de rotas.

7. Conclusões

A diversidade de tecnologias de rede prevista em redes NGN traz novos desafios tanto do ponto de vista do Gerenciamento adequado de *Handovers* quanto do provimento de acesso e de serviços. Busca-se, na prática, maximizar o tempo de conexão sobre as melhores redes encontradas durante o percurso do usuário móvel. Mas, também, serviços podem ser especializados e disponibilizados como meios atrativos de adesão de novos nós e usuários nas redes presentes no percurso.

Nesse sentido, a principal finalidade deste trabalho foi explorar as informações contextuais em NGN e, a partir delas, promover novas possibilidades de serviços. Para tanto, dois cenários foram projetados com o objetivo de melhorar a experiência do usuário: um *Mashup* que combina aplicações Web e informações de contexto; e um Gerenciador de Conexões baseado em preferências do usuário para auxiliar a decisão de *handover*.

O Gerenciamento de Mobilidade e de *Handovers* em ambientes de acesso heterogêneo demandam soluções mais robustas, como a arquitetura SOHand. Por isso, uma das etapas deste trabalho foi auxiliar na especificação dos módulos dessa arquitetura para atender as necessidades e requisitos das redes NGN. Uma abordagem ciente de contexto e a iniciativa de padronização por meio de ontologia são seus diferenciais perante as outras propostas.

Realizar experimentos não simulados de rede em cenários complexos como NGN é uma tarefa trabalhosa e um tanto quanto atípica. Encontram-se, em maioria na literatura, ambientes simulados que são utilizados para validação de novos protocolos e soluções algorítmicas específicas. Se por um lado a simulação permite aplicar soluções a diversos cenários, inclusive mais complexos, por outro ela pode fugir do realismo desejado em virtude do fator da aleatoriedade dos parâmetros não previstos no plano inicial de simulação e que são comuns em ambientes experimentais.

Dessa forma, neste trabalho optou-se pela realização de experimentos reais em um *testbed* em contrapartida às soluções em ambientes simulados. Por outro lado, interferências externas dificultam o controle dos ambientes experimentais, como por exemplo, a configuração adequada da rede e dos computadores. Nesse sentido, a identificação e a correção de problemas no ambiente, bem como a coleta dos dados experimentais em quantidades estatisticamente confiáveis, podem representar um entrave no tempo de realização do experimento inicialmente previsto. Entretanto, decidiu-se superar as

dificuldades e implantar um *testbed* NGN com o protocolo de gerenciamento de mobilidade MIPv6 para experimentação das plataformas desenvolvidas.

Uma visão abrangente das fontes de contexto que podem ser utilizados em NGN despertaram novas possibilidades de serviços, além da tradicional prestação de QoS. A coleta e o armazenamento de contexto mostraram, por exemplo, a possibilidade de serviços *Web* como o *mashup*. Outra aplicação foi com o Gerenciador de Conexões aplicando as informações de rede e do usuário.

A razão pela qual foram implementados apenas dois cenários para validar a proposta é o tempo demandado na prática de implantação de ambiente experimental, como mencionado anteriormente. Mesmo com apenas dois protótipos, diversos problemas tiveram de ser tratados, o principal deles, no Gerenciador de Conexões, foi como decidir por uma rede alvo com base em várias informações e visando atender as preferências do usuário. Para tanto, foi adaptado o algoritmo AHP que, por meio de cálculos hierárquicos e objetivos predefinidos, decide qual será a rede destino.

Na última etapa, foram realizadas avaliações do impacto da captura de informações de contexto e da relação custo/benefício do *handover*. Com a avaliação percebe-se que o desempenho da rede Wi-Fi é prejudicado com a captura das informações e que um *handover*, baseado em QoS da rede, pode não ter boa relação custo/benefício dependendo da quantidade de dados a ser transmitida na rede alvo e do tempo de da troca, i.e., a latência de *handover*.

Os principais resultados e contribuições deste trabalho, bem como os trabalhos futuros são sumarizados nas Seções seguintes.

7.1. Principais resultados e contribuições

Os principais resultados e contribuições deste trabalho estão relacionados a seguir.

1. Implantação do *Testbed* NGN – Na literatura existem poucos trabalhos que analisam suas soluções utilizando um *testbed* NGN. Portanto, a implantação do *testbed* mostra-se um diferencial e também gera resultados mais confiáveis. Além disso, outros trabalhos (Kimura et al, 2009; Lopes et al, 2009) utilizam o *testbed*;
2. Especificação dos módulos do lado cliente da arquitetura SOHand – Algumas arquiteturas são encontradas na literatura, porém auxiliar na especificação do provimento de acesso e serviços com base em contexto é uma das contribuições do trabalho;

3. Serviços com contexto em NGN - Uma das principais contribuições deste trabalho foi aproveitar a infraestrutura da rede sem fio para capturar contexto e utilizá-los para prover serviços. Neste sentido, alguns cenários foram propostos e dois foram validados. Esses resultados foram relatados em uma publicação (Yokoyama, 2008);
4. Avaliação do impacto da captura de informações contextuais – Uma avaliação dos impactos mostrou que, apesar dos benefícios, a captura do contexto prejudica o desempenho da rede (Yokoyama et al., 2009). Além disso, os trabalhos focados em QoS deveriam analisar o custo/benefício do *handover*.

Os resultados da avaliação de desempenho do *testbed* revelaram problemas relacionadas às interferências de rádio externas (Carvalio Jr. et al., 2009) e gerenciamento de mobilidade envolvendo o MIPv6 e *handover* vertical com Bluetooth (Lopes et al., 2007). Ainda, este trabalho discorre sobre a possibilidade de utilização de informações de contexto para prover serviços em NGN. As avaliações também resultaram em dois modelos, um para estimar o impacto da captura de contexto e outro para a relação custo/beneficio do *handover*.

7.2. Trabalhos Futuros

Com a conclusão deste trabalho, podem ser apontadas outras direções como objeto de estudo para trabalhos futuros. Entre elas, tem-se o novo padrão para Gerenciamento de *Handover*, o IEEE 802.21. Suas informações poderiam ser utilizadas como contexto para serviços. Ainda, poderiam ser realizadas diversas avaliações do protocolo utilizando o *testbed*. Com relação à tecnologia, o rádio cognitivo adéqua-se à ideia de ciência de contexto, por isso, poderia-se também incorporá-lo ao gerenciador de contexto e *handover*.

Atualmente, um pequeno conjunto de informações de contexto é capturado e armazenado de forma centralizada. Outro ponto para ser aprimorado é expandir o número de informações contextuais capturadas e compartilhar essas informações entre os usuários, ou seja, como uma troca de experiências. Contudo, as informações a serem compartilhadas demandam também um estudo da privacidade e segurança do usuário.

Com relação à arquitetura SOHand é importante a implementação dos outros módulos e integrá-los ao Gerenciamento de Contexto. Por exemplo, o módulo de negociação poderia usar contexto como incentivos ao *handover*. Ainda, SOHand poderia ser melhor explorado em rede móveis *Mesh* e Redes Sociais (*Social Networks)*.

Referências Bibliográficas

6NET – “Mobile IPv6 Handovers: Performance Analysis and Evaluation”. 2005. Disponível em: http://www.6net.org/publications/deliverables/D4.1.3v2.pdf .Acesso em 10-02-2008

Ahmed, T.; Kyamakya, K.; Ludwig, M., "Architecture of a Context-Aware Vertical Handover Decision Model and Its Performance Analysis for GPRS - WiFi Handover," Computers and Communications, 2006. ISCC '06. Proceedings. 11th IEEE Symposium on, vol., no., pp. 795-801, 26-29 June 2006.

Akyildiz, I., F.; Mcnair, J.; Ho, J., S., M.; Uzunalioglu, H.; Wang, W.; “Mobility Management in Next-Generation Wireless Systems”; Proceedings of the IEEE, Volume 87; Issue 8; Pages(s): 1347 – 1384; August 1999.

Balasubramaniam, S.; Indulska, J.; “Vertical handover supporting pervasive computing in future wireless networks”. Computer Communications, Volume 27, Issue 8, Advances in Future Mobile/Wireless Networks and Services, May 2004, Pages 708-719.

Berndt, H., “Towards 4G Technologies: service with iniciative”. Ed. Jonny Wiley. 2008.

Carvalio Jr, D.; Yokoyama, R. S.; Moreira, E. S.; “Análise da utilização de espectro em redes IEEE 802.11: Um estudo de caso”. In. XIV Workshop de Gerência e Operação de Redes e Serviços (WGRS), 2009. Recife, Brasil.

Davies, J., “Ipv6 – Understanding IPv6 Second edition”. Ed. Microsoft Press, 2008

Dey, A. 2001. “Understanding and Using Context. Personal Ubiquitous Comput”. 5, 1 (Jan. 2001), 4-7.

Dey, A.K. and Abowd, G.D. ‘A conceptual *framework* and a toolkit for supporting rapid prototyping of context-awareapplications’, Human-Computer Interactions (HCI) Journal, Vol. 16, Nos. 2–4, pp.7–166.2001

Dutta A., Das S., Famolari D., Ohba Y., Taniuchi K., Fajardo V., Lopez R. M, Kodama T., Schulzrinne H. Seamless proative handover across heterogeneous Access network. Wireless Pers Commun 43. p. 837-855.2007

Frattasi, S.; Fathi, H.; Fitzek, F.H.P.; Prasad, R.; Katz, M.D., “Defining 4G technology from the users perspective,” Network, IEEE , vol.20, no.1, pp.35-41, Jan.-Feb. 2006

Gu, T., Pung, H. K., Zhang, D. Q. “A service-oriented middleware for building context-aware services”. Journal of computer and computer applications 28 (2005) 1-18.

Han Gyol Kim; Myong Ju Yu; Jong Min Lee; Yong Hun Yu; Song Gon Choi, "Network Based Global Mobility Management Scheme in NGN," Networked Computing and Advanced Information Management, 2008. NCM '08. Fourth International Conference on , vol.2, no., pp.547-553, 2-4 Sept. 2008

Heissenhuber, F. e Fritsche, W. “Mobile IPv6 - Mobility support for the Next Generation Internet”, In. IPv6 Forum, White Paper. (2002). Disponível em: http://cnscenter.future.co.kr/resource/hot-topic/mip/MobileIPv6_Whitepaper.pdf. Acesso em: 10-02-2008

Hofer, T., Schwinger, W., Pichler, M., Leonhartsberger, G and Altmann, J. “Context-awareness on móbile devices – the hydrogen approach”, Proceedings of the 36th Annual Hawaii International Conference on System Sciences, pp.292–302.2002

ITU-T – “Definition of NGN”- Disponível em: http://www.itu.int/ITU-T/ngn/definition.html. Acesso em: 10-02-2009

ITU-T, Recommendation Q.1703 – “Service and network capabilities *framework* of network aspects for systems beyond IMT-2000”. 2004. Disponível em: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Q.1703-200405-I!!PDF-E&type=items. Acesso em: 10-02-2008

Johnson, D., Perkin, C., Arkko, J. , “ Mobility Support in IPv6” – IETF RFC 3775. http://www.ietf.org/rfc/rfc3775.txt. 2004

Kimura, B. Y. L, Yokoyama R. S., Moreira E. S, Mapp G, Lopes R.R, Guardia H. C. “A Fault-tolerant Approach for IP Mobility Management”. Submetido para: 28th International Symposium on Reliable Distributed Systems (SDRS´09)

Kimura, B., Y., L; Guardia, H., C.; “TIPS: Mobilidade IP sobre a Camada de Transporte”. XXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC'08); 2008.

Koodli, R.; “Fast Handovers for Mobile IPv6”; IETF RFC 4068; July 2005.

Kuran, Mehmet S., Tuna Tugcu, “A survey on emerging broadband wireless access Technologies”. Computer Networks 51 (2007) 3013–3046

Lee W., Kang, M., Lim, M. “Implementation of 802.21 for Seamless Handover Across Heterogeneous Network”. APNOMS 2007, LNCS 4773, pp. 326–333, 2007

Lopes, R .R; Yokoyama R. S; Kimura B. L. Y; Pawar P; Beijnum B; Moreira E.S. “A Context-aware and Feedback-based Mechanism for Wireless Connectivity Management”. Submetido para: IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. 2009

Lopes, R. R. F. ; Yokoyama, R. S. ; Santos, D. P. ; Moreira, E. S. ; Guardia, H. C..“Wireless Footprintig: Um mecanismo ciente de contexto para gerenciar handovers entre redes de acesso sem fio”. In: I Workshop on Pervasive and Ubiquitous Computing, 2007, Gramado. Proceedings of I Workshop on Pervasive and Ubiquitous Computing. Aceito para publicação, mas não publicado.

Maltz, D., A.; Bhagwat, P.; “MSOCKS: An Architecture for transport layer mobility”; Proceedings of the Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM’98); Volume 3; Issue; Page(s):1037 – 1045; April 1998.

Manner, J. and Kojo, M.; “Mobility Related Terminology”; IETF RFC 3753; June 2004.

Martins, L., Barbosa, A., Lima, M. B.- “Redes móveis baseadas nos protocolos IPv4 e IPv6 - uma visão geral do MIP e MIPv6”. Boletim bimestral sobre tecnologia de redes produzido e publicado pela RNP. Abril de 2003. volume 7. n.1. Disponível em: http://www.rnp.br/newsgen/0301/mip.html. Acesso em: 10-02-2008.

MIPL, “Mobile IPv6 for Linux project at Helsinki University of Technology”. Disponível em: www.mobile-ipv6.org. Acesso em: 12/01/2009.

Moreira, E.D.S.; Cottingham, D.N.; Crowcroft, J.; Pan Hui; Mapp, G.E.; Vanni, R.M.P., "Exploiting contextual handover information for versatile services in NGN environments," Digital Information Management, 2007. ICDIM '07. 2nd International Conference on , vol.1, no., pp.506-512, 28-31 Oct. 2007

Moskowitz, R; Nicander, P.; (2006) “*Host* Identity Protocol (HIP) Architecture”, IETF RFC 4423, May 2006.

Myoung Ju Yu; Jong Min Lee; Seong Gon Choi; Eunah Kim; Junghoon Jee, "Performance Comparison of Existing Mobility Management Schemes for NGN," Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference , vol.2, no., pp.991-995, 20-22 Feb. 2006

Ohba, Y. (Ed), (2007). “Protocol for carrying authentication for network access (PANA)”. draft-ietfpana-pana-14, IETF Draft, work in progress.

OWL , “Web Ontology Language Overview” . http://www.w3.org/TR/owl-features/. . Acesso em: 12/05/2009.

Pawar, P., Beijnum, B., Wac, K., Maret, P., Halteren, A., Hermens, H. “Context-Aware Middleware Architecture for Vertical Handover Support to Multi-homed Nomadic Mobile Services”, '23rd ACM Symposium on Applied Computing (ACM SAC 2008)', Middleware Engineering Track, Brazil, March 2008.

Perkins, C., E.; “IP Mobility Support for IPv4”; IETF RFC 3344; August 2002.

Prekop, P. and Burnett, M. “Activities, context and ubiquitous computing”, Special Issue on Ubiquitous Computing Computer Communications, Vol. 26, No. 11. pp.1168–1176.

Protégé, “Protégé”. Disponível em: http://protege.stanford.edu/. . Acesso em: 12/05/2009.

Quoc-Thinh Nguyen-Vuong, Nazim Agoulmine, Yacine Ghamri-Doudane “A user-centric and context-aware solution to interface management and access network selection in heterogeneous wireless environments”, Computer Networks, Volume 52, Issue 18, 22 December 2008, Pages 3358-3372.

Rappaport, T (2009) “Comunicações sem fio: Princípios e Práticas”. 2 edição. Prentice Hall PTR.

Rosenberg, J.; Schulzrinne, H.; Camarillo, G.; Johnston, A.; Peterson, J.; Sparks, R.; Handley, M.; Schooler, R.; “SIP: Session Initiation Protocol”; IETF RFC 3261; June 2002.

Saaty, T.L. "How to make a decision: the analytic hierarchy process". European Journal of Operational Research 48 (1990) 9–26.

Schilit, B.N.; Theimer, M.M., "Disseminating active map information to mobile *host*s". Network, IEEE , vol.8, no.5, pp.22-32, Sep/Oct 1994

Schmidt, A., Beigl, M, Gellersen, H., "There is more to context than location". Computers & Graphics, Volume 23, Issue 6, December 1999, Pages 893-901

Silva, A. J., Faria, M. R. "Hierarquia de Endereços IPv6". Boletim bimestral sobre tecnologia de redes produzido e publicado pela RNP – Rede Nacional de Ensino e Pesquisa 16 de março de 2001 | volume 5, número 2. http://www.rnp.br/newsgen/0103/end_ipv6.html#ng-1-1

Soliman, H., Castelluccia, C., Malki, K. E, Bellier, L. "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)". IETF RFC 4140. http://www.ietf.org/rfc/rfc4140.txt, 2005

Stewart, R.; Xie, Q.; Morneault, K.; Sharp, C.; Schwarzbauer, H.; Taylor, T.; Rytina, I.; Kalla, M.; Zhang, L.; Paxon, V; "Stream Control Transmission Protocol"; IETF RFC 2960; October 2000.

Studer, R., Benjamins, R., Fensel, D. "Knowledge Engineering:Principles and Methods". Data and Knowledge Engineering. 25(1998):161-197

Suk Y. H.; Kai H. Y. "Challenges in the migration to 4G mobile systems" Communications Magazine, IEEE , vol.41, no.12, pp. 54-59, Dec. 2003

Tanenbaum, A.S., "Redes de Computadores". 4º. Ed. Editora Campus. 2003.

Urtado, A. A, Alves Jr. N. "Implementação do protocolo IPv6 na RedeRio" http://www.ipv6.br/IPV6/ArtigoImplementacaoRedeRioParte06

Vanni,R. M. P; Moreira, E. S; Goularte, R. – "DOHand: An ontology to support building services to exploit handover information in mobile heterogeneous networks". In: I2TS, 2006, Cuiabá, MT, Brazil. 5th International Information and Telecommunication Technologies Symposium, 2006. v. 1. p. 105-112.

Vidales,P.; Bernardos, C. J.; Soto,I.; Cottingham, D.; Baliosian, J.; Crowcroft, J.; "MIPv6 experimental evaluation using overlay networks". Computer Networks, Volume 51, Issue 10, 11 July 2007, Pages 2892-2915.

Wei, Q., Farkas, K., Prehofer, C., Mendes, P., and Plattner, B. 2006. "Context-aware handover using active network technology". Computer Network. 50, 15 (Oct. 2006), 2855-2872.

Wong, J. and Hong, J. "What do we "*mashup*" when we make *mashup*s?" In Proceedings of the 4th international Workshop on End-User Software Engineering (Leipzig, Germany, May 12 - 12, 2008). WEUSE '08. ACM, New York, NY, 35-39.

Yokoyama, R. S. ; Kimura, B. Y. ; Lopes, R, R, F. ; Moreira, E. S. . Uma Abordagem Ciente de Contexto para Handovers Orientados a Serviços em Ambientes NGN. In: 7th International Information and Telecommunication Technologies Symposium (I2TS'2008), 2008, Foz do Iguaçu.