



Universidade Federal do Ceará  
Centro de Ciências  
Departamento de Computação  
Mestrado e Doutorado em Ciência da Computação

**UMA PROPOSTA DE INTEGRAÇÃO DAS REDES UMTS E IEEE  
802.11 COM SUPORTE A MOBILIDADE**

Antonia Diana Braga Nogueira

DISSERTAÇÃO DE MESTRADO

Fortaleza  
Agosto/2007

Universidade Federal do Ceará  
Centro de Ciências  
Departamento de Computação

Antonia Diana Braga Nogueira

**UMA PROPOSTA DE INTEGRAÇÃO DAS REDES UMTS E IEEE  
802.11 COM SUPORTE A MOBILIDADE**

Dissertação apresentada ao Programa de Mestrado e Doutorado em Ciência da Computação do Departamento de Computação da Universidade Federal do Ceará como requisito parcial para obtenção do grau de Mestre em Ciência da Computação.

Orientadora: Profa. Rossana M. de C. Andrade, PhD.

Fortaleza  
Agosto/2007

# Uma Proposta de Integração das Redes UMTS e IEEE 802.11 com Suporte a Mobilidade

Antonia Diana Braga Nogueira

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal do Ceará como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.

---

Profa. Rossana M. de C. Andrade, PhD.  
Universidade Federal do Ceará

---

Prof. Miguel Franklin de Castro, PhD  
Universidade Federal do Ceará

---

Profa. Judith Kelner, PhD  
Universidade Federal de Pernambuco

*Dedico este trabalho a minha avó Lalã (in memorian) e a  
minha irmã gêmea, minha anjinha (in memorian).*

## AGRADECIMENTOS

A Deus, por ter me dado oportunidade para iniciar e saúde para concluir este trabalho.  
À minha família, pelo incentivo e compreensão durante o período do desenvolvimento deste trabalho.

À professora Rossana, pelo acolhimento cordial em seu grupo de pesquisa, por sua zelosa orientação e dedicação.

Aos amigos do Grupo de Redes de Computadores, Engenharia de Software e Sistemas (GREat) da UFC pelo compartilhamento de equipamentos, troca de conhecimento e, principalmente, amizade.

Às minhas amigas de colégio, que sempre compreenderam minha ausência em aniversários, encontros e sempre torceram pelo meu sucesso e crescimento profissional. Amo vocês!!!

Aos meus amigos de graduação, que sempre me deram forças para continuar este trabalho.

À UFC e ao Programa de Mestrado e Doutorado em Ciência da Computação pelas instalações e pela excelência do ensino.

À Funcap e o CNPq pelo apoio financeiro, que foi indispensável para minha dedicação exclusiva a realização deste trabalho.

E, por fim, mas não em último lugar, ao meu amor, Marcos Dantas, pelo apoio incondicional, e toda a sua família, que representa a minha família também.

*Aqueles que passam por nós,  
não vão sós, não nos deixam sós.  
Deixam um pouco de si,  
levam um pouco de nós.*

—ANTOINE DE SAINT-EXUPERY

## RESUMO

As redes locais sem fio (*Wireless Local Area Networks* - WLANs) IEEE 802.11 atingem taxas de transmissão de dados relativamente altas quando comparadas à outras redes sem fio, por exemplo, *Bluetooth*. Essas altas taxas de transmissão têm interessado as operadoras de redes celulares, as quais começam a ver as redes IEEE 802.11 como um complemento às suas redes de acesso. Esta interoperabilidade entre sistemas celulares e WLANs tem sido um tema bastante discutido na literatura. Por exemplo, o 3GPP (*Third Generation Partnership Project*) define seis níveis para a total integração das redes celulares de terceira geração com as redes locais sem fio. No entanto, a integração com suporte a mobilidade ainda não foi especificada, o que é necessário para viabilizar a transparência de transmissão de voz e dados para os usuários finais. Esta dissertação apresenta então duas abordagens para o gerenciamento de mobilidade na integração do sistema 3G UMTS com as redes IEEE 802.11: uma baseada no SIP (*Session Initiation Protocol*) e a outra no MIP versão 6 (*Mobile IP version 6* - MIPv6). A proposta estende a arquitetura *Loose Interworking* e utiliza os requisitos do nível 4 do 3GPP. Para especificar a proposta, as abordagens de integração das redes UMTS e IEEE 802.11 foram modeladas em diagramas de seqüência e, em seguida, mapeadas para a técnica de descrição formal SDL (*Specification and Description Language*). SDL, que é bastante utilizada para especificar formalmente sistemas de telecomunicações, apresenta procedimentos de simulação e validação que são aplicados para avaliar a especificação e, em conseqüência, as abordagens propostas.

**Palavras-chave:** UMTS, IEEE 802.11, Redes da Próxima Geração, SIP, MIPv6, SDL

## ABSTRACT

Wireless Local Area Networks (WLANs) IEEE 802.11 reach relatively high data transmission rates when compared to other wireless networks, such as Bluetooth. These high data transmission rates have gained attention from the cellular networks operators, which have been considering IEEE 802.11 networks as a complement to their access networks. This interoperability between cellular systems and WLANs has been frequently discussed in the literature. For example, 3GPP (Third Generation Partnership Project) has defined six levels for the complete integration of the third generation cellular networks and WLANs. However, the mobility support has not been specified yet, which is necessary to make feasible voice and data transmission transparency for the final users. Thus, this work presents two approaches for the mobility management of the integration between UMTS and IEEE 802.11 networks: the first one is based on SIP (Session Initiation Protocol), and the other one is based on MIPv6 (Mobile IP version 6). This proposal extends the Loose Interworking architecture and uses the fourth level of the 3GPP specification. First, these approaches are modeled using sequence diagrams and, then, they are mapped to the SDL (Specification and Description Language) formal description technique. SDL, which is largely used to formally specify telecommunications systems, presents simulation and validation procedures that are applied to evaluate the specification and, consequently, the proposed approaches.

**Keywords:** UMTS, IEEE 802.11, Next Generation Networks, SIP, MIPv6, SDL

# SUMÁRIO

<b>Capítulo 1—Introdução</b>	1
1.1 Caracterização do Problema e Motivação . . . . .	1
1.2 Objetivo e Metodologia . . . . .	3
1.3 Contribuições e Resultados Esperados . . . . .	5
1.4 Estrutura da Dissertação . . . . .	5
<b>Capítulo 2—Sistemas Celulares e Redes sem Fio</b>	7
2.1 Evolução dos Sistemas Celulares . . . . .	7
2.1.1 As Redes GSM/GPRS/EDGE . . . . .	8
2.1.2 As Redes UMTS . . . . .	10
2.2 Redes sem Fio . . . . .	13
2.2.1 O padrão IEEE 802.11 . . . . .	15
2.3 As Redes da Próxima Geração . . . . .	19
<b>Capítulo 3—Integração do Sistema UMTS com as redes IEEE 802.11</b>	22
3.1 O procedimento de <i>Handoff</i> entre as redes UMTS e IEEE 802.11 . . . . .	22
3.2 Níveis de Integração do 3GPP . . . . .	24
3.3 Arquiteturas de Integração . . . . .	26
3.4 Gerenciamento de Mobilidade . . . . .	29

3.4.1	Mobile IP – MIP	30
3.4.2	Session Initiation Protocol – SIP	32
3.5	Comparação entre os Protocolos SIP e MIPv6	40
<b>Capítulo 4—Mob4Loose: Uma extensão da Arquitetura Loose Interworking baseada no nível 4 do 3GPP</b>		<b>43</b>
4.1	Características Principais	43
4.2	Arquitetura	44
4.3	Comportamento Funcional	45
4.4	Especificação Formal	50
<b>Capítulo 5—Simulação e Validação em SDL</b>		<b>63</b>
5.1	Características da Simulação e Validação em SDL	63
5.2	Simulação do Sistema de Integração UMTS e IEEE 802.11	66
5.3	Validação do Sistema de Integração UMTS e IEEE 802.11	67
<b>Capítulo 6—Considerações Finais</b>		<b>84</b>
6.1	Contribuições e Resultados Alcançados	84
6.2	Trabalhos Futuros	85

## LISTA DE ABREVIATURAS

- 16QAM** 16 Quadrature Amplitude Modulation
- 1G** Primeira Geração
- 2G** Segunda Geração
- 3G** Terceira Geração
- 3GPP** Third Generation Partnership Project
- 3GPP2** Third Generation Partnership Project 2
- 4G** Quarta Geração
- 8-PSK** eight Phase Shift Keying
- AAA** Authentication, Authorization and Accounting
- ABC** Always Best Connected
- AK** Authentication Key
- AKA** Authentication and Key Agreement
- AMF** Authentication Management Field
- AMPS** American Mobile Phone System
- AP** Access Point
- APGW** Access Point Gateway
- AuC** Authentication Center
- AUTN** Authentication Token Number
- BA** Binding Acknowledgement

- BC** BroadCast
- BRAN** Broadband Radio Access Networks
- BS** Base Station
- BSC** Base Station Control
- BSS** Basic Service Set
- BTS** Base Transceiver Station
- BU** Binding Update
- CDMA2000** Code Division Multiple Access 2000
- CF** Cellular Function
- CK** Ciphering Key
- CN** Core Network
- CoA** Care-of-Address
- CH** Correspondent Host
- CS** Circuit Switched
- CSCF** Call Session Control Function
- CSMA** Carrier Sense Multiple Access
- DHCP** Dynamic Host Configuration Protocol
- DS** Distribution System
- DSL** Digital Subscriber Line
- EAP** Extensible Authentication Protocol
- EDGE** Enhanced Data Rate for GSM Evolution
- EPCU** Electrical Power Control Unit
- ESS** Extended Service Set

**ETSI** European Telecommunications Standards Institute

**FA** Foreign Agent

**FDT** Formal Description Technique

**FIFO** First-In First-Out

**GERAN** Generic Radio Access Network

**GGSN** Gateway GPRS Support Node

**GHSN** Gateway Hotspot Network Support Node

**GMSK** Gaussian Minimum Shift Keying

**GPRS** General Packet Radio Service

**GSM** Global System for Mobile communications

**HA** Home Address

**HA** Home Agent

**HIPERACCESS** High Performance Radio ACCESS

**HIPERLAN** High Performance European Radio LAN

**HIPERMAN** High Performance Radio Metropolitan Area Network

**HLR** Home Location Register

**HNAC** Hotspot Network Area Controller

**HSDPA** High-Speed Downlink Packet Access

**HSPA** High-Speed Packet Access

**HSS** Home Subscriber Server

**HSUPA** High-Speed Uplink Packet Access

**iBSS** independent BSS

**I-CSCF** Interrogation-Call Session Control Function

- IEEE** Institute of Electrical and Electronics Engineers
- IETF** Internet Engineering Task Force
- IK** Integrity Key
- IMS** IP Multimedia Subsystem
- IMSI** International Mobile Subscriber Identity
- IMS-MGW** IMS Media Gateway
- IMT-2000** International Mobile Telephony 2000
- IP** Internet Protocol
- ISDN** Integrated Services Digital Network
- ISM** Industrial, Scientific, and Medical
- ITU** International Telecommunications Union
- ITU-T** International Telecommunications Union – Telecommunications
- LOTOS** Language Of Temporal Ordering and Specification
- MAC** Message Authentication Code
- MBWA** Mobile Broadband Wireless Access
- MEGACO** Media Gateway Control Protocol
- MGCF** Media Gateway Control Function
- MIP** Mobile IP
- MN** Mobile Node
- MH** Mobile Host
- MRFC** Media Resource Function Processor
- MRFP** Common Object Policy Service)
- MSC** Message Sequence Chart

- NGN** Next Generation Networks
- NMT** Nordic Mobile Telephone
- NS** Network Simulator
- P-CSCF** Proxy-Call Session Control Function
- PCU** Packet Control Unit
- PDA** Personal Digital Assistants
- PIN** Personal Identification Number
- PS** Packet Switched
- PSTN** Public Switched Telephone Network
- PUK** Personal Unblocking Key
- QoS** Quality of Service
- QPSK** Quadrature Phase Shift Keying
- RAB** Radio Access Bearers
- RAND** RANDom number
- RES** RESponse
- RNC** Radio Network Controller
- RNS** Radio Network Subsystem
- S/MIME** Secure/Multipurpose Internet Mail Extensions
- S-CSCF** Serving-Call Session Control Function
- SDL** Specification Description Language
- SGSN** Serving GPRS Support Node
- SIM** Subscribe Identity Module
- SIP** Session Initiation Protocol

**SMS** Short Message Service

**SN** SeQueNce number

**SSID** Service Set Identifier

**STA** STAtion

**TCP** Transmission Control Protocol

**TDF** Técnica de Descrição Formal

**TDMA** Time Division Multiple Access

**TMSI** Temporary Mobile Subscriber Identity

**TTCN** Tree and Tabular Combined Notation

**UA** User Agent

**UAC** User Agent Client

**UAS** User Agent Server

**UCM** Use Case Map

**UDP** User Datagram Protocol

**UE** User Equipment

**UMTS** Universal Mobile Telecommunication System

**USIM** UMTS Subscriber Identity Module

**UTRAN** UMTS Terrestrial Radio Access Network

**VLR** Visitor Location Register

**WCDMA** Wideband Code-Division Multiple Access

**WEP** Wired Equivalent Privacy

**WIMAx** Worldwide Interoperability for Microwave Access

**WLAN** Wireless Local Area Network

**WPAN** Wireless Personal Area Networks

**XMAC** eXpected MAC

**XRES** eXpected RES

## LISTA DE FIGURAS

2.1	Domínios do UMTS (adaptado de [1]) . . . . .	10
2.2	Processo de autenticação na rede UMTS (adaptado de [2]) . . . . .	13
2.3	Tecnologias sem fio (adaptado de [3]) . . . . .	15
2.4	Componentes da arquitetura IEEE 802.11 . . . . .	16
2.5	Tipos de rede IEEE 802.11 . . . . .	17
2.6	Processo de autenticação na rede IEEE 802.11 (adaptado de [4]) . . . . .	19
2.7	Redes das próxima geração . . . . .	20
3.1	Handoff vertical e horizontal entre os sistemas 2G, 3G e WLAN . . . . .	23
3.2	Arquiteturas de integração definidas em [5] . . . . .	26
3.3	Pontos de conexão das arquiteturas <i>Tight</i> e <i>Loose</i> . . . . .	27
3.4	Esquema híbrido <i>Tight</i> e <i>Loose</i> (adaptado de [6]) . . . . .	28
3.5	Proposta de integração com novos componentes no CN da rede GPRS (adaptado de [7]) . . . . .	29
3.6	Gerenciamento de mobilidade com o MIPv6 . . . . .	31
3.7	Mensagem SIP <i>re-INVITE</i> . . . . .	33
3.8	Gerenciamento de mobilidade com o SIP . . . . .	35
3.9	Arquitetura do UMTS/IMS . . . . .	37
3.10	Mensagem de registro IMS (adaptado de [8]) . . . . .	39

3.11	Formato da mensagem de registro IMS (adaptado de [8]) . . . . .	39
3.12	Formato da mensagem 401 <i>Unauthorized</i> (adaptado de [8]) . . . . .	40
4.1	Integração das redes UMTS e WLAN . . . . .	44
4.2	Troca de mensagens durante o <i>handoff</i> da rede UMTS para 802.11 com SIP	46
4.3	Troca de mensagens durante o <i>handoff</i> da rede UMTS para 802.11 com MIPv6 . . . . .	46
4.4	Troca de mensagens durante o <i>handoff</i> da rede IEEE 802.11 para UMTS com SIP . . . . .	48
4.5	Troca de mensagens durante o <i>handoff</i> da rede IEEE 802.11 para UMTS com MIPv6 . . . . .	48
4.6	Restabelecimento de conexão UMTS através da entidade Converge . . . . .	49
4.7	Economia de Energia através da entidade Converge . . . . .	50
4.8	Visão Geral do Ciclo de uma Especificação em SDL . . . . .	51
4.9	Visão Geral do sistema através do Organizer . . . . .	55
4.10	Sistema SDL de Integração das redes UMTS e IEEE 802.11 . . . . .	56
4.11	Bloco MH . . . . .	57
4.12	Diagrama de Estados do Bloco MH apresentando o processo de autenticação nas redes UMTS e IEEE 802.11 . . . . .	58
4.13	Diagrama de Estados do Bloco MH apresentando o comportamento SIP e MIP na rede IEEE 802.11 . . . . .	59
4.14	Diagrama de Estados do Bloco MH apresentando o comportamento SIP e MIP na rede UMTS . . . . .	60
4.15	Diagrama de estados da entidade Converge . . . . .	61
4.16	Diagrama de estados do servidor IMS: I-CSCF . . . . .	62

5.1	Passos do processo de simulação em SDL (adaptado de [9]) . . . . .	63
5.2	Primeiro passo do processo de simulação em SDL (adaptado de [9]) . . . .	64
5.3	Segundo passo do processo de simulação em SDL (adaptado de [9]) . . . .	65
5.4	Terceiro passo do processo de simulação em SDL (adaptado de [9]) . . . . .	65
5.5	O aplicativo <i>Simulator</i> UI da ferramenta <i>Telelogic</i> Tau . . . . .	66
5.6	Diagrama de Seqüência gerado pelo <i>Simulator</i> UI durante o processo de autenticação à rede IEEE 802.11 . . . . .	71
5.7	Diagrama de Seqüência gerado pelo <i>Simulator</i> UI durante o processo de autenticação à rede UMTS . . . . .	72
5.8	Diagrama de Seqüência gerado pelo <i>Simulator</i> UI durante o processo de <i>handoff</i> para a rede UMTS, utilizando o MIP . . . . .	73
5.9	Diagrama de Seqüência gerado pelo <i>Simulator</i> UI durante o processo de <i>handoff</i> para a rede UMTS, utilizando o SIP . . . . .	74
5.10	Diagrama de Seqüência gerado pelo <i>Simulator</i> UI durante o processo de <i>handoff</i> para a rede IEEE 802.11, utilizando o MIP . . . . .	75
5.11	Diagrama de Seqüência gerado pelo <i>Simulator</i> UI durante o processo de <i>handoff</i> para a rede UMTS, utilizando o SIP . . . . .	76
5.12	Diagrama de Seqüência gerado pelo <i>Simulator</i> UI durante o processo de restabelecimento da conexão com a rede UMTS através da <i>Converge</i> . . .	77
5.13	Diagrama de Seqüência gerado pelo <i>Simulator</i> UI durante o processo de economia de energia através da <i>Converge</i> . . . . .	78
5.14	O aplicativo <i>Validator</i> UI da ferramenta <i>Telelogic</i> Tau . . . . .	79
5.15	Validação utilizando o algoritmo <i>Bit-State</i> com profundidade máxima de 200 níveis . . . . .	79
5.16	Validação utilizando o algoritmo <i>Bit-State</i> simples com profundidade máxima de 300 níveis . . . . .	80

5.17 Validação utilizando o algoritmo <i>Bit-State</i> avançado com profundidade máxima de 800 níveis . . . . .	80
5.18 Validação utilizando o algoritmo <i>Bit-State</i> configurando o parâmetro tamanho da <i>Hash-Table</i> para 100000000 bytes . . . . .	81
5.19 Validação utilizando o algoritmo <i>Random Walk</i> . . . . .	81
5.20 Validação utilizando o algoritmo <i>Tree Walk</i> . . . . .	82
5.21 Validação utilizando o algoritmo <i>Exhaustive</i> . . . . .	82
5.22 Validação utilizando o algoritmo <i>Tree Search</i> . . . . .	83

## LISTA DE TABELAS

2.1	A evolução da tecnologia GSM . . . . .	9
2.2	Parâmetros do processo de autenticação AKA . . . . .	12
3.1	Características das Redes UMTS e IEEE 802.11 . . . . .	24
3.2	Os Níveis de Integração do 3GPP e suas Características (adaptado de [10])	25
3.3	As principais mensagens SIP de requisição e resposta (adaptado de [11]) .	34
3.4	Interfaces utilizadas entre as entidades IMS . . . . .	38
3.5	Comparação do SIP IETF x SIP 3GPP (adaptado de [12]) . . . . .	41
3.6	Comparação SIP x MIPv6 . . . . .	42
5.1	Parâmetros relevantes após execução dos algoritmos de Exploração . . . . .	68

# CAPÍTULO 1

## INTRODUÇÃO

Esta dissertação aborda a integração entre sistemas celulares e redes locais sem fio. Neste capítulo inicial, uma visão geral de cada um dos temas relacionados bem como a caracterização do problema e as motivações para a escolha da solução são apresentados na Seção 1.1; na Seção 1.2 o objetivo principal e a metodologia utilizada são descritos; as contribuições e os resultados a serem alcançados são detalhados na Seção 1.3; e, finalmente, na Seção 1.4, a estrutura da dissertação é definida.

### 1.1 CARACTERIZAÇÃO DO PROBLEMA E MOTIVAÇÃO

A evolução dos sistemas celulares está dividida em gerações. As redes da Primeira Geração (1G) surgiram em meados dos anos 80, sendo redes móveis analógicas ou semi-analógicas, tais como o sistema *Nordic Mobile Telephone* (NMT) e o *American Mobile Phone System* (AMPS). Estas redes ofereciam serviços básicos para usuários e a ênfase estava nos serviços de voz.

Com a necessidade de um sistema de comunicação móvel globalizado, grupos internacionais iniciaram a especificação da chamada Segunda Geração (2G). A ênfase na 2G está na compatibilidade e na transparência internacional. Do ponto de vista do usuário, as redes 2G incrementaram os serviços. Além do tradicional serviço de voz, estas redes podem fornecer serviços de dados e serviços suplementares (e.g., identificação do número, encaminhamento de chamadas, dentre outros). O sucesso comercial nessa geração é o GSM (*Global System for Mobile communications*). O GPRS (*General Packet Radio Service*) ficou conhecido com uma tecnologia 2.5G por representar uma transição das redes 2G para as redes da Terceira Geração (3G).

O processo de padronização dos sistemas de 3G iniciou com o *International Telecommunication Union* (ITU) através do *International Mobile Telecommunications 2000* (IMT-2000). O *European Telecommunications Standards Institute* (ETSI) era responsável

pela padronização do UMTS (*Universal Mobile Telecommunication System*), mas em 1998 foi formado o órgão *Third Generation Partnership Project* (3GPP) para continuar a especificação técnica do UMTS, que possui cinco áreas de padronização: rede de acesso, núcleo da rede, terminais, GERAN (*GEneric Radio Access Network*) e serviços. O *Third Generation Partnership Project 2* (3GPP2) foi formado para o desenvolvimento da tecnologia CDMA2000 (*Code Division Multiple Access 2000*), que é membro da família IMT-2000 (*International Mobile Telecommunications-2000*).

Atualmente, as pesquisas estão sendo focadas na chamada Quarta Geração (4G), também conhecida como redes da próxima geração (*Next Generation Networks - NGNs*), constituída por redes celulares de longa distância e por um conjunto de tecnologias heterogêneas (e.g., redes locais sem fio, rede de telefonia fixa, dentre outras) disponíveis ao usuário de forma transparente.

No caso das redes locais sem fio, as redes IEEE (*Institute of Electrical and Electronics Engineers*) 802.11 [13] representam um marco para as redes locais sem fio. Essas redes constituem-se como uma alternativa às redes convencionais com fio, fornecendo as mesmas funcionalidades, no entanto, provê-las de forma flexível e com boa conectividade em áreas denominadas *hotspots*, termo que designa um local público (e.g., aeroportos, universidades, *shoppings*, dentre outros) onde é fornecido o serviço de rede local sem fio para usuários finais, fornecendo áreas com altas taxas de transmissão de dados.

Um importante passo rumo ao acesso a sistemas heterogêneos de forma contínua e sem rupturas, é a integração das redes locais sem fio (*Wireless Local Area Network - WLAN*) com as redes 3G [14]. Por exemplo, imagine que um usuário está caminhando pela rua participando de uma chamada em conferência com outros usuários através do seu celular utilizando uma conexão GSM/GPRS. Ao chegar ao escritório, que possui uma rede local IEEE 802.11b [15], o usuário transfere a conexão para a rede local, de forma que a sessão do serviço de conferência continua e ele permanece conversando. Esse procedimento é denominado *handoff* vertical, que é o processo de transferir o controle de um serviço em andamento de uma célula para outra entre redes diferentes (neste caso, da rede GSM/GPRS para 802.11b).

O 3GPP, mencionado anteriormente, é uma associação de organizações de padronização da Europa, Japão, China, América do Norte e Coréia do Sul. Embora o 3GPP tenha sido criado para especificar os sistemas de 3G baseado no UMTS, ele já vem se preocupando com a integração das redes UMTS e IEEE 802.11 e em [10] define alguns

princípios e níveis de integração. Existe ainda a preocupação com a segurança, por exemplo, na especificação em [16] há uma descrição dos aspectos necessários para prover um ambiente seguro na integração das redes 3G e WLAN.

Por outro lado, o 3GPP2 (Third Generation Partnership Project 2) padroniza a evolução do sistemas celulares baseado no CDMA2000, que, no entanto, não é foco deste trabalho. Em [17] é apresentado uma especificação do 3GPP2 sobre essa integração.

A integração dos sistemas é desejável, pois embora a taxa de transmissão das redes 3G seja mais alta do que a das redes 2G, ela é pequena se comparada com a de uma rede local sem fio, entretanto, as redes 3G possuem uma cobertura de alcance global. Uma WLAN fornece uma taxa de dados de até 54Mbps (para redes 802.11 a/g), mas com uma cobertura de curto alcance. Portanto, essas características tornam essas duas redes complementares.

Desse modo, a idéia de integração dos dois sistemas para unificar as vantagens e diminuir as desvantagens de cada um deles representa uma oportunidade para o mercado. Entretanto, as redes 3G e WLAN são baseadas em tecnologias diferentes e a integração delas é uma questão crítica. Sendo assim, conforme mencionado anteriormente, pesquisas vêm sendo propostas para a integração das redes celulares e WLANs. O 3GPP, por exemplo, vem trabalhando para solucionar esse aspecto, mas, até o momento, especificou somente a integração das redes 3G e WLAN sem suporte a mobilidade. Outras soluções com suporte a mobilidade têm sido discutidas no âmbito da pesquisa acadêmica.

## 1.2 OBJETIVO E METODOLOGIA

Este trabalho tem como objetivo propor a integração das redes 3G e WLAN. A rede 3G a ser considerada é a rede UMTS e como exemplo de redes locais sem fio, a família IEEE 802.11 [13]. Como essas redes não apresentam um suporte nativo para o processo de *handoff* entre elas, nesta dissertação serão utilizados dois protocolos de gerenciamento de mobilidade já existentes para prover esse suporte.

Nesta dissertação, a convergência entre as redes UMTS e IEEE 802.11 é baseada na arquitetura *Loose Interworking* [5]. Esta arquitetura foi proposta pelo ETSI (European Telecommunications Standard Institute) para a interconexão entre as WLANs e os sistemas celulares. No entanto, a arquitetura *Loose* considera a *High-Performance European Radio LAN* (HIPERLAN) como WLAN, diferentemente desta dissertação, que

considera a interconexão UMTS com as redes IEEE 802.11. O motivo da escolha do padrão IEEE 802.11 é o fato da sua larga aceitação pelos usuários finais, representando um marco para as redes locais sem fio também pela sua capacidade de interoperabilidade e evolução. Como prova desse sucesso pode-se citar o fato de a maioria dos computadores portáteis novos já saírem de fábrica equipados com interfaces IEEE 802.11 e o crescente número de *hotspots*.

Como a proposta é baseada na arquitetura *Loose*, que não possui suporte à mobilidade, dois protocolos para gerenciamento de mobilidade foram utilizados. Dentre os protocolos de mobilidade existentes na literatura [18][19][11][20][21], este trabalho utiliza o MIP (*Mobile Internet Protocol*) [19], protocolo da camada de rede desenvolvido pelo *Internet Engineering Task Force* (IETF), e o SIP (*Session Initiation Protocol*) [11], protocolo da camada de aplicação também definido pelo IETF. Esses protocolos diferem na camada em que atuam na pilha de protocolos da *Internet* e, por isso, apresentam comportamentos específicos.

Este trabalho também apresenta uma entidade, denominada *Converge*, que oferece um melhor serviço ao usuário 3G na rede IEEE 802.11. O comportamento da entidade possui duas etapas: uma referente à economia de energia do dispositivo; e outra referente ao nível de serviço prestado pela WLAN (sinal para transmissão de dados em um limite aceitável).

A metodologia utilizada para o desenvolvimento dessa dissertação é baseada em técnicas formais de desenvolvimento de software e protocolos de comunicação [22]. A proposta será inicialmente modelada utilizando diagramas de seqüência [23], em seguida, especificada formalmente com SDL (*Specification and Description Language*). SDL foi definida pela órgão de padronizações de telecomunicações ITU-T (*International Telecommunications Union – Telecommunications*) [24] no padrão Z.100 [25] para especificar e descrever sistemas de telecomunicações. Esta técnica possui ferramentas que permitem procedimentos de simulação e validação automáticas [26], as quais representam uma grande vantagem sobre outras Técnicas de Descrição Formal (TDFs), onde a obtenção de tais procedimentos é usualmente ineficaz devido ao alto custo e tempo envolvidos.

### 1.3 CONTRIBUIÇÕES E RESULTADOS ESPERADOS

A principal contribuição desta dissertação é a extensão da arquitetura *Loose Interworking* para suportar *handoff* vertical entre UMTS e IEEE 802.11, utilizando duas abordagens diferentes: uma baseada em MIP e a outra em SIP. Além disso, características para oferecer um melhor serviço ao usuário 3G na rede IEEE 802.11 são inseridas, através da *Converge*, visando a economia de energia do dispositivo do usuário e ao restabelecimento da conexão com a rede celular, caso a conexão da WLAN falhe (i.e., o sinal de rádio da WLAN passe de um limite aceitável).

O desenvolvimento de cenários utilizando diagramas de seqüência e da modelagem em SDL para prover a integração das redes UMTS e IEEE 802.11 com os protocolos MIP e SIP também são contribuições deste trabalho. Por fim, a utilização de uma ferramenta como *Telelogic TAU* [26] para a especificação, simulação e validação da proposta pode ser considerada como um diferencial desta dissertação.

Os resultados esperados são, portanto, os produtos finais gerados a partir das contribuições principais e secundárias, a seguir:

- Cenários disjuntos da proposta de gerenciamento de mobilidade utilizando MSC;
- especificação em SDL das duas abordagens para o gerenciamento de mobilidade na integração das redes UMTS e IEEE 802.11 (baseadas no SIP e no MIP), utilizando o IPv6 como protocolo da Internet;
- Cenários da avaliação do trabalho proposto através da ferramenta *Telelogic TAU SDL Suite* [26], que possui componentes para simulação e validação da modelagem SDL;
- Publicação nacional referente a proposta [27].

### 1.4 ESTRUTURA DA DISSERTAÇÃO

Além desse capítulo de Introdução, a dissertação está organizada nos capítulos descritos a seguir:

- Capítulo 2 - apresenta a evolução dos sistemas celulares e uma visão geral das redes locais sem fio, focando na evolução do sistema GSM e nas redes IEEE 802.11. Este capítulo também descreve as redes da próxima geração.
- Capítulo 3 - aborda a integração das redes UMTS e IEEE 802.11, apresentando importantes trabalhos relacionados encontrados na literatura.
- Capítulo 4 - descreve o trabalho proposto, apresentando as principais características, a arquitetura, o comportamento funcional através de diagramas de seqüência, a especificação formal em SDL dos blocos do sistema e os diagramas de estados dos principais processos.
- Capítulo 5 - apresenta o ambiente de simulação e validação utilizado, demonstrando os tipos de testes realizados e os resultados obtidos.
- Capítulo 6 - finaliza a dissertação com as considerações finais, onde são apresentadas as contribuições, os resultados alcançados bem como os trabalhos futuros.

## CAPÍTULO 2

# SISTEMAS CELULARES E REDES SEM FIO

Neste capítulo, a Seção 2.1 mostra a evolução do sistema GSM e os conceitos envolvidos, apresentando também o sistema UMTS. A Seção 2.2 descreve as principais normas técnicas existentes para as redes locais sem fio, detalhando as redes IEEE 802.11. Finalmente, a Seção 2.3, apresenta as redes da próxima geração, descrevendo suas principais características.

### 2.1 EVOLUÇÃO DOS SISTEMAS CELULARES

Com o desenvolvimento dos sistemas celulares 2G, passando de sistemas analógicos para sistemas digitais, houve um aumento na qualidade dos serviços de voz oferecidos ao usuário. Os sistemas 2G utilizam comutação por circuito e apresentam taxas de transmissão de dados que são insuficientes para a implementação de serviços mais avançados.

No entanto, para as operadoras, a migração dos sistemas 2G para os 3G envolve novos investimentos e tanto a escolha do sistema 3G a ser adotado, quanto à estratégia de migração devem considerar aspectos como a rede atual da operadora, o espectro disponível e os serviços a serem oferecidos.

Para minimizar os custos nesta transição, órgãos de padronização buscaram desenvolver normas técnicas para os sistemas 3G, as quais facilitassem a evolução dos sistemas 2G existentes. Isto originou dois tipos de evolução de tecnologias: a baseada no UMTS [28] e a baseada no CDMA2000 [29][30]. Neste trabalho, o foco está na evolução baseada no UMTS.

O UMTS foi elaborado para ser o sucessor do sistema GSM, no entanto, essa evolução passa pelo sistema GPRS, o qual adiciona novos elementos à rede núcleo para o tratamento da comutação por pacotes, e pelo EDGE (*Enhanced Data Rate for GSM Evolution*), que utiliza uma nova técnica de modulação para aumentar a taxa de transmissão.

### 2.1.1 As Redes GSM/GPRS/EDGE

O GSM, projetado pelo ETSI, possui uma taxa de transferência de dados de 9.6 kbps, fornecendo serviços básicos de dados, como SMS (*Short Message Service*). Esse sistema celular é baseado na rede TDMA (*Time Division Multiple Access*) e divide cada canal de rádio de 200 KHz em um quadro com 8 *time-slots* (25KHz).

Uma grande inovação do sistema celular GSM é o módulo de identificação do assinante (*Subscriber Identification Module - SIM*), que contém a identificação do usuário, chave de autenticação e outras informações (e.g., *Personal Identification Number - PIN* e *Personal Unblocking Key - PUK*). Outro benefício desse sistema é a característica denominada “*roaming* internacional”, a qual permite que usuários possam ter acesso aos serviços mesmo quando não estão na sua rede de origem.

A mudança dos sistemas celulares 2G para 3G passa por alguns desafios, visto que existe a necessidade de troca dos equipamentos dos usuários e da introdução de novos equipamentos de rede. Durante essa transição, surgiram os sistemas denominados 2,5G, tais como GPRS e EDGE, os quais tinham o objetivo de oferecer maiores taxas de transmissão de dados.

O GPRS, evolução do GSM, também projetado pelo ETSI, foi desenvolvido com o intuito de otimizar a transmissão de dados através do chaveamento de pacotes. Esse novo serviço, que é mais adequado para transmissão em rajadas (e.g., tráfegos gerados pelas aplicações da *Internet*), foi desenvolvido para melhorar o acesso a serviços baseados em IP quando comparados aos serviços baseados em comutação por circuitos. Com isso, surgiu a possibilidade de transmitir dados em velocidades maiores (teoricamente, as taxas podem chegar a 171.2 Kbps) do que as existentes nos sistemas anteriores. O GPRS não prevê alterações nos elementos utilizados no sistema GSM (e.g., BSS - *Base Station System*), mas sim a introdução de novos elementos de rede (e.g., *Serving GPRS Support Node-SGSN* e *Gateway GPRS Support Node-GGSN* ) responsáveis pela comutação por pacotes. Esse sistema celular é baseado na técnica de modulação denominada *Gaussian Minimum Shift Keying* (GMSK) [31].

O sistema EDGE é baseado em uma outra técnica de modulação que permite uma taxa de transmissão de bits maior do que a do GPRS. Esta nova técnica é denominada 8 *Phase Shift Keying* (8-PSK), que aumenta em até três vezes a taxa de transmissão, como pode ser observado na Tabela 2.1. A principal idéia deste sistema é adicionar

novas características na rede GSM mantendo compatibilidade com os telefones celulares GSM/GPRS e com os equipamentos da rede que continuam operando, sendo necessário atualizar o software da BTS (*Base Transceiver Station*) para possibilitar o funcionamento das modulações GMSK e 8-PSK, além da troca da placa PCU (*Packet Control Unit*) por uma placa EPCU (*Electrical Power Control Unit*) na BSC (*Base Station Control*).

Por outro lado, a base do UMTS é a tecnologia WCDMA (*Wideband Code-Division Multiple Access*), que é considerada como 3G em relação à velocidade de acesso aos serviços de dados. No entanto, o 3GPP desenvolveu também um complemento ao UMTS denominado HSPA (*High-Speed Packet Access*). O HSPA é composto tanto de propostas para *uplink* (*High-Speed Uplink Packet Access* - HSUPA) quanto para *downlink* (*High-Speed Downlink Packet Access* - HSDPA) de alto desempenho. Para que os benefícios do HSPA possam ser utilizados, é necessário que a operadora possua a rede UMTS em funcionamento. A rede HSPA necessita de atualização da rede UMTS em nível de *software* e *hardware* para suportar o processamento adicional das BTSs, como também, a adição de novos terminais, que são compatíveis com o novo serviço de dados.

Geração	2G	2,5G	2,5/3G	3G	
Tecnologia	GSM	GPRS	EDGE	UMTS	
				WCDMA	HSDPA
Taxa de dados máxima teórica (kbit/s)	14.4	171.2	433.6	2000	14000
Taxa de dados máxima prática (kbit/s)	9.6	26-40	100-130	200-300	400-700
Canal (kHz)	200	200	200	5000	5000
Modulação	GMSK	GMSK	8-PSK	QPSK	16QAM

**Tabela 2.1** A evolução da tecnologia GSM

O WCDMA usa a modulação *Quadrature Phase Shift Keying* (QPSK) para transmissão e o HSDPA utiliza o 16 *Quadrature Amplitude Modulation* (16QAM), que fornece uma taxa de transmissão de dados maior por utilizar quatro bits por símbolo, ao invés de dois bits utilizados no QPSK.

Na Tabela 2.1 pode-se observar algumas características das tecnologias envolvidas na evolução do GSM, sempre buscando taxas de transmissão de dados maiores. A tabela apresenta a taxa de transferência de dados máxima na teoria (i.e., a taxa definida na norma técnica), a taxa de transferência de dados máxima na prática (i.e., a taxa que é realmente atingida), o canal e a técnica de modulação utilizada por cada tecnologia.

### 2.1.2 As Redes UMTS

As redes UMTS suportam serviços multimídia e acesso à *Internet* com alto desempenho e provisionamento de qualidade de serviço (*Quality of Service - QoS*), oferecendo vantagens que os usuários da 2G jamais obteriam, como por exemplo, um usuário poder assistir a um programa de televisão no seu celular.

#### *A arquitetura da rede UMTS*

O sistema UMTS utiliza o mesmo *Core Network (CN)* do GPRS, com uma nova interface de acesso de rádio, a UTRAN (*UMTS Terrestrial Radio Access Network*), a qual é conectada ao CN via interface “Iu”.

O UMTS pode ser dividido em três domínios lógicos, como mostrado na Figura 2.1 [1]:

- UE (*User Equipment*) - equipamento do usuário;
- UTRAN - a rede de acesso;
- CN - a rede núcleo, que é responsável pela comutação, autenticação, encaminhamento de dados e acesso às redes externas.

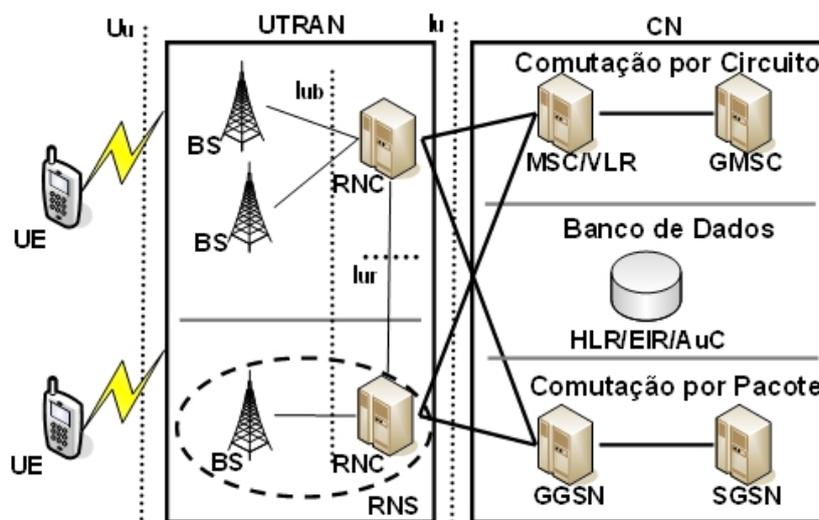


Figura 2.1 Domínios do UMTS (adaptado de [1])

O UE utiliza a interface “ $U_u$ ” e o cartão USIM (UMTS *Subscriber Identity Module*), o qual contém a identidade do assinante. No cartão USIM, que é semelhante ao cartão SIM do GSM, estão armazenadas as chaves de autenticação e os códigos criptográficos, fornecendo, dessa forma, funções de segurança e autenticação do usuário. Além disso, o USIM pode suportar, no mesmo cartão, mais de um perfil do usuário (*user profile*), que é designado quando o usuário faz a assinatura com a operadora e contém informações sobre identificação do usuário e os serviços que devem ser providos a ele.

A rede de acesso UTRAN tem como tarefa principal criar e manter os *Radio Access Bearers* (RABs) para a comunicação entre o UE e o CN. O UTRAN é localizado entre as interfaces “ $U_u$ ” e “ $I_u$ ”.

A arquitetura UTRAN consiste de RNSs (*Radio Network Subsystems*). Cada RNS contém Estações Base (*Base Stations* – BSs) e uma RNC (*Radio Network Controller*). A interface que conecta a BS à RNC é a “ $I_{ub}$ ” e as RNSs são separadas por uma interface UMTS denominada “ $I_{ur}$ ”, que possibilita o tráfego de dados e sinalização.

O CN contém o domínio de comutação por circuito (*Circuit Switched* - CS) e o domínio de comutação por pacote (*Packet Switched* - PS). A interface entre o CN e a rede de acesso UTRAN é chamada “ $I_u$ ”. Devido ao tipo de tráfego para identificar o domínio, a interface pode ser chamada também de “ $I_{ucs}$ ” (i.e., interface entre uma rede de acesso e o domínio CS), e “ $I_{ups}$ ” (i.e., interface entre uma rede de acesso e o domínio PS).

### ***Autenticação na rede UMTS***

No processo de autenticação, as redes UMTS utilizam uma arquitetura de autenticação chamada *Authentication and Key Agreement* (AKA) [2][32]. O mecanismo de autenticação UMTS AKA provê autenticação mútua, na qual o terminal autentica a rede, que também autentica o terminal. Do mesmo jeito que ocorre nas redes GSM/GPRS, o UMTS AKA segue o paradigma “Desafio-Resposta” (*Challenge-Response*), no qual o terminal tem de responder a uma requisição da rede para que seja autenticado [33]. A Tabela 2.2 apresenta os parâmetros utilizados na autenticação AKA.

Como mostrado na Figura 2.2, o início do processo de autenticação ocorre com o envio da identificação permanente, IMSI (*International Mobile Subscriber Identity*), ou temporária, TMSI (*Temporary Mobile Subscriber Identity*), do terminal para o SGSN. Em

seguida, o SGSN faz uma requisição ao AuC (*Authentication Center*) ou ao HLR (*Home Location Register*) dos dados de autenticação do terminal identificado pelo IMSI ou TMSI. O AuC inicia um processo para obter o vetor de autenticação através da execução de vários algoritmos de criptografia (f1, f2, f3, f4 e f5). O resultado do processo de autenticação UMTS gera os seguintes valores: valor aleatório RAND, chave cifrada (*Ciphering Key* – CK), chave de integridade (*Integrity Key* – IK), AK (*Anonymity Key*) (i.e., chave gerada utilizando K e RAND), resposta esperada (*eXpected REsponse* - XRES) e AUTN (*Authentication Token Number*). O AUTN é formado por: número seqüencial SQN, valor MAC (*Message Authentication Code*) e um campo administrativo AMF (*Authentication Management Field*).

Parâmetro AKA	Tamanho (bits)	Descrição	
Vetor de Autenticação (AV)	RAND	128	Desafio gerado pela rede durante o processo de autenticação
	CK	128	Chave de cifragem
	IK	128	Chave de integridade gerada durante a autenticação
	AK	128	Chave gerada pelo algoritmo f5 utilizando K e RAND
	XRES	32-128	Resposta de autenticação gerada pelo ISIM
	AUTN	128	Token de autenticação formado por SQN, MAC e AMF
AUTN	SQN	48	Número de seqüência
	MAC	64	Código de autenticação, que serve para autenticar a rede
	AMF	16	Campo de gerenciamento da autenticação

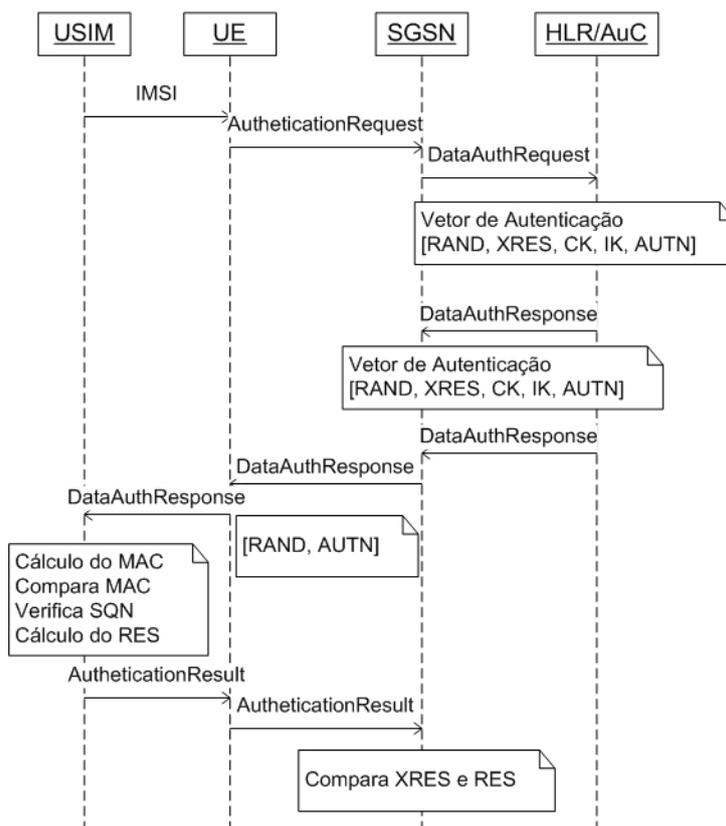
**Tabela 2.2** Parâmetros do processo de autenticação AKA

O AuC compõe então o vetor de autenticação, formado por RAND, XRES, CK, IK, AUTN, e o envia para o SGSN, o qual envia os valores RAND e AUTN do vetor de autenticação como uma mensagem de “Desafio-Resposta” para o MH (*Mobile Host*)<sup>1</sup>.

Do lado do usuário, os cálculos são feitos no USIM, o qual também armazena a chave “K”. Dessa forma, o MH calcula o valor de XMAC (*eXpected MAC*) utilizando os algoritmos e os valores RAND, K, SQN e AMF para autenticar a rede. Em seguida,

<sup>1</sup>Nesta dissertação denomina-se *Mobile Host* (MH) como o usuário que inicia a sessão e *Correspondent Host* (CH), o destinatário.

compara os valores MAC e XMAC. Se os valores forem iguais, o cartão USIM assume que os valores RAND e AUTN foram gerados por uma rede que conhece a chave “K” e continua o processo, enviando o valor RES para o SGSN. O SGSN compara os valores de RES e XRES e se estes valores forem iguais, o acesso à rede é autorizado. Se os valores XMAC e MAC forem diferentes, o processo de autenticação é interrompido.



**Figura 2.2** Processo de autenticação na rede UMTS (adaptado de [2])

## 2.2 REDES SEM FIO

As redes sem fio são utilizadas como uma alternativa interessante às redes com fio, pela facilidade de instalação de uma infra-estrutura onde o cabeamento de rede gera custos elevados ou que áreas a serem cobertas pela rede fossem de difícil acesso. Além disso, as redes sem fio permitem que os usuários se locomovam permanecendo conectados.

O IEEE possui quatro grupos de trabalho destinados às redes sem fio, os quais fazem parte do Comitê de Normas Técnicas 802, a seguir: grupo de trabalho 11 [15], grupo de trabalho 15 [34], grupo de trabalho 16 [35] e grupo de trabalho 20 [36].

O padrão 802.11 [15] usado nas redes locais sem fio (WLANs) utiliza faixas de frequências não-licenciadas, denominadas ISM (*Industrial, Scientific, and Medical*). Essas faixas podem ser utilizadas sem pagamento de tarifas, diferentemente das frequências licenciadas, como as que são utilizadas pelos sistemas celulares (e.g., GSM e UMTS), que dependem do pagamento de taxas de permissão e de uma licença de um órgão regulador dos serviços de telecomunicações de cada país. As WLANs oferecem um alcance típico de 30 a 500 metros na faixa de frequência ISM, em torno de 2,4 GHz, e uma taxa de transmissão de até 54 Mbps (e.g., IEEE 802.11a até 11 Mbps, IEEE 802.11b e IEEE 802.11g, a qual é compatível com as extensões “a” e “b” com taxa de até 54 Mbps), dependendo das condições de transmissão do local.

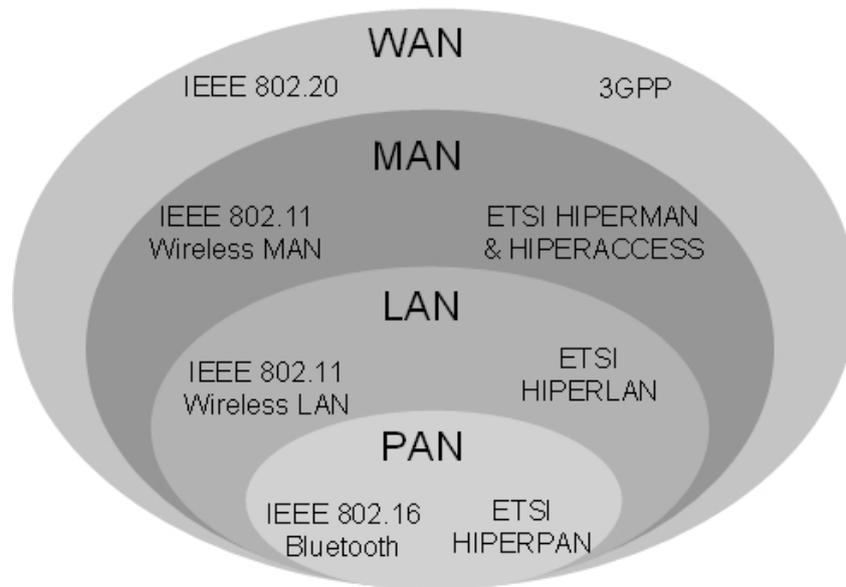
O grupo de trabalho 15 [34] define as redes de área pessoal sem fio (*Wireless Personal Area Networks* - WPANs), que são as redes que integram dispositivos portáteis e de computação móvel como computadores pessoais, PDAs (*Personal Digital Assistants*), periféricos, telefones celulares e eletrodomésticos. O *Bluetooth* [37] é uma das principais tecnologias desse sistema, também utiliza a banda ISM e oferece taxas de até 1 Mbps.

O grupo de trabalho 16 [35] representa as redes metropolitanas sem fio (*Broadband Wireless Metropolitan Area Networks*) ou *Wireless* MANs, as quais utilizam as faixas licenciadas entre 10 e 66 GHz. Essa norma técnica, largamente conhecida como WIMAX (*Worldwide Interoperability for Microwave Access*), tem como proposta inicial disponibilizar o acesso a banda larga sem fio cobrindo grandes distâncias sem a necessidade de investimento em uma infra-estrutura de alto custo (como ocorre com uma rede de acesso banda larga cabeada) e sem as limitações de distância das tecnologias DSL (*Digital Subscriber Line*). O padrão IEEE 802.16 pode ser definido como um padrão global, pois foi desenvolvido de modo a ser compatível com os padrões do ITU e do ETSI, mais especificamente com os padrões HIPERACCESS (*High Performance Radio ACCESS*) e HIPERMAN (*High Performance Radio Metropolitan Area Network*) [38].

O grupo de trabalho 20 [36], conhecido como *Mobile-Fi*, ou *Mobile Broadband Wireless Access* (MBWA), opera em bandas licenciadas abaixo de 3,5 GHz. O 802.20 oferece suporte à mobilidade veicular de alta velocidade (até 250 Km/h) em ambientes de redes metropolitanas, sendo projetado para garantir alta eficiência espectral e baixa latência. Essas garantias são obtidas graças aos valores atingidos pelo IEEE 802.20 para as taxas de transmissão de dados e o número de usuários ativos, que são significativamente mais elevados do que aqueles alcançados pelos sistemas móveis existentes. O objetivo do 802.20 é habilitar o desenvolvimento global do acesso banda larga sem fio ubíquo, inte-

roperável entre diferentes vendedores, atendendo as necessidades de usuários residenciais e empresariais.

A Figura 2.3 [3] apresenta o posicionamento de cada uma das tecnologias sem fio, mostrando do lado esquerdo a norma técnica do IEEE e do lado direito a equivalente do ETSI.



**Figura 2.3** Tecnologias sem fio (adaptado de [3])

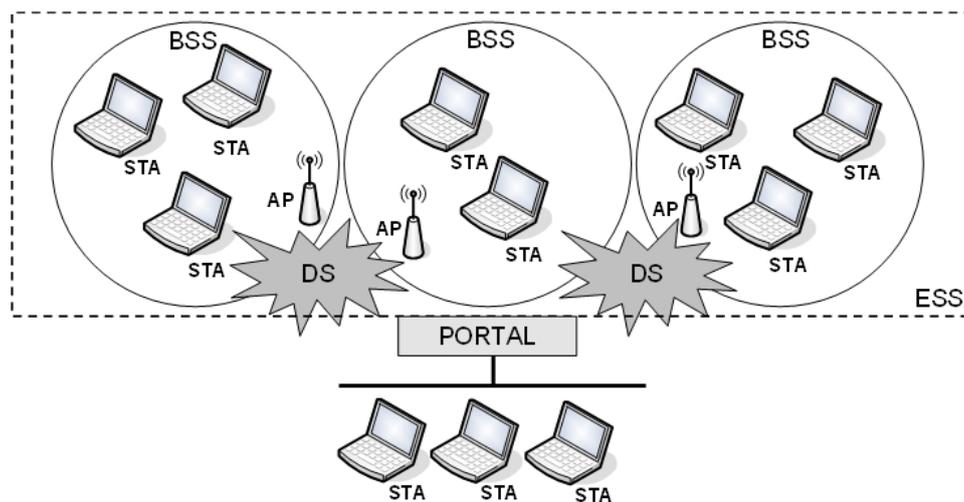
### 2.2.1 O padrão IEEE 802.11

Conforme mencionado anteriormente, existem dois padrões importantes para as WLANs: o *High-Performance European Radio LAN* (HIPERLAN), definido pelo ETSI; e o IEEE 802.11 WLAN [13], que é o foco deste trabalho e que é detalhado nesta seção.

#### *A arquitetura da rede 802.11*

Os componentes da arquitetura de uma rede IEEE 802.11 estão ilustrados na Figura 2.4. O Conjunto Básico de Serviço (*Basic Service Set - BSS*) corresponde a uma célula de comunicação sem fio que está dentro do alcance de uma estação rádio base, o ponto de acesso (*Access Point - AP*). Em um BSS estão contidas as estações (*STations - STAs*) que estão sob o controle de uma mesma função de coordenação. Esta função determina quando cada STA pode enviar ou receber dados através do meio sem fio.

Vários BSSs podem ser interligados através de um sistema de distribuição (*Distribution System - DS*), de modo a aumentar a cobertura da rede. Esse sistema de distribuição forma o Conjunto Estendido de Serviço (*Extended Service Set - ESS*). O ESS consiste na conexão de vários BSSs comportando-se como um só, podendo estar ligado a uma rede tradicional. O portal funciona como uma ponte entre uma rede sem fio e uma rede cabeada.



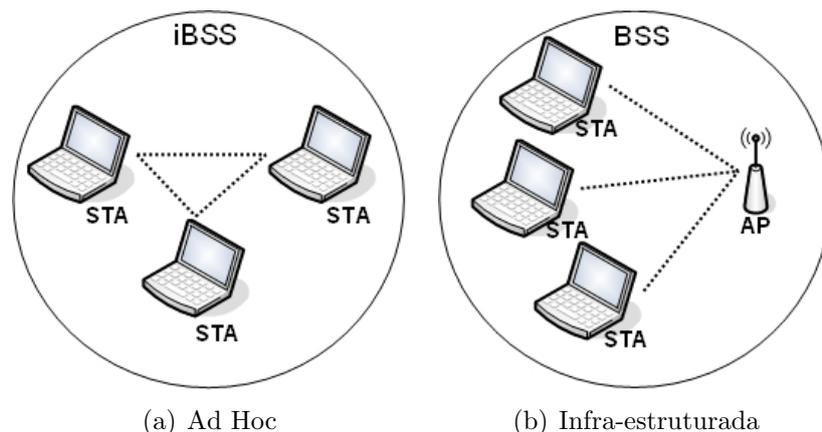
**Figura 2.4** Componentes da arquitetura IEEE 802.11

Como mostrado na Figura 2.5(a), o conjunto de STAs sem infra-estrutura, onde cada STA comunica-se com as outras diretamente, é chamado de rede *Ad Hoc*. Em uma rede *Ad Hoc*, o BSS é chamado de BSS independente (iBSS). O outro tipo de WLAN é o de redes infra-estruturadas como mostrado na Figura 2.5(b). Nesse caso, são utilizados pontos de acesso, que coordenam a comunicação entre STAs dentro de uma BSS.

### ***Os processos de Associação e Autenticação na rede IEEE 802.11***

O processo de associação das STAs inicia quando uma estação, ao perceber um sinal de um AP, resolve se associar a ele. Esse processo é realizado antes da transmissão dos dados e é baseado na intensidade do sinal do ponto de acesso.

A estação também pode verificar se existe outro AP que ofereça uma intensidade de sinal mais forte. Se um outro AP oferece um sinal melhor, a STA muda a sintonia para o canal do AP com sinal mais forte. Este processo é conhecido como re-associação e normalmente acontece devido à mobilidade do terminal em relação ao AP no qual ele estava associado. A associação é uma pré-condição necessária para o processo de autenticação 802.11.



**Figura 2.5** Tipos de rede IEEE 802.11

O procedimento de autenticação em uma rede 802.11 é o processo de validação das credenciais de um usuário para se conectar a uma rede e usar os seus serviços. Existem dois algoritmos especificados pelo padrão 802.11:

- Autenticação de sistema aberto, na qual qualquer estação com o SSID (*Service Set Identifier*) do AP pode se conectar na rede; e
- Autenticação com chave compartilhada, na qual a estação e o AP possuem a cópia de uma chave compartilhada para que o acesso seja permitido. Se a estação tiver uma chave inválida, que não é aquela esperada pelo AP, o processo de autenticação falha, e a associação da estação não é permitida com o AP.

O processo de criptografia utiliza o protocolo *Wired Equivalent Privacy* (WEP), o qual provê serviços de autorização e de criptografia aos usuários de uma WLAN.

Estes mecanismos de autenticação do 802.11 apresentam limitações. Os valores SSID e os endereços físicos das estações (*Media Access Control* - MAC) podem ser facilmente obtidos através de ferramentas de capturas de pacotes (e.g., *Sniffers*) e o mecanismo de criptografia, usado pelo WEP, já foi quebrado [39].

### ***Autenticação de um terminal UMTS na rede IEEE 802.11***

O EAP (*Extensible Authentication Protocol*) AKA [4] define um tipo de autenticação que permite que um terminal UMTS seja autenticado em ambientes WLANs.

Nas WLANs, o processo EAP AKA é um mecanismo para autenticação e distribuição de chaves usando o AKA, que é utilizado nas redes 3G, tais como UMTS e CDMA2000.

O EAP AKA também segue o paradigma “Desafio-Resposta”. O processo de autenticação EAP AKA para um terminal UMTS é ilustrado na Figura 2.6. O procedimento de autenticação é baseado no IEEE 802.1x [40] e no EAP AKA [4]. O AP é um cliente que repassa as mensagens EAP do terminal para o servidor AAA e vice-versa, e provê acesso à rede de acordo com o resultado final da autenticação.

O processo inicia com a associação do UE e o AP. O UE envia a mensagem *EAP-Start*. Em seguida, o AP e o UE trocam mensagens (*EAP-Request/Identity* e *EAP-Response/Identity*) onde é requisitada a identidade do terminal. A requisição é enviada para o servidor AAA correspondente.

O servidor AAA faz a requisição do vetor de autenticação [RAND, XRES, CK, IK, AUTN] e envia os dados do usuário para o AuC, que retorna o vetor de autenticação. Então, o servidor AAA envia a mensagem *EAP-Request/AKA-Challenge* contendo os valores de RAND e AUTN, os quais serão utilizados pelo cartão USIM, a fim de verificar a autenticação da rede pelo terminal.

O AP repassa a mensagem *EAP-Request/AKA-Challenge* para o UE. O terminal executa os algoritmos de autenticação para os valores de RAND e AUTN recebidos.

Se XMAC for diferente de MAC, a autenticação é rejeitada pelo terminal. Se XMAC for igual ao MAC recebido no AUTN, a rede é autenticada e o USIM calcula os valores RES, CK e IK.

O terminal então envia uma mensagem contendo o valor RES. O AP repassa a mensagem *EAP-Request/AKA-Challenge* com o valor de RES, para o servidor AAA.

O servidor compara os valores de RES e SRES e se estes valores forem iguais, o acesso à rede é autorizado (mensagem *EAP-Success*). Se os valores de RES e XRES forem diferentes, uma mensagem *EAP-Failure* é enviada ao AP, que encaminha a mensagem *EAP-Success* ou *EAP-Failure* para o terminal.

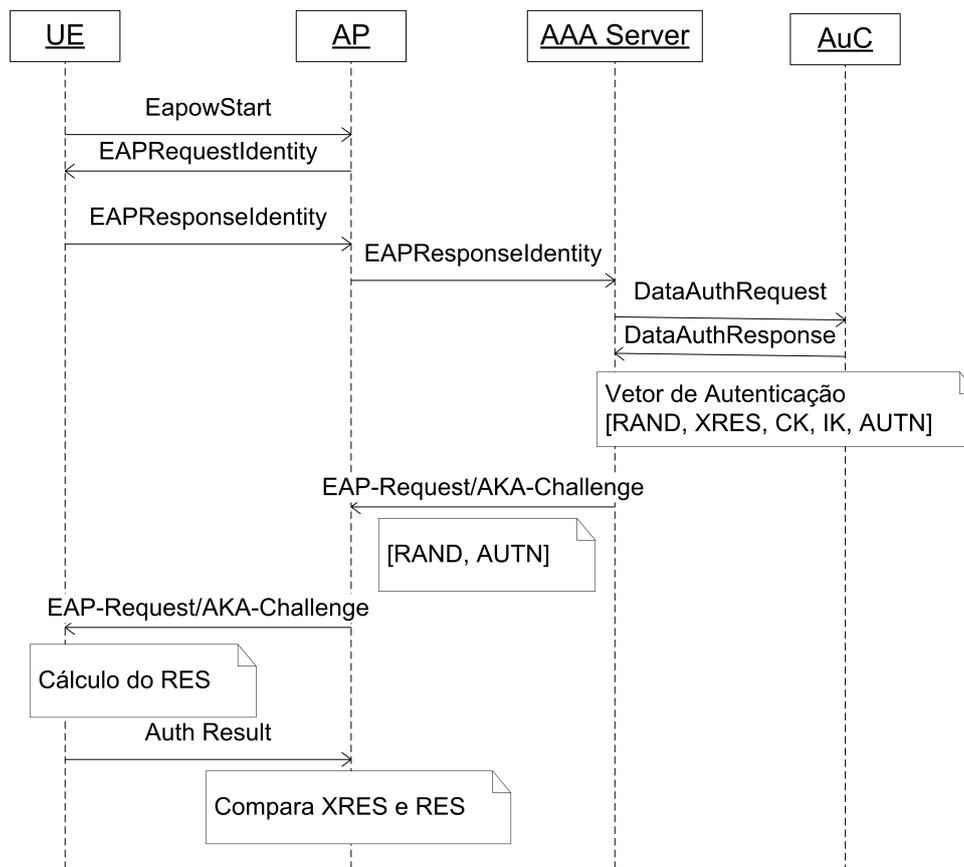


Figura 2.6 Processo de autenticação na rede IEEE 802.11 (adaptado de [4])

## 2.3 AS REDES DA PRÓXIMA GERAÇÃO

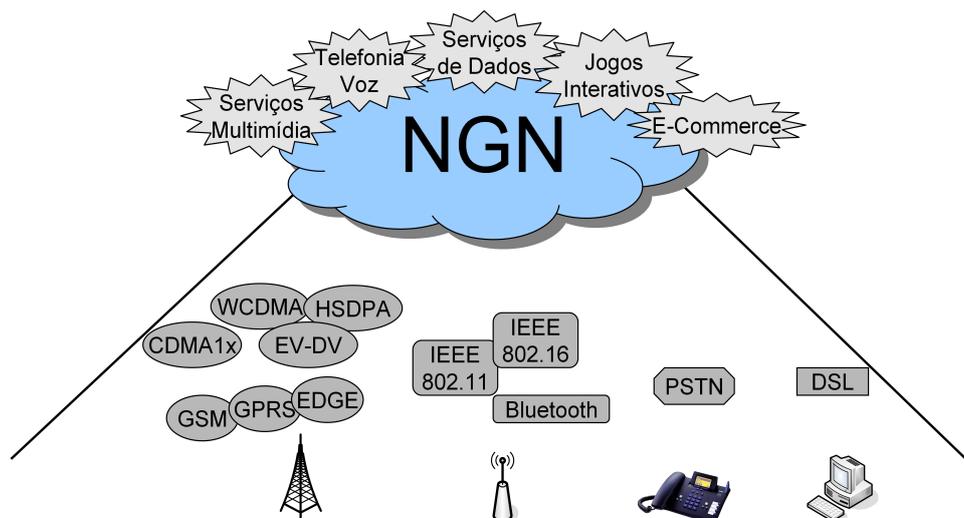
As redes da próxima geração vêm sendo bastante abordadas na literatura, por exemplo, algumas abordagens podem ser encontradas em [41] [42] [43].

A seguir, os principais fatores que devem ser considerados como critério para caracterizar uma NGN [44]:

- Transparência IP - Todos os elementos envolvidos na comunicação fim-a-fim devem suportar o protocolo IP tanto para a parte fixa como móvel da rede.
- Gerenciamento de Mobilidade - Característica importante para permitir o *roaming* entre as redes.
- Endereçamento - Todos os usuários devem possuir um único endereço, independente de sua localização corrente.

- Informação Personalizada - Selecionar e agregar informações de acordo com o perfil do usuário.
- Segurança e Gerenciamento dos Direitos Digitais – O conteúdo eletrônico deve possuir segurança no acesso e proteção dos dados através de restrições sobre quais operações um usuário autorizado pode tomar sobre esse conteúdo.

Tais fatores são essenciais para a convergência requerida pelas NGNs, as quais serão constituídas por um conjunto de tecnologias heterogêneas (e.g., redes locais sem fio, redes celulares, telefonia fixa, dentre outras) disponíveis ao usuário de forma transparente. A figura 2.7 apresenta uma abordagem das NGNs através da integração das redes celulares, WLAN, WPAN, redes fixas, telefonia, dentre outras. Alguns exemplos de serviços que serão fornecidos nesse tipo de rede também são apresentados. Dentre eles: serviços multimídia, jogos interativos, *e-commerce*, serviços de dados, além do serviço de voz.



**Figura 2.7** Redes das próxima geração

Em um ambiente de múltiplas tecnologias de acesso, como visto na Figura 2.7, o conceito de estar conectado da melhor forma possível é bastante relevante e um dos principais objetivos das redes 4G é proporcionar sempre a melhor conectividade (*Always Best Connected* - ABC) aos usuários móveis [45].

Para um usuário da rede, este conceito não significa apenas estar sempre conectado, mas também significa estar conectado através do melhor dispositivo disponível e

através da melhor tecnologia de acesso. A decisão depende de diferentes aspectos, tais como:

- Preferências pessoais;
- Capacidade do dispositivo;
- Necessidades da aplicação;
- Políticas da operadora;
- Disponibilidade dos recursos na rede, dentre outros.

Desse modo, diversas configurações e parâmetros podem ser empregados para a tomada de decisão, a qual deve fornecer uma solução ótima para o problema do ABC de cada usuário particular.

## CAPÍTULO 3

# INTEGRAÇÃO DO SISTEMA UMTS COM AS REDES IEEE 802.11

Um importante passo rumo ao acesso de sistemas integrados de forma contínua e sem rupturas é a integração das redes locais sem fio com as redes 3G. O 3GPP já vem se preocupando com isso e iniciou as especificações para esta integração. Em [10], o 3GPP define alguns princípios e cenários de integração. Existe ainda a preocupação com a segurança, na especificação em [16] há uma descrição dos aspectos necessários para prover um ambiente seguro na integração das redes 3G e WLAN. Entretanto, a segurança não é o foco desse trabalho.

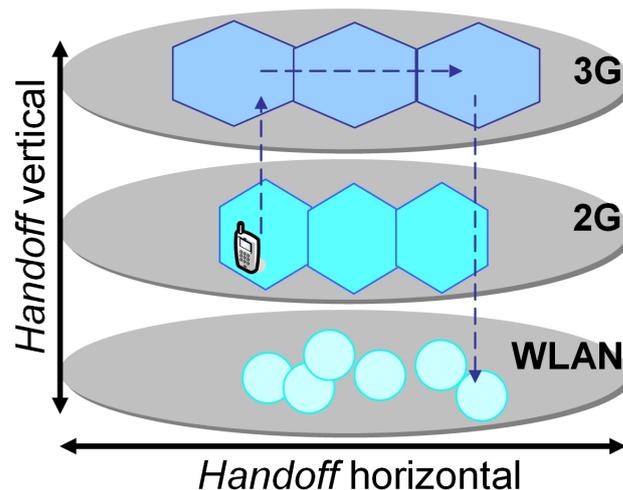
Neste capítulo, a Seção 3.1 descreve o procedimento de *handoff*. Em seguida, são apresentados os trabalhos relacionados, onde são abordados os níveis de integração definidos pelo 3GPP (Seção 3.2) e algumas arquiteturas de integração encontradas na literatura (Seção 3.3). Por fim, na Seção 3.4, os protocolos para o gerenciamento de mobilidade utilizados nesse trabalho são descritos.

### 3.1 O PROCEDIMENTO DE HANDOFF ENTRE AS REDES UMTS E IEEE 802.11

O processo de transferir o controle de um serviço em andamento de uma célula para outra dentro de um mesmo sistema ou entre sistemas diferentes é denominado *handoff*. A Figura 3.1 ilustra um exemplo de um processo de *handoff* vertical e horizontal. O *handoff* vertical ocorre quando um terminal móvel desloca-se entre duas redes diferentes (e.g., da rede UMTS para GSM/GPRS). Já o *handoff* horizontal é executado quando um terminal move-se de uma célula para outra dentro de um mesmo sistema sem fio. Entretanto, para que ocorra a integração dessas redes, é necessário também que o terminal opere em modo dual (i.e., o terminal deve possuir interfaces GSM/GPRS e UMTS).

Um aspecto importante do *handoff* é a duração do procedimento. Se o *handoff*

não ocorrer rapidamente, o nível de recepção do sinal no terminal móvel pode cair abaixo de um limiar aceitável e a execução do serviço pode terminar, o que não é desejável pelos usuários da rede nem pelas padronizações dos sistemas celulares 3G em diante, onde falhas de *handoff* não são toleradas.



**Figura 3.1** Handoff vertical e horizontal entre os sistemas 2G, 3G e WLAN

Um dos serviços a serem oferecidos nas redes 4G pelas operadoras de telefonia celular é a integração dos sistemas celulares aos *hotspots*, termo que designa um local público (e.g., aeroportos, universidades, shoppings, dentre outros), onde é oferecido serviço de rede local sem fio para usuários finais, fornecendo áreas com altas taxas de transmissão de dados. Com a integração dos sistemas celulares e as WLANs, os serviços e as funcionalidades dos sistemas celulares serão estendidos para o ambiente WLAN. Assim, os usuários passam a utilizar WLANs como uma tecnologia de acesso a dados por pacotes com taxas mais altas não suportadas pelos sistemas celulares.

Os *hotspots* podem ter proprietários diferentes. Um *hotspot* pode ser propriedade da própria operadora da rede celular que faz o gerenciamento da WLAN, como também pode estar dentro de uma empresa ou organização. Embora as WLANs tenham diferentes proprietários, os usuários das operadoras de celulares podem fazer uso dos *hotspots*. Entretanto, para isso são necessários acordos de *roaming* entre as operadoras e os proprietários das WLANs, pois é a operadora de celular que é responsável pelos processos de autenticação e contabilização.

Além da necessidade de acordos de *roaming*, como mencionado anteriormente, os usuários precisam de um equipamento que aceite os sistemas envolvidos. Nesse caso, é necessário um cartão com as funções de WLAN e sistema celular disponível (*dual mode card*). O Nokia N95 [46] é um exemplo desse tipo de dispositivo com funções UMTS/802.11b/g.

A Tabela 3.1 apresenta um resumo das principais características da rede UMTS e 802.11b. Percebe-se que as redes diferem bastante entre si (e.g., cobertura, taxa de transmissão de dados, custo de implantação) e que a desvantagem de uma rede é suprida pela outra rede, o que caracteriza o benefício da integração dessas redes para os usuários. Entretanto, por serem baseadas em tecnologias diferentes, a integração dessas redes é uma questão crítica.

Características	Redes	
	UMTS	IEEE 802.11b
Faixa de frequência	1900-2025 MHz	24 GHz
Cobertura	Total	Hotspot (50-100m)
Taxa de transmissão	Até 2 Mbps	Até 11 Mbps
Modulação	QPSK (Quadrature Phase Shift Keying) e QAM (Quadrature Amplitude Modulation)	CCK (Complementary Code Keying)
Timeslot	Tem diversas configurações, as quais dependem do canal utilizado	20us
Segurança	Alta	Baixa
Custo de implantação	Alto	Baixo

**Tabela 3.1** Características das Redes UMTS e IEEE 802.11

### 3.2 NÍVEIS DE INTEGRAÇÃO DO 3GPP

Em [10], o 3GPP define seis níveis de integração, e cada nível adquire as características do nível anterior, conforme apresentado na Tabela 3.2.

O primeiro nível de integração do 3GPP é o mais simples e refere-se à integração no nível de serviço e suporte ao cliente. O modelo de cobrança dos serviços oferecidos pelas redes deve unificar os débitos em uma única fatura. O suporte ao cliente é uma

integração apenas administrativa e não requer implicações técnicas na rede. Um exemplo desse nível de integração ocorre quando um usuário da rede 3G requisita o acesso aos serviços oferecidos por uma WLAN da operadora. A operadora então fornece um “login” e uma “senha” para que ele possa utilizar os serviços da WLAN, no entanto, não pode acessar os serviços 3G na WLAN.

Características	Níveis					
	1	2	3	4	5	6
Pagamento Único	X	X	X	X	X	X
Atendimento ao Cliente	X	X	X	X	X	X
Controle de acesso baseado nos sistemas 3GPP		X	X	X	X	X
Cobrança de acesso baseado nos sistemas 3GPP		X	X	X	X	X
Acesso aos serviços dos sistemas PS de uma WLAN			X	X	X	X
Continuidade do Serviço				X	X	X
Continuidade do Serviço com QoS					X	X
Acesso aos serviços dos sistemas CS de uma WLAN						X

**Tabela 3.2** Os Níveis de Integração do 3GPP e suas Características (adaptado de [10])

No segundo nível, o controle de acesso e cobrança baseado em sistemas 3G é realizado através do compartilhamento de informações de autenticação, autorização e cobrança. Nesse cenário, os usuários podem ter acesso à *Internet*, no entanto, não podem acessar os serviços 3G através da WLAN.

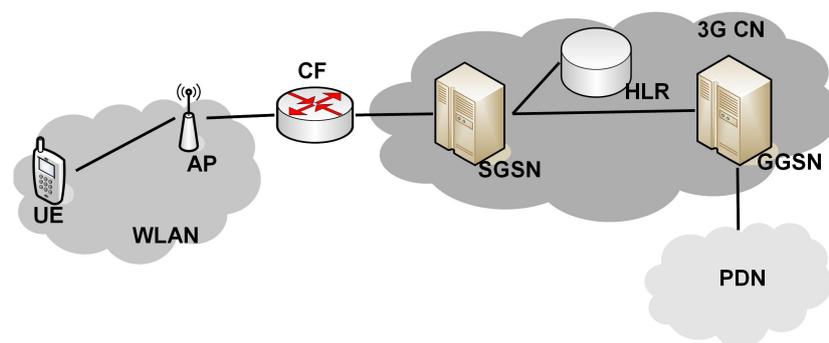
No terceiro nível, o usuário tem acesso aos serviços multimídia através da WLAN, no entanto, não tem suporte à continuidade do serviço com a mobilidade. Dessa forma, o usuário deve restabelecer a sessão ao acessar uma nova rede.

O quarto e o quinto níveis introduzem suporte à mobilidade para a continuidade dos serviços. Entretanto, no quarto nível, interrupções do serviço durante o *handoff* vertical podem ocorrer e esse processo pode ser perceptível ao usuário. No quinto nível é oferecido um acesso transparente aos serviços. Finalmente, o último nível permite ao usuário acessar os serviços baseados em comutação por circuitos, como ligações de voz, de uma WLAN.

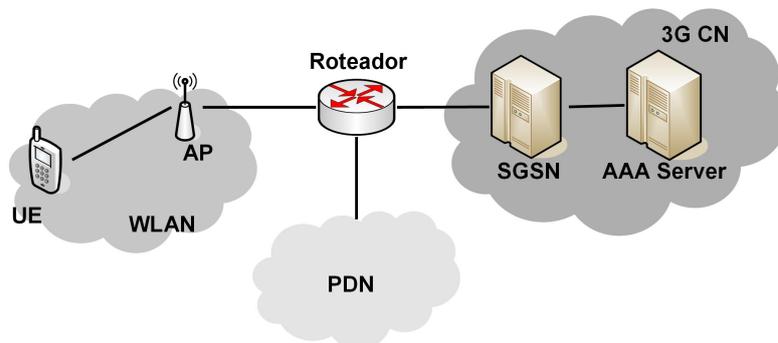
O foco deste trabalho está no nível 4 do 3GPP, onde é fornecido suporte a mobilidade na integração das redes 3G e WLAN.

### 3.3 ARQUITETURAS DE INTEGRAÇÃO

A literatura apresenta soluções para a criação de arquiteturas de integração das redes celulares e WLANs [5][6][7]. Por exemplo, o ETSI especifica duas arquiteturas de integração em [5]: *Tight Interworking* e *Loose Interworking*, que são apresentadas na Figura 3.2.



(a) Tight



(b) Loose

LEGENDA	
AAA: Authorization, Authentication and Accounting	GGSN: Gateway GPRS Support Node
AP: Access Point	PDN: Packet Data Network
CF: Cellular Function	SGSN: Serving GPRS Support Node
CN: Core Network	WLAN: Wireless Local Area Network
UE: User Equipment	

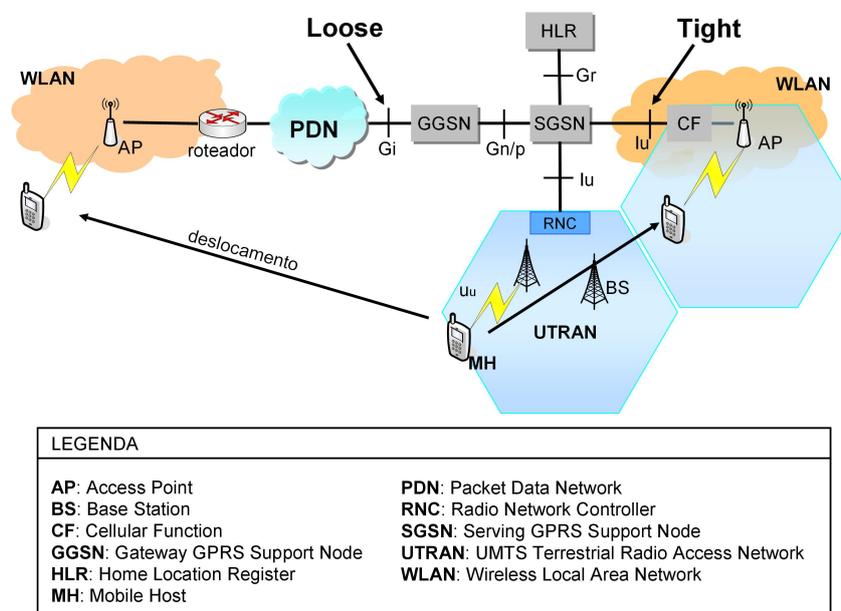
**Figura 3.2** Arquiteturas de integração definidas em [5]

Na arquitetura *Tight Interworking*, como mostra a Figura 3.2(a), a WLAN é conectada diretamente ao SGSN da mesma forma que outras redes de acesso (e.g., GPRS RAN). Esta arquitetura tem como principal vantagem o fato de reutilizar os mecanismos de autenticação e gerenciamento de mobilidade da rede celular. Para isso, ela necessita

de um elemento que entenda o funcionamento dos procedimentos da rede celular para poder interpretá-los para a WLAN. Entretanto, devido ao fato de a WLAN ser conectada diretamente ao SGSN, todo o fluxo de dados de uma WLAN passa através do CN para então alcançar as redes externas, podendo, dessa forma, sobrecarregar a rede. Com isso, há limitações na taxa de tráfego e desempenho da rede UMTS.

A arquitetura *Loose Interworking*, como mostra a Figura 3.2(b), não necessita que a WLAN se adapte às interfaces 3G, pois não reutiliza os processos de autenticação e mobilidade da rede celular. Este cenário apresenta um acoplamento mais leve e por isso menos complicado. No entanto, esta arquitetura, diferentemente da *Tight*, necessita de suporte externo para mobilidade, como, por exemplo, a utilização do *Mobile IP* [18][19].

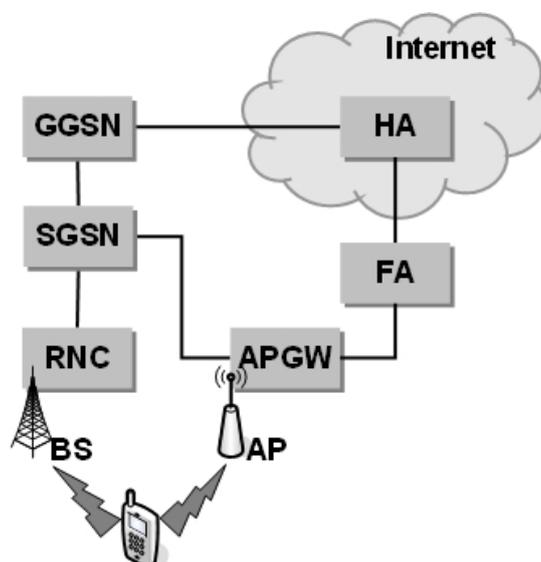
A Figura 3.3 apresenta o ponto de conexão das redes UMTS e 802.11 considerando a arquitetura *Tight* e *Loose*. O ponto de conexão da rede 802.11 à rede UMTS na arquitetura *Tight* ocorre através da interface  $I_u$  da rede celular (nesse caso, a mesma interface da rede de acesso UTRAN ao CN da rede UMTS). A rede 802.11 fica diretamente ligada ao SGSN e deve interpretar as funções da rede UMTS. Na Figura 3.3, esse processo está representado pelo CF (*Cellular Function*). O ponto de conexão da rede 802.11 à rede UMTS na arquitetura *Loose* ocorre através da interface  $G_i$ , a qual representa a interface da rede celular com as redes externas (e.g., *Internet*).



**Figura 3.3** Pontos de conexão das arquiteturas *Tight* e *Loose*

Em [6], é proposto um esquema híbrido (*Tight* e *Loose*) para a integração das

redes UMTS e WLAN, que pode ser observado na Figura 3.4. A entidade responsável pela integração é denominada APGW (*Access Point GateWay*), que comporta-se de forma diferenciada dependendo do tipo do tráfego. O APGW se torna um dispositivo *Tight* para tráfegos em tempo real e comporta-se como *Loose*, caso contrário. O protocolo de gerenciamento de mobilidade utilizado é o MIPv4. Entretanto, por comportar-se como *Tight*, as funções de controle da rede celular também devem ser implementadas na WLAN. Além disso, os autores propõem que a conexão UMTS continue ativa, mesmo quando um MS se deslocar para uma WLAN, o que ocasiona, a reserva desnecessária dos recursos de rádio UMTS.

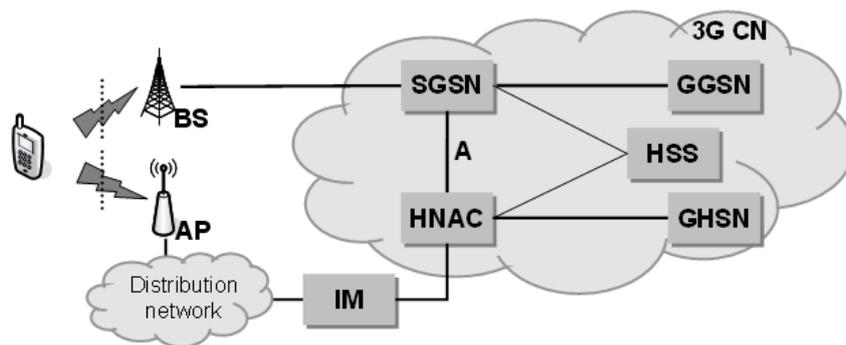


**Figura 3.4** Esquema híbrido *Tight* e *Loose* (adaptado de [6])

Em [7], é proposta uma arquitetura que adiciona elementos ao CN da rede GPRS, a qual é referente ao nível de integração 5 do 3GPP. Esta proposta pode ser observada na Figura 3.5. Dois novos componentes são adicionados ao CN da rede: HNAC (*Hotspot Network Area Controller*), que controla as WLANs, e o GHSN (*Gateway Hotspot Network Support Node*), que é responsável pelo gerenciamento do contexto e acesso à *Internet*. O GHSN tem funcionalidades similares ao GGSN.

Além das novas entidades adicionadas ao CN da rede GPRS, em [7], uma nova interface também deve ser adicionada para permitir a conexão entre o HNAC e o SGSN com o intuito de promover o *handoff* vertical. O usuário sempre está conectado a rede GPRS, que é considerada a rede primária e qualquer uso da WLAN é complementar. Como consequência, a interface de rádio GPRS deve estar sempre ativa, ocasionando a

reserva desnecessária de recursos. Para comprovar a proposta, os autores fizeram uma simulação utilizando o *Network Simulator* (NS). Entretanto, as simulações foram executadas separadamente e os tempos correspondentes de cada simulação foram armazenados para serem utilizados no cálculo do tempo total do *handoff*, o que dificulta o entendimento de como de fato ocorre o processo.



**Figura 3.5** Proposta de integração com novos componentes no CN da rede GPRS (adaptado de [7])

A solução proposta neste trabalho é baseada no nível 4 do 3GPP e na arquitetura *Loose*, a qual é definida em [5], no entanto, não é mencionado como gerenciar a mobilidade. Desse modo, a rede IEEE 802.11 não precisa implementar as funções de mobilidade da rede celular e o usuário não precisa permanecer com a interface de rádio UMTS ativa. Entretanto, é necessário um protocolo de gerenciamento de mobilidade para a integração das redes, conforme mencionado anteriormente. Os protocolos utilizados nesta dissertação são: o MIPv6 e o SIP.

### 3.4 GERENCIAMENTO DE MOBILIDADE

A arquitetura proposta neste trabalho é baseada na arquitetura *Loose*, onde não existe nenhuma função para executar o processo de *handoff* entre as redes UMTS e IEEE 802.11. Portanto, há a necessidade de suporte externo a mobilidade. Dentre os protocolos de mobilidade existentes na literatura [18][19][11][20][21], este trabalho utiliza o MIP versão (MIPv6) [19] e o SIP [11], detalhados nesta seção. Trabalhos referentes aos protocolos MIPv4 [18], TCP Migrate [21] e SCTP (*Stream Control Transmission Protocol*) [20] podem ser encontrados em [6][47][48][49].

### 3.4.1 Mobile IP – MIP

Um dos maiores desafios das redes IP é o suporte a mobilidade. *Mobile IP* [RFC 2002] é um protocolo da camada de rede desenvolvido pelo IETF para fornecer essa mobilidade. Dessa forma, os nós (*Mobile Node* - MN) podem se movimentar através de diferentes pontos de acesso mantendo a conectividade com outros nós na rede. Duas versões do MIP foram definidas de acordo com a versão do protocolo IP usada pela rede: MIPv4 [18] para as redes IPv4 e MIPv6 [19] para as redes IPv6.

No MIPv4 cada nó móvel pode ter dois endereços IPs com uma associação entre eles. Um deles é um endereço único atribuído na rede de origem e é denominado *Home Address* (HA) e o outro endereço, denominado *Care of Address* (CoA), é específico para a localização corrente atribuído em uma rede visitante.

O endereço de origem é um endereço estático, enquanto que, o CoA muda sempre que o MN muda de rede. As camadas de transporte e aplicação continuam utilizando o endereço de origem. Desse modo, essas camadas ficam inerentes ao conhecimento da mobilidade que o MIPv4 fornece aos MNs, significando transparência às camadas superiores através do CoA

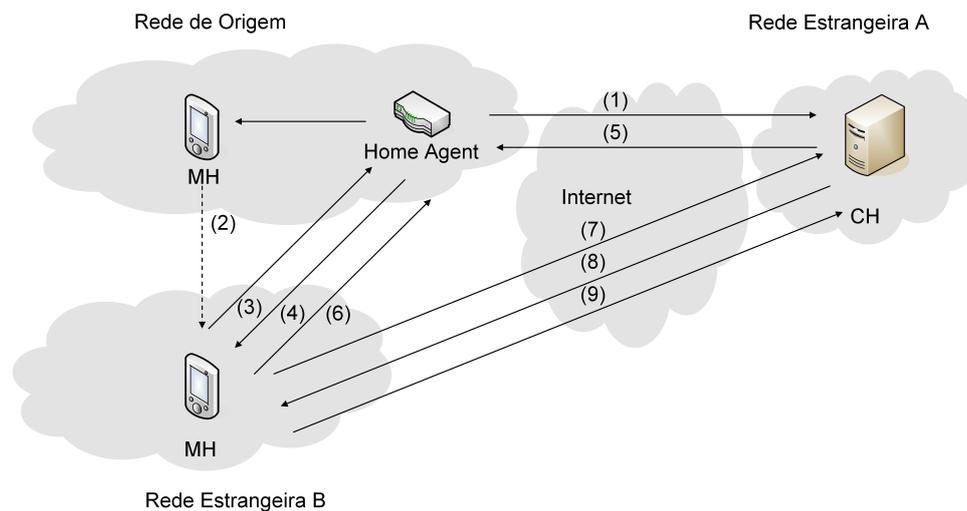
O MIPv4 tem limitações em termos de desempenho. Ao visitar uma nova rede, o MN registra-se com o agente estrangeiro (*Foreign Agent* - FA), que é um roteador localizado na rede onde o nó móvel está momentaneamente conectado. Quando existem pacotes de dados destinados ao MN, eles necessitam ser tunelados pelo agente de origem (*Home Agent* - HA), que também é um roteador, porém está localizado na rede de origem do MN. Com isso, todos os pacotes enviados para o MN são roteados através do HA adicionando um retardo na transmissão dos dados e aumentando a sobrecarga na rede. Este problema é denominado roteamento triangular [50].

O MIPv6 não apresenta tais problemas. Nesse protocolo não há a necessidade do FA, pois ele utiliza um mecanismo de otimização de rotas, onde cada nó armazena a associação entre o seu IP da rede de origem e o seu IP da nova rede (CoA), permitindo comunicações entre o MN e o nó correspondente (*Correspondent Node* - CN) sem ter que atravessar o HA. Dessa forma, o problema do roteamento triangular é evitado, reduzindo a quantidade de *overhead* gerado na rede quando comparado ao MIPv4.

A associação entre HA e o CoA (*binding*) é feita através de mensagens trocadas entre o MN e o HA. A associação, realizada por um processo denominado *Binding Re-*

*gistration*, inicia através do envio da mensagem *Binding Update* pelo MN ao HA, que responde com uma mensagem de *Binding Acknowledgement*.

A Figura 3.6 ilustra o gerenciamento de mobilidade com o MIPv6. Os passos enumerados na figura são explicados a seguir:



**Figura 3.6** Gerenciamento de mobilidade com o MIPv6

1. O usuário (i.e., MH) está alocado na Rede de Origem e comunica-se com o CH *Correspondent Host*, que está na Rede Estrangeira A;
2. O MH se movimenta e atinge a Rede Estrangeira B;
3. Ao obter um CoA, o MH envia a mensagem *Binding Update* para seu HA;
4. O HA responde com a mensagem *Binding Acknowledgement*;
5. Antes de o MH registrar seu novo endereço com o CH, o HA pode receber pacotes de dados vindos do CH para o MH;
6. Neste caso, o HA recebe os pacotes de dados e os encaminha para o MH;
7. O MH também registra seu novo endereço com o CH através da mensagem *Binding Update*;
8. O CH responde com a mensagem *Binding Acknowledgement*;

9. MH e CH se comunicam diretamente sem a necessidade de interação com o HA, diminuindo, dessa forma, o *overhead* gerado na rede pelo MIPv4 com o roteamento dos pacotes enviados para o MN através do HA.

Maiores detalhes quanto aos procedimentos MIPv4 e MIPv6 podem ser encontrados em [18] e [19], respectivamente.

### 3.4.2 Session Initiation Protocol – SIP

O Protocolo de Iniciação de Sessão (*Session Initiation Protocol* - SIP), definido pelo IETF na RFC 3261 [11], é um protocolo de sinalização desenvolvido para iniciar, modificar e terminar sessões multimídia através de redes IP. O SIP foi definido para se encaixar com outros padrões da *Internet* tais como: *Transmission Control Protocol* (TCP), *Transmission Layer Security* (TLS), *User Datagram Protocol* (UDP), IP, *Domain Name System* (DNS), dentre outros.

Existem quatro componentes principais na arquitetura SIP [51]:

- SIP *User Agent* (UA) é um terminal (telefones SIP ou *gateways* para outras redes) usado para estabelecer, modificar e finalizar sessões. Um UA pode agir como *User Agent Client* (UAC) e *User Agent Server* (UAS). UAC é uma entidade lógica que inicia uma requisição e o UAS, por outro lado, gera uma resposta à requisição SIP. Dessa forma, a arquitetura básica do SIP é cliente/servidor.
- SIP *Redirect Server* é um UAS que gera uma resposta fornecendo informações sobre o endereço do servidor para que o cliente possa redirecionar a requisição.
- SIP *Proxy Server* exerce o papel do UAC e do UAS, agindo como entidade intermediária entre outros UAs para rotear mensagens SIP ao destino.
- SIP *Registrar* é um UAS que processa requisições de registro SIP. Ele mantém uma tabela com informações da localização dos usuários SIP.

Cada mensagem SIP é formada por uma mensagem de requisição (*request*) e de uma resposta (*response*). Elas são escritas em formato de texto e podem conter descrições das sessões. Dessa forma, os participantes podem negociar os tipos de mídia e outros

parâmetros usados durante uma sessão. A Tabela 3.3 apresenta as principais mensagens SIP de requisição e resposta utilizadas durante uma sessão.

O endereçamento do usuário utilizado nas mensagens SIP é “id\_usuario@domínio”, onde “id\_usuario” é o nome do usuário ou número do telefone, e “domínio” é o nome do domínio ou um endereço numérico.

Quando um MH muda de rede (i.e., executa o *handoff* vertical) durante uma sessão em andamento, ele deve enviar uma mensagem de re-INVITE para o CH usando o mesmo identificador de sessão e deve indicar o novo endereço IP, onde as futuras mensagens SIP devem ser entregues.

A Figura 3.7 descreve um exemplo de mensagem re-INVITE. Nesse exemplo, o usuário móvel “Diana” executa o *handoff* vertical durante uma sessão com o usuário “Marcos”, então envia uma mensagem de re-INVITE para “Marcos” indicando onde deseja receber as futuras mensagens. O novo endereço de “Diana” é indicado no campo “*Contact*”. Esse processo se repete sempre que um dos participantes da sessão muda de uma rede para outra.

```
INVITE sip:marcos@lia.ufc.br SIP/2.0
Via: SIP/2.0/UDP great.ufc.br;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Marcos <sip:marcos@lia.ufc.br>
From: Diana <sip:diana@lia.ufc.br>;tag=1928301774
Call-ID: a84b4c76e66710@lia.ufc.br
CSeq: 314159 INVITE
Contact: <sip:diana@great.ufc.br>
Content-Type: application/sdp
Content-Length: 142
```

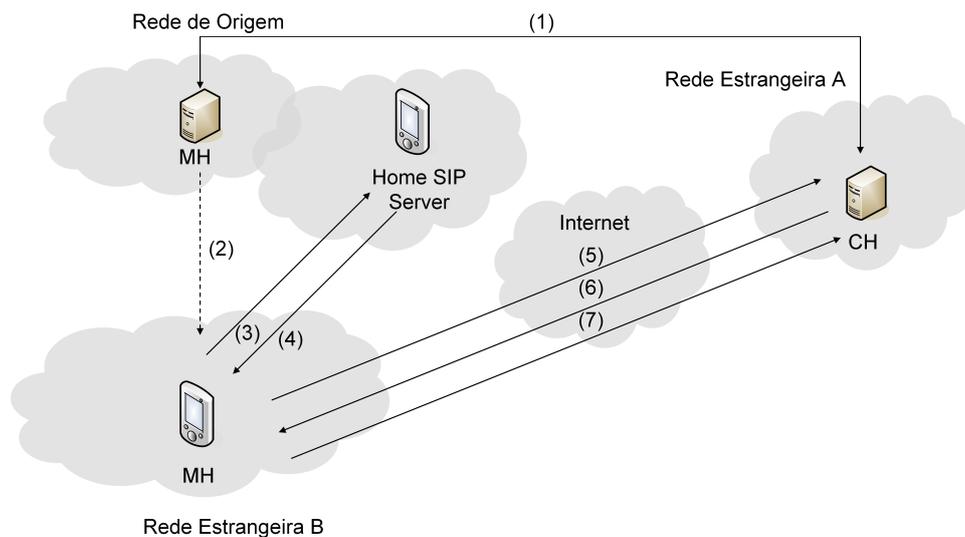
**Figura 3.7** Mensagem SIP *re-INVITE*

A Figura 3.8 ilustra o gerenciamento de mobilidade com o SIP. Os passos enumerados na figura são explicados a seguir:

1. O usuário (i.e., MH) está alocado na Rede de Origem e comunica-se com o CH, que está na Rede Estrangeira A;
2. O MH se movimenta e atinge a Rede Estrangeira B;
3. O MH envia uma mensagem para o servidor SIP da Rede de Origem para atualizar sua localização. Dessa forma, quando novas requisições de *Invite* chegarem, poderão ser redirecionadas corretamente;

Mensagem SIP		Descrição
Requisição	Invite	Convida um usuário a estabelecer uma sessão SIP
	Register	Registra um usuário em um servidor
	Ack	Confirma uma resposta final
	Bye	Termina uma sessão
	Cancel	Cancela uma requisição SIP
	Options	Consulta os servidores sobre o perfil do usuário
	Info	Transmite informações de controle da sessão
	Subscribe	Checa o estado corrente de um usuário remoto
	Notify	Notifica ao usuário a ocorrência de um evento, que foi requerido anteriormente pelo método <i>subscribe</i>
	Update	Atualiza os parâmetros de uma sessão
Message	Transfere mensagens instantâneas ( <i>Instant Messages - IM</i> )	
Resposta	1XX	Mensagens informativas (por exemplo, 100 – <i>trying</i> e 180 – <i>ringing</i> )
	2XX	Requisição satisfeita com sucesso (por exemplo, 200 – OK)
	3XX	Encaminhamento de chamada, dessa forma, a requisição deve ser dirigida para outro servidor (por exemplo, 302 – <i>temporarily moved</i> e 305 – <i>use proxy</i> )
	4XX	Erro (por exemplo, 403 – <i>forbidden</i> )
	5XX	Erro no servidor (por exemplo, 500 – <i>Server Internal Error</i> e 501 – <i>not implemented</i> )
	6XX	Falha global (por exemplo, 606 – <i>Not Acceptable</i> )

**Tabela 3.3** As principais mensagens SIP de requisição e resposta (adaptado de [11])



**Figura 3.8** Gerenciamento de mobilidade com o SIP

4. O servidor SIP atualiza a localização e envia uma mensagem de reconhecimento;
5. Em seguida, o MH envia uma nova requisição de *Invite* para o CH utilizando o identificador da sessão anterior. Esta requisição contém o novo endereço do MH para que ele possa receber as mensagens SIP;
6. O CH envia uma mensagem de reconhecimento ao MH;
7. O MH e o CH continuam a comunicação.

Vale ressaltar que o 3GPP utiliza na arquitetura do UMTS, um subsistema para prover serviços multimídia, o qual utiliza o SIP como protocolo de sinalização.

### ***IP Um exemplo de utilização do SIP***

O 3GPP especifica o *IP Multimedia Subsystem* (IMS) para prover os serviços multimídia para UMTS. O IMS utiliza o SIP como protocolo de sinalização e controle de sessão dos serviços em tempo real, fornecendo aplicações multimídia às redes NGN. As principais funções do IMS têm como finalidade permitir a autenticação e a autorização dos usuários de redes móveis e fixas, QoS, *roaming*, segurança e a integração de serviços.

No IMS, os serviços multimídia são gerenciados pela função controladora de sessão da chamada (*Call Session Control Function – CSCF*), que é responsável também pelo

tratamento das requisições SIP. São definidos três tipos de CSCFs: *Proxy-CSCF* (P-CSCF), *Interrogating-CSCF* (I-CSCF) e *Serving-CSCF* (S-CSCF).

O P-CSCF é o primeiro contato para um usuário SIP obter acesso à rede IMS. Todo tráfego de sinalização SIP de/para um UE passa pelo P-CSCF. As suas principais funções são [52]:

- Enviar as solicitações de registro SIP (*SIP Register*) para o I-CSCF baseado no nome do domínio de origem fornecido pelo UE na requisição;
- Coordenar, com a rede de acesso, o controle de recursos e qualidade das chamadas/sessões (QoS); e
- Enviar as solicitações e as respostas SIP para o UE.

O I-CSCF é o ponto de contato de uma operadora de rede para todas as conexões destinadas a um assinante da rede desta operadora, ou para um usuário visitante em uma rede, tendo como funções principais [52]:

- Comunicar-se com a base de dados (*Home Subscriber Server – HSS*) para obter o endereço do S-CSCF que está servindo um usuário específico;
- Enviar solicitações ou respostas SIP para o S-CSCF; e
- Rotear uma requisição SIP recebida de outra rede em direção ao S-CSCF.

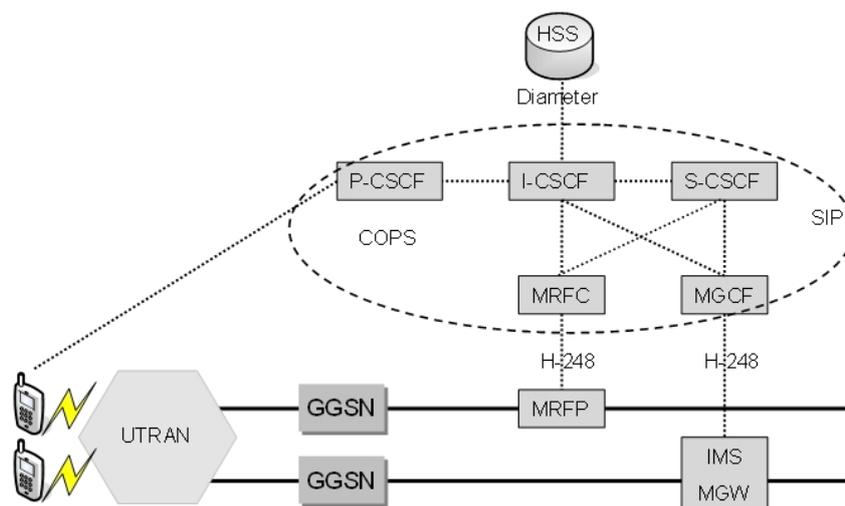
Já o elemento S-CSCF fornece os serviços de controle da sessão e de registro para um usuário. O S-CSCF é responsável pelas seguintes funções [52]:

- Autenticar usuários pelo método de autenticação IMS e definir o acordo de chaves (AKA);
- Fazer o download das informações do usuário e dos dados relacionados aos serviços através do HSS durante um registro ou quando controla um pedido de um usuário não registrado; e
- Supervisionar o tempo de registro dos usuários.

A Figura 3.9 ilustra uma visão geral da arquitetura do UMTS/IMS. Percebe-se a organização em duas redes: a rede de sinalização e a de transporte de dados. Como mencionado, a rede de sinalização é composta por um conjunto de nós de controle (e.g., P-CSCF, I-CSCF, S-CSCF), no entanto, também existem outras entidades relacionadas. Por exemplo, o MGCF (*Media Gateway Control Function*) conecta as redes baseadas em circuito através do IMS-MGW (*IMS Media Gateway*) e o MRFC (*Media Resource Function Processor*) controla o fluxo de mídia do elemento MRFP (*Media Resource Function Processor*). O HSS é uma base de dados centralizada contendo os dados dos usuários, como dados de autenticação e o perfil do usuário.

Além do SIP, como mostrado na Figura 3.9, outros protocolos também são utilizados no IMS:

- COPS (*Common Object Policy Service*) [53] - para administração, configuração e aplicação de políticas;
- *Diameter* [54] - para buscar registros de usuários no banco de dados; e
- MEGACO (*Media Gateway Control Protocol* [55]) - também conhecido como H.248, serve de interface com redes baseadas em circuito.



**Figura 3.9** Arquitetura do UMTS/IMS

Para que possam trabalhar juntos, esses protocolos são “combinados” com o SIP, através de extensões, onde uma mensagem de um protocolo é responsável por disparar as

mensagens do outro, e ainda alguns parâmetros e cabeçalhos são mapeados de um para o outro.

Na Tabela 3.4 observa-se as interfaces envolvidas como ponto de conexão entre as principais entidades do IMS.

Interface	Entidades Envolvidas	Descrição
$G_m$	UE, P-CSCF	Utiliza o SIP como protocolo na troca de mensagens entre UE e P-CSCF
$M_w$	P-CSCF, I-CSCF, S-CSCF	Utiliza o SIP como protocolo na troca de mensagens entre os CSCFs
$C_x$	I-CSCF, S-CSCF, HSS	Utiliza o Diameter como protocolo na troca de mensagens entre as entidades envolvidas
$D_x$	I-CSCF, S-CSCF, SLF	Utiliza o Diameter como protocolo na troca de mensagens entre as entidades envolvidas para buscar o HSS correspondente

**Tabela 3.4** Interfaces utilizadas entre as entidades IMS

### *Exemplo de Registro IMS*

A Figura 3.10 mostra os procedimentos executados durante o registro IMS e a Figura 3.11 mostra o formato da mensagem *Register*.

Como mostrado na Figura 3.10, antes do usuário iniciar o procedimento de registro IMS, é necessário ativar o contexto PDP para estabelecer uma conexão lógica com a rede. Esse procedimento é iniciado pelo UE, que recebe um endereço IP e faz a reserva dos recursos de rádio. Após o estabelecimento dessa conexão, o UE está habilitado para transmitir e receber pacotes IP.

Em seguida, o UE precisa descobrir o endereço do P-CSCF, que é o primeiro ponto de entrada para todas as mensagens SIP, para, então, poder enviar mensagens SIP. Para descobrir o endereço do P-CSCF, o UE pode fazer uma requisição ao GGSN durante o estabelecimento do contexto PDP. O GGSN irá retornar o endereço IPv6 de um P-CSCF na resposta do contexto PDP (*PDP Context Response*).

O S-CSCF, ao receber a mensagem *Register* de um UE, identifica o usuário pela PrUI (*Private User Identity*) e obtém o vetor de autenticação (AV) no HSS. Baseado nos dados do AV, ele envia um campo *WWW-Authenticate* na resposta 401 (*Unauthorized*), como mostrada na Figura 3.12.

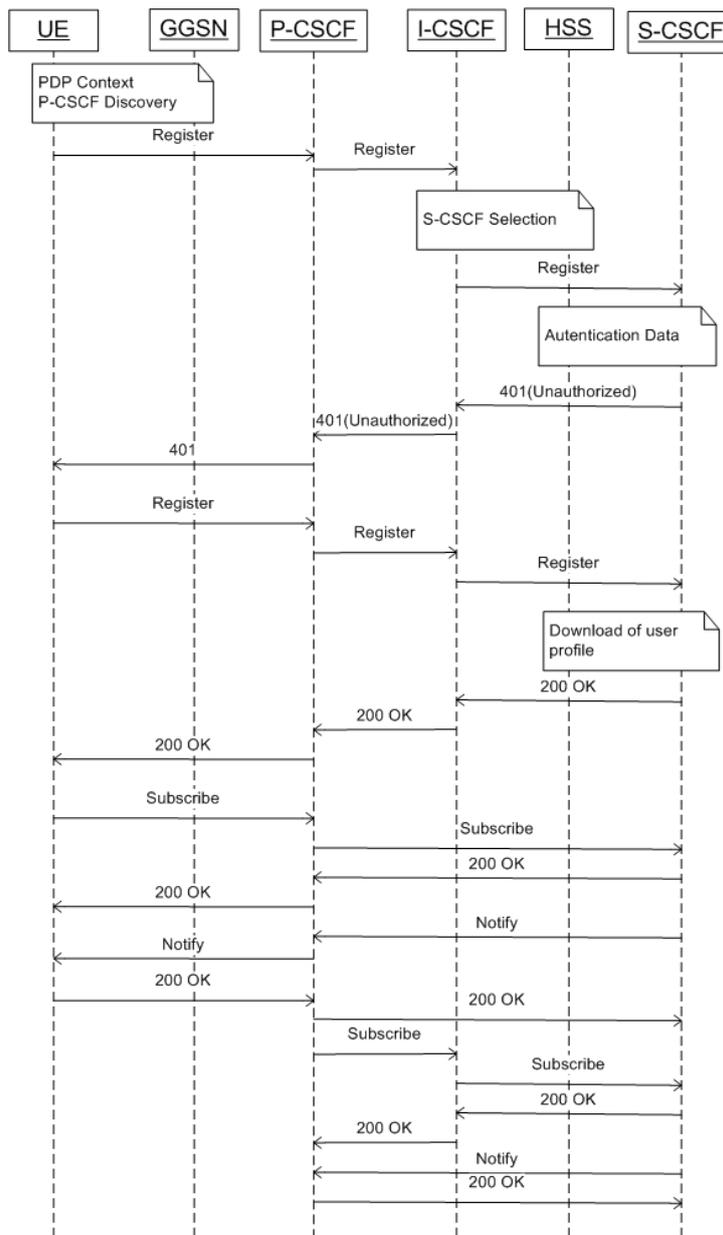


Figura 3.10 Mensagem de registro IMS (adaptado de [8])

```

INVITE sip:ufc.br SIP/2.0
Via: SIP/2.0/UDP [5555::1:2:3:4];branch=z9hG4bK776asdhds
Max-Forwards: 70
To: sip:diana@ufc.br
From: <sip:diana@ufc.br>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 25 REGISTER
Contact: <sip: [5555::1:2:3:4]>, EXPIRES=600000
Content-Length: 0
    
```

Figura 3.11 Formato da mensagem de registro IMS (adaptado de [8])

```
SIP/2.0/ 401 Unauthorized
WWW-Authenticate: Digest realm="ufc.br",
nonce=A34Cm+Fva37UYWpGNB34JP, algorithm=AKAv1-MD5,
ik="0123456789abcdeabcde0123456789",
ck=9876543210abcdeabcde9876543210"
```

**Figura 3.12** Formato da mensagem 401 *Unauthorized* (adaptado de [8])

O campo *nonce* contém os parâmetros RAND e AUTN, e o campo *algorithm* possui o valor “AKAv1-MD5”, que identifica o mecanismo AKA, e também os campos “ik” e “ck”, contendo as chaves de integridade e cifragem. Esses campos são definidos em [56].

### *Desafios do SIP na Integração*

A integração das redes, permitindo o acesso heterogêneo aos serviços 3G, influencia a criação de novos serviços. Entretanto, um dos principais desafios é propor uma arquitetura para acesso WLAN aos serviços multimídia compatíveis com o padrão 3GPP e que pode ser desenvolvido pelas operadoras.

Conforme mencionado anteriormente, o protocolo usado pelo 3GPP durante a negociação da sessão dos serviços multimídia é o SIP. Entretanto, a integração das redes utilizando o SIP, pode causar alguns danos devido ao protocolo SIP ser extensível. Isso significa que o protocolo SIP utilizado pelo 3GPP pode apresentar extensões que não são aplicáveis ao SIP definido pelo IETF [12].

Na Tabela 3.5, são relatadas as principais diferenças encontradas na comparação entre o SIP definido pelo IETF e o SIP que deve ser implantado pelo 3GPP [12].

## 3.5 COMPARAÇÃO ENTRE OS PROTOCOLOS SIP E MIPV6

A Tabela 3.6 apresenta um resumo das características dos protocolos de mobilidade descritos neste trabalho e utilizados para suporte e mobilidade na integração das redes UMTS e IEEE 802.11.

Como mencionado anteriormente, o MIP e o SIP atuam em camadas diferentes. O MIP é um protocolo da camada de rede, e o SIP da camada de aplicação. Dessa forma, quanto a transparência, o MIP oferece transparência para as camadas de transporte e aplicação, enquanto o SIP oferece transparência relativa ao usuário.

SIP IETF	SIP 3GPP
Características Gerais	
Cabeçalhos e corpos da mensagem fim-a-fim podem ser cifrados usando S/MIME	Cabeçalhos e corpos da mensagem fim-a-fim não podem ser cifrados usando S/MIME, desde que proxies intermediários tem que lê-los e atuar conseqüentemente
Autenticação UA-proxy é opcional	Não é permitida autenticação UA-proxy
Características da Transação SIP	
Os proxies não devem filtrar os cabeçalhos Record-Route ou Route. Além disso, record-routing é opcional	P-CSCF filtra os cabeçalhos Record-Route ou Route para o UE (com o objetivo de esconder detalhes da topologia da rede do usuário). Além disso, record-routing é obrigatório para proxies CSCFs
Um proxy não deve iniciar um procedimento de encerramento de sessão	S-CSCF e P-CSCF devem implementar o procedimento de encerramento de sessão
Suporte a Extensões	
Mecanismo de Privacidade [57] é opcional	Mecanismo de Privacidade [57] é obrigatório
Compressão SIP [58] é opcional para UE e proxy	Compressão SIP [58] é obrigatório para UE e P-CSCF
Acordo de Mecanismo de Segurança [59] é opcional para UE e proxy	Acordo de Mecanismo de Segurança [59] é obrigatório para UE e P-CSCF

**Tabela 3.5** Comparação do SIP IETF x SIP 3GPP (adaptado de [12])

Em relação ao protocolo de transporte utilizado, tanto no caso do MIP quanto do SIP podem ser utilizados os protocolos TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*). No entanto, em [60][8] mostram que no SIP, o protocolo UDP deve ser o principal protocolo de transporte utilizado. Em [61] [60], é descrito uma abordagem alternativa, onde o SIP utilizando o UDP em conjunto com o MIP utilizando o TCP é uma configuração capaz de melhorar o desempenho desses protocolos.

Como citado anteriormente, em relação à infra-estrutura, no caso do MIP é necessário o *Home Agent* na rede de origem, enquanto o SIP requer um servidor SIP na rede de origem para então prover o gerenciamento da mobilidade. Os dispositivos utilizados pelos usuários devem possuir de suportar tais protocolos.

Características	Protocolo	
	MIPv6	SIP
Camada atuante	Rede	Aplicação
Transparência	Sim	Sim
Protocolo de Transporte	TCP/UDP	TCP/UDP
Infra-estrutura Necessária	<i>Home Agent</i>	Servidor SIP
Características dos Dispositivos	MH deve implementar MIPv6	MH tem que ser um agente SIP

**Tabela 3.6** Comparação SIP x MIPv6

## CAPÍTULO 4

# MOB4LOOSE: UMA EXTENSÃO DA ARQUITETURA LOOSE INTERWORKING BASEADA NO NÍVEL 4 DO 3GPP

Este capítulo apresenta a proposta de integração das redes UMTS e IEEE 802.11. Na Seção 4.1, são abordadas as principais características da proposta. Em seguida, a Seção 4.2 descreve a arquitetura da proposta que é uma extensão da arquitetura *Loose Interworking* com suporte a mobilidade, o qual refere-se ao nível 4 do 3GPP. Na Seção 4.3 é apresentado o comportamento funcional através dos diagramas de seqüência. Por fim, a Seção 4.4 descreve os principais blocos e processos da especificação em SDL, que foi gerada a partir dos diagramas de seqüência.

### 4.1 CARACTERÍSTICAS PRINCIPAIS

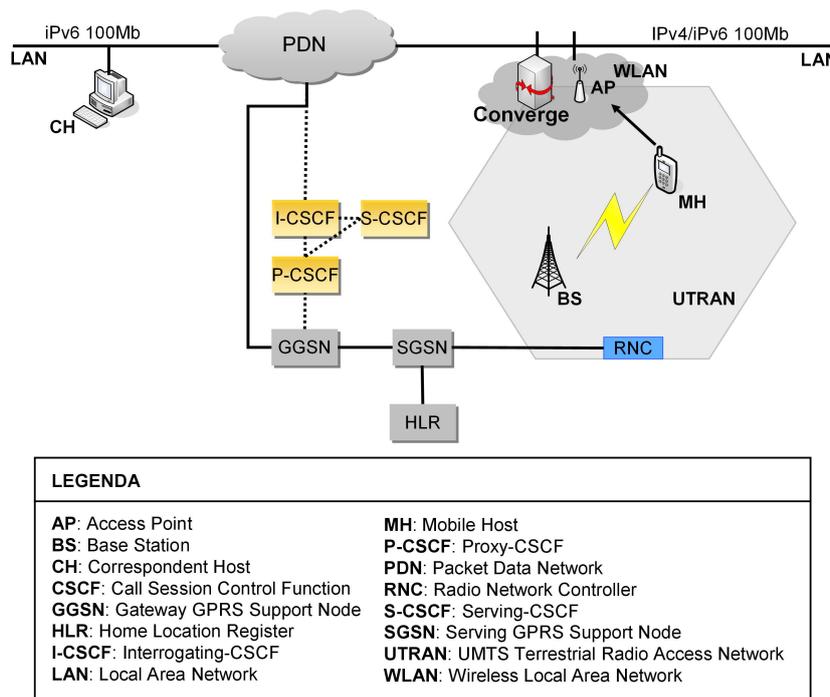
A solução proposta neste trabalho, denominada *Mob4Loose*, é uma extensão da arquitetura *Loose*, que define a arquitetura de integração conforme detalhada no Capítulo 3, porém, não especifica como gerenciar a mobilidade. Além disso, a proposta é baseada no nível 4 do 3GPP, que oferece suporte à mobilidade na integração das redes 3G e WLAN.

Por ser baseada na arquitetura *Loose*, a proposta necessita de suporte externo a mobilidade. Este trabalho utiliza os protocolos MIPv6 e SIP, levando em consideração as seguintes premissas:

- O MH e o CH devem ser agentes SIP para então ter o SIP como protocolo de mobilidade; e
- O MH e o CH devem ser agentes MIPv6 para então ter o MIP como protocolo de mobilidade.

## 4.2 ARQUITETURA

A Figura 4.1 ilustra a arquitetura do *Mob4Loose*, onde cada rede funciona de forma independente da outra, já que, diferentemente da arquitetura *Tight*, a WLAN não necessita se adaptar às interfaces 3G e, portanto, não reutiliza os processos de autenticação e mobilidade da rede celular.



**Figura 4.1** Integração das redes UMTS e WLAN

Na Figura 4.1, observa-se a rede IEEE 802.11 ligada a uma rede fixa local (*Local Area Network* - LAN) de 100Mb, o CH em uma outra LAN, o CN da rede UMTS, os servidores IMS (P-CSCF, I-CSCF e S-CSCF), que são os servidores SIP responsáveis pela sinalização, e o HLR, que é a principal base de dados e contém as informações dos assinantes.

A figura também ilustra uma entidade funcional proposta neste trabalho, denominada *Converge*, que é localizada no *gateway* de acesso à rede IEEE 802.11. Esta entidade provê funcionalidades adicionais às abordagens de gerenciamento de mobilidade propostas. Essas funcionalidades serão descritas na Seção 4.3.

Neste trabalho considera-se o protocolo IPv6, no entanto, como nem todas as redes operam com IPv6, deve-se considerar que os pacotes IPv6 podem ser tunelados

como IPv4, permitindo que redes IPv6 se comuniquem mesmo que a conexão entre elas seja feito em IPv4 [62].

Os usuários podem se deslocar entre as duas redes, desde que possuam dispositivos (i.e., MHs) capacitados para isso (módulos: UMTS, IEEE 802.11, MIP e SIP) e que seja permitido pelo seu perfil de usuário.

### 4.3 COMPORTAMENTO FUNCIONAL

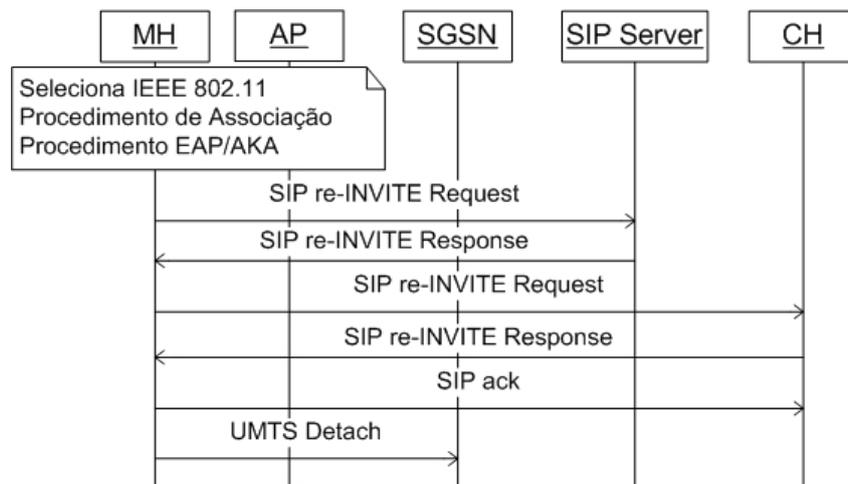
A Técnica de Descrição Formal (TDF) *Message Sequence Chart* - MSC (i.e., Diagramas de Seqüência), definida pelo ITU-T na norma técnica Z.120 [23], é usada para descrever o comportamento funcional da proposta.

Este comportamento já vem sendo descrito ao longo deste trabalho. No Capítulo 2 foram apresentados os diagramas de autenticação nas redes UMTS e IEEE 802.11 que também serão considerados nesta proposta. Mesmo a segurança não sendo foco desse trabalho, os processos de autenticação nas redes UMTS e IEEE 802.11 são considerados, pois sempre que o usuário se desloca para uma nova rede, o processo de autenticação é necessário.

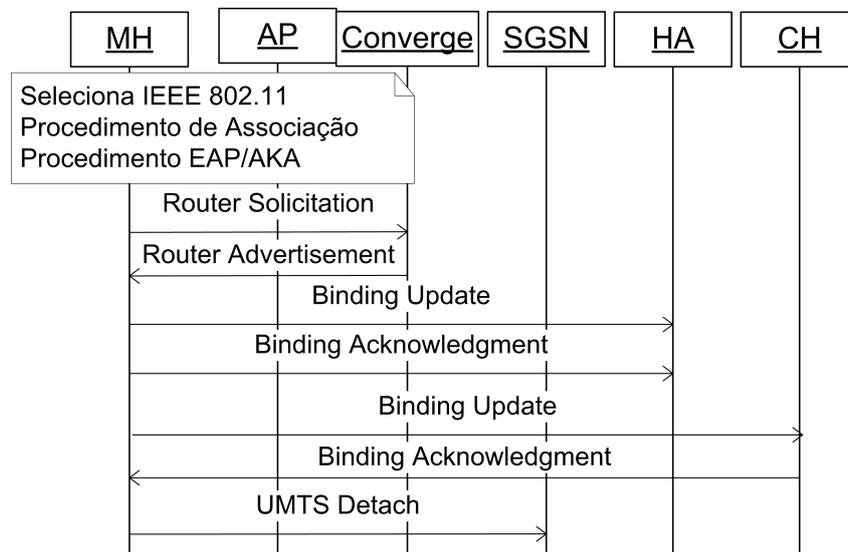
O processo de *handoff* entre redes heterogêneas é dividido em duas fases: o processo de decisão do *handoff*, onde o MH ou a rede decide quando executar o *handoff*, e a execução do *handoff*, onde após tomada a decisão, ocorre a execução do procedimento. Detalhes sobre o procedimento de *handoff* podem ser encontrados em [63].

Os protocolos MIPv6 e SIP são utilizados para suportar a execução do *handoff* vertical entre as redes UMTS e IEEE 802.11. Dessa forma, quatro cenários de sucesso, que são mostrados na Figura 4.2, Figura 4.3, Figura 4.4 e Figura 4.5, respectivamente, são considerados nessa proposta, a seguir:

- *handoff* da rede UMTS para a rede IEEE 802.11 com o SIP;
- *handoff* da rede UMTS para a rede IEEE 802.11 com o MIPv6;
- *handoff* da rede IEEE 802.11 para a rede UMTS com SIP; e
- *handoff* da rede IEEE 802.11 para a rede UMTS com MIPv6.



**Figura 4.2** Troca de mensagens durante o *handoff* da rede UMTS para 802.11 com SIP



**Figura 4.3** Troca de mensagens durante o *handoff* da rede UMTS para 802.11 com MIPv6

A troca de mensagens durante o *handoff* da rede UMTS para a rede IEEE 802.11 com o SIP como protocolo de gerenciamento de mobilidade é apresentada na Figura 4.2. O processo inicia com a detecção de uma rede IEEE 802.11. O usuário decide utilizar a rede local sem fio e, então, ele seleciona no seu dispositivo móvel a mudança para essa rede de acesso. Em seguida, o MH e o AP iniciam o processo de associação e autenticação baseado na especificação IEEE 802.1X [40]. O procedimento de autenticação, que permite que um dispositivo móvel UMTS seja autenticado em ambientes WLANs, denominado EAP-AKA [4], é observado na Figura 2.6. Este processo é recomendado em [64], como o protocolo de autenticação a ser utilizado na arquitetura *Loose*.

Após o procedimento de autenticação com a rede local, o MH se registra com o servidor SIP para atualizar a sua nova localização e, finalmente, envia a requisição de *dettach* da rede UMTS, liberando os recursos de rádio UMTS. Em seguida, o MH convida o CH para continuar a sessão que estava em andamento. Para tanto, o MH envia uma nova mensagem de *SIP re-INVITE Request* para o CH usando o mesmo identificador de sessão e deve indicar o novo endereço IP onde as futuras mensagens SIP devem ser entregues. Ao obter a mensagem *SIP re-INVITE Response*, o fluxo de dados entre o MH e o CH é restabelecido. .

A troca de mensagens durante o *handoff* da rede UMTS para a rede 802.11 com o MIPv6 é mostrada na Figura 4.3. Após o procedimento de autenticação com a rede IEEE 802.11, inicia-se o processo de registro MIP com seu HA através da mensagem *Binding Update*, onde o MH informa sua nova localização. O HA responde com a mensagem *Binding Acknowledgment* para indicar que recebeu a mensagem contendo a nova localização. Em seguida, inicia-se o processo de atualização com o CH, enviando o *Binding Update* e recebendo o *Binding Acknowledgment*.

O *handoff* da rede IEEE 802.11 para a rede UMTS com o SIP como protocolo de gerenciamento é mostrado na Figura 4.4, que é semelhante ao processo citado anteriormente. O processo de autenticação na rede UMTS é mostrado na Figura 2.2. As redes UMTS utilizam o processo de autenticação AKA, que provê autenticação mútua.

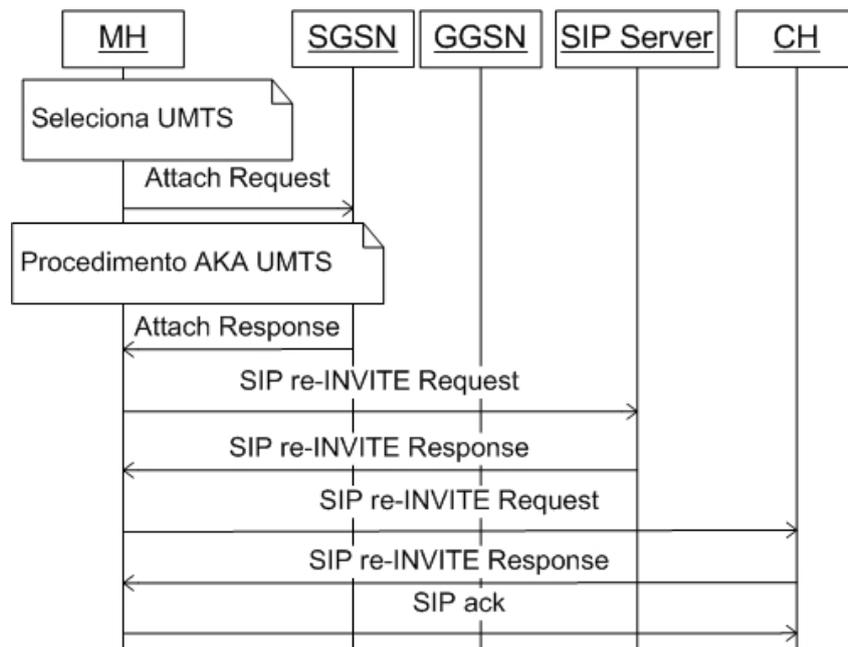
Após o processo de autenticação, o MH atualiza sua localização com o servidor SIP e o CH através das mensagens *SIP re-INVITE Request* e *SIP re-INVITE Response* para, então, continuar a sessão de dados.

A Figura 4.5 ilustra o *handoff* da rede IEEE 802.11 para a rede UMTS com o MIPv6 como protocolo de gerenciamento. Para atualizar seu endereço corrente, o MH troca mensagens (*Binding Update* e *Binding Acknowledgment*) com o HA e o CH, processo que foi explicado anteriormente.

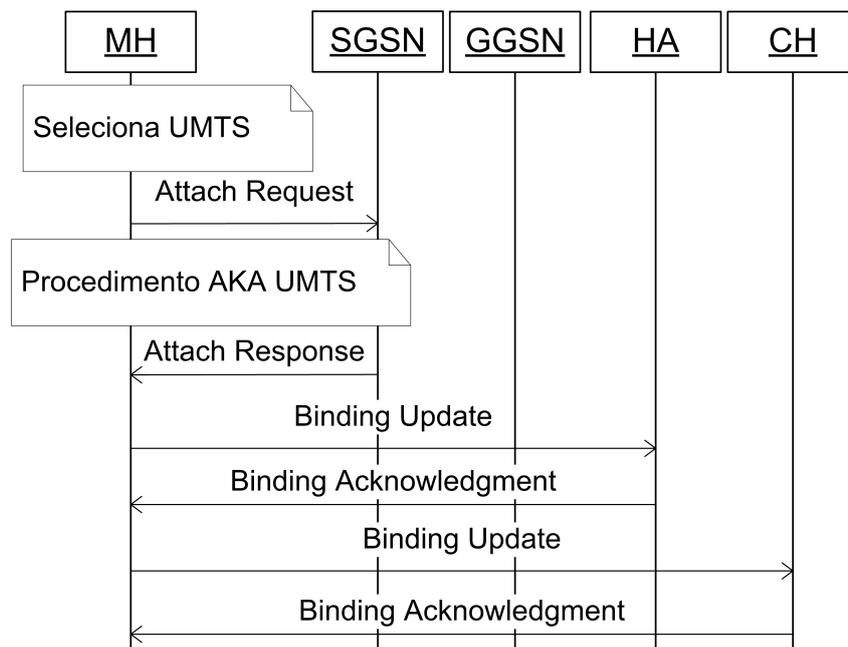
### ***Funcionalidades Adicionais***

No *gateway* de acesso à rede IEEE 802.11 foi inserida a entidade funcional *Converge*, que quando implantada deve possuir interfaces para as redes UMTS, 802.11 e *Ethernet*, para prover as características adicionais explanadas a seguir.

Se a conexão na rede IEEE 802.11 falhar durante uma sessão de um serviço de um determinado MH para um CH, a entidade *Converge* informa a BS local para restabelecer



**Figura 4.4** Troca de mensagens durante o *handoff* da rede IEEE 802.11 para UMTS com SIP



**Figura 4.5** Troca de mensagens durante o *handoff* da rede IEEE 802.11 para UMTS com MIPv6

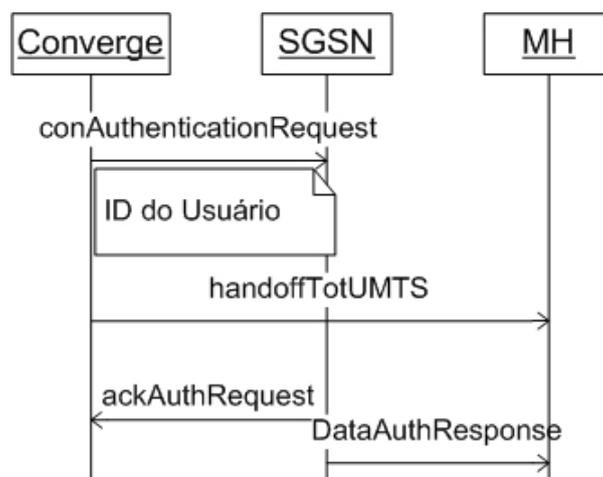
a conexão do MH com a rede celular.

Essa técnica de restabelecimento da conexão acrescenta uma nova mensagem, denominada *conAuthenticationRequest* na norma técnica do sistema UMTS, no entanto,

utiliza a mesma interface que os dispositivos UMTS utilizam para se comunicar com a UTRAN, a interface “ $U_u$ ”.

Quando ocorre uma queda no sinal da WLAN (i.e., passando de um limiar aceitável), a *Converge* envia essa mensagem para a rede celular informando o identificador do usuário, que está conectado a WLAN, e que para evitar a perda de conexão do usuário com a ausência ou baixo sinal oferecido pela rede IEEE 802.11, têm sua conexão com a rede celular restabelecida. O diagrama de seqüência relacionado com esse processo é observado na Figura 4.6.

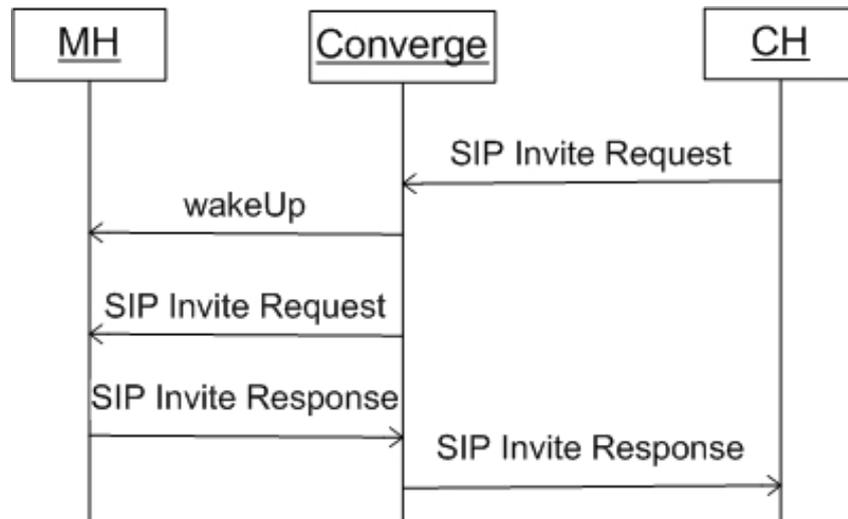
Desse modo, a entidade *Converge* tem um controle sobre todos os usuários que estão conectados a WLAN para restabelecer a conexão UMTS dos usuários que necessitam. Essa característica já é um passo rumo as NGNs, considerando também o conceito de ABC, no qual é necessário além de estar conectado, restabelecer essa conexão da melhor forma possível.



**Figura 4.6** Restabelecimento de conexão UMTS através da entidade Converge

Outra importante característica da *Converge* é com o gasto desnecessário de energia do MH durante o gerenciamento da comunicação. A energia dos dispositivos móveis, por ser um recurso crítico, deve ser economizada. Dessa forma, caso após uma sessão, o MH permaneça conectado a rede IEEE 802.11, ele pode permanecer com o agente SIP desativado e se alguma mensagem SIP (e.g., INVITE) chegar para ele, a entidade *Converge*, envia a mensagem *wakeUp* para “acordar” o MH (i.e., ativar o agente SIP) e, então, repassa a mensagem para o seu destino. Dessa forma, não é necessário que o MH mantenha o agente SIP ativo para receber mensagens SIP, reduzindo o consumo de

energia dos MHs. O diagrama de seqüência relacionado a este cenário é observado na Figura 4.7.



**Figura 4.7** Economia de Energia através da entidade Converge

Essa técnica de economia de energia pode representar um bom recurso para a otimização da energia do dispositivo, já que o usuário pode desfrutar dos serviços, mesmo não estando com o agente SIP ativo no momento em que chega a mensagem *SIP Invite*.

#### 4.4 ESPECIFICAÇÃO FORMAL

Este trabalho utiliza a linguagem formal SDL, padronizada pela ITU-T na recomendação Z.100 [25], que é uma das TDFs mais utilizadas para a especificação e descrição de sistemas complexos e críticos, por exemplo, sistemas de telecomunicações. A escolha de SDL deve-se, ainda, a facilidade de aprendizado e a disponibilidade de ferramentas. A linguagem SDL é baseada em eventos e estados, facilitando ainda a sua modelagem. Além disso, ela é a linguagem formal adotada pelos órgãos de padronização dos sistemas celulares considerados neste trabalho. No caso deste trabalho, o mapeamento para a linguagem SDL foi feito com base nos diagramas de seqüência apresentados na Seção 4.3.

Em [65] é realizado uma análise das seguintes linguagens de especificação: UCM, LOTOS, MSC e SDL. As linguagens são comparadas em 13 critérios, que são agrupados em 4 categorias: usabilidade, validação e verificação, suporte a ferramenta e treinamento. Nenhuma das linguagens cobriu efetivamente todos os critérios analisados. No entanto,

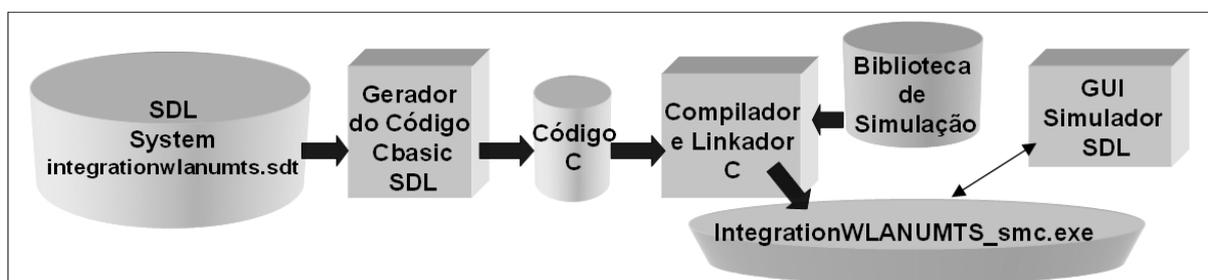
a junção das técnicas MSC e SDL, utilizadas neste trabalho, mostrou-se bastante relevante para o que está sendo proposto. Os principais critérios abordados em [65] que são relevantes para este trabalho são: Testes, Simulação e Verificação. Dessa forma, SDL foi escolhida para especificar e validar a nossa proposta.

A linguagem SDL, que é utilizada, principalmente, para a descrição de sistemas em comunicação em tempo real e dirigidos a eventos, possui as seguintes características:

- Disponibiliza um conjunto de conceitos bem definidos para a construção do modelo;
- Provê uma visão de todo o sistema a ser modelado e com uma especificação clara e sem ambigüidades;
- Possibilita o uso de ferramentas para simular e validar as modelagens;
- Fornece a possibilidade de geração de aplicações sem a necessidade da fase tradicional de código para que possa ser observado o comportamento do sistema.

A Figura 4.8 apresenta o ciclo geral que uma especificação em SDL pode ter. Através do editor SDL, que serve para visualizar os modelos, pode ser gerada a especificação gráfica SDL. Em seguida, a especificação pode ser compilada e caso erro sejam gerados, possam ser corrigidos. Há também a possibilidade da simulação e validação da especificação. A simulação ocorre através de um processo interativo, enquanto que a validação representa uma simulação exaustiva da especificação.

Além da simulação e validação da especificação em SDL, podem ser gerados códigos em outras linguagens automaticamente. Casos de testes em TTCN (*Tree and Tabular Combined Notation*) e códigos na linguagem C podem ser reproduzidos através da especificação [66][67].



**Figura 4.8** Visão Geral do Ciclo de uma Especificação em SDL

### ***Especificação em SDL para a integração das Redes UMTS e IEEE 802.11***

A modelagem em SDL deste trabalho foi feita utilizando a ferramenta Telelogic Tau SDL Suite [26] versão 5.1, que oferece editores gráficos para a modelagem bem como ferramentas adicionais para simulação e testes. Esta ferramenta pode ser dividida nas seguintes funcionalidades:

- SDL Organizer, que permite a modelagem do sistema a ser validado;
- Simulator UI, que permite a simulação do modelo;
- Validator UI, que permite validar o modelo, criando cenários de simulação e detectando falhas.

Uma visão completa do sistema através do SDL Organizer é mostrada na Figura 4.9. Um sistema SDL é composto de vários blocos, que pode ser dividido em outros blocos, formando uma hierarquia de blocos. A comunicação dos blocos é definida pelos canais entre os blocos e o ambiente, e o comportamento de cada bloco baseia-se em processos, os quais são descritos por máquinas de estados finitos. Os processos se comunicam através da troca de sinais. Cada processo contém uma fila do tipo FIFO (*First-In First-Out*) com os sinais, a qual comporta a ordem dos sinais e os estados dos processos ao receberem um determinado sinal.

Neste trabalho, a Figura 4.10 mostra os blocos MH, CH, IEEE8021.11\_Network, UTRAN, CNUMts, IMSNetwork, AccessGateway80211, HA e DHCP\_Network.

Os canais definem os caminhos de comunicação, pelos quais os blocos se comunicam uns com os outros ou com o ambiente. Cada canal usualmente contém uma fila FIFO, que contém os sinais (mensagens) que são transportados no canal. O comportamento dos blocos é descrito por processos, que são apresentados por máquinas de estado.

Uma visão completa dos blocos e sinais do sistema de integração é mostrada na Figura 4.10.

O bloco MH, que é um dos principais blocos, por ser atuante tanto no comportamento do *handoff* utilizando o MIP quanto com o SIP é mostrado na Figura 4.11. Os diagramas de estados do MH, os quais determinam seu comportamento, são apresentados nas figuras 4.12, 4.13 e 4.14.

A Figura 4.11 apresenta os dois processos que formam o MH: UE e USIM. O UE refere-se ao terminal do usuário e o USIM representa o cartão UMTS, que contém a identificação do usuário e os dados para autenticação. Esse bloco possui diversos canais de comunicação e recebe e envia vários sinais, indicados na figura. Ao clicarmos duas vezes sobre o bloco MH, obteremos os diagramas de estados referentes às figuras 4.12, 4.13 e 4.14.

A Figura 4.12 contém todos os sinais recebidos e enviados pelo MH durante o processo de seleção e autenticação da rede. Esses sinais foram mapeados através dos diagramas de seqüência mostrados no Capítulo 2.

A Figura 4.13 apresenta o comportamento do MH com a atualização da sua localização ao executar o processo de *handoff*. Este diagrama é referente ao MH se movimentando para a rede IEEE 802.11, que na figura está representado pelo estado de transição “*MobilityWLAN*”. Os sinais foram mapeados de acordo com os diagramas apresentados na Seção 4.3. As principais mensagens com o SIP como protocolo são: “*SIPPreInviteRequest*”, “*SIPPreInviteResponse*”, “*Binding\_Update*” e “*Binding\_Acknowledgment*”.

As mensagens “SIP” e “MIP” são enviadas pelo usuário através do *Environment* para indicar qual protocolo será usado no gerenciamento.

A Figura 4.14 apresenta o comportamento no gerenciamento de mobilidade do MH com a execução do processo de *handoff* para a rede UMTS. Os sinais foram mapeados de acordo com os diagramas apresentados na Seção 4.3 e tem o comportamento semelhante ao citado anteriormente.

O diagrama de estados da *Converge* é mostrado na Figura 4.15. A *Converge* é localizada no bloco do *gateway* de acesso à rede IEEE 802.11. Essa entidade pode receber três tipos de mensagens: “*SIPPreInviteRequest*”, “*handoffToUMTS*” e “*SIPInviteRequest*”.

A mensagem “*SIPPreInviteRequest*” é recebida quando o MH executa o *handoff* para a rede IEEE 802.11. Ela é então encaminhada para o servidor SIP para atualizar a localização do MH.

A mensagem “*handoffToUMTS*” é enviada pelo usuário para representar a queda do sinal da rede WLAN, e quando a conexão da rede IEEE 802.11 falha durante uma sessão de um serviço de um determinado MH para um CH, a entidade *Converge* é responsável por informar a BS local para restabelecer a conexão do MH com a rede celular.

A mensagem utilizada é a “*conAuthenticationRequest*” e, em seguida, envia a mensagem “*handoffToUMTS*” para o MH para que ele saiba que sua conexão está sendo restabelecida com a rede celular.

A mensagem “*SIPInviteRequest*” é utilizada na técnica de economia de energia. Essa mensagem também é enviada pelo usuário.

Ao receber essa mensagem, a entidade *Converge* é responsável por informar ao MH (através da mensagem “*wakeUp*”) que ele precisa ativar o agente SIP. Em seguida, envia a mensagem “*SIPInviteRequest*” para que seja estabelecida a sessão SIP.

O diagrama de estados do I-CSCF, que é o ponto de entrada de mensagens SIP de usuários visitando outras redes, é mostrado na Figura 4.16.

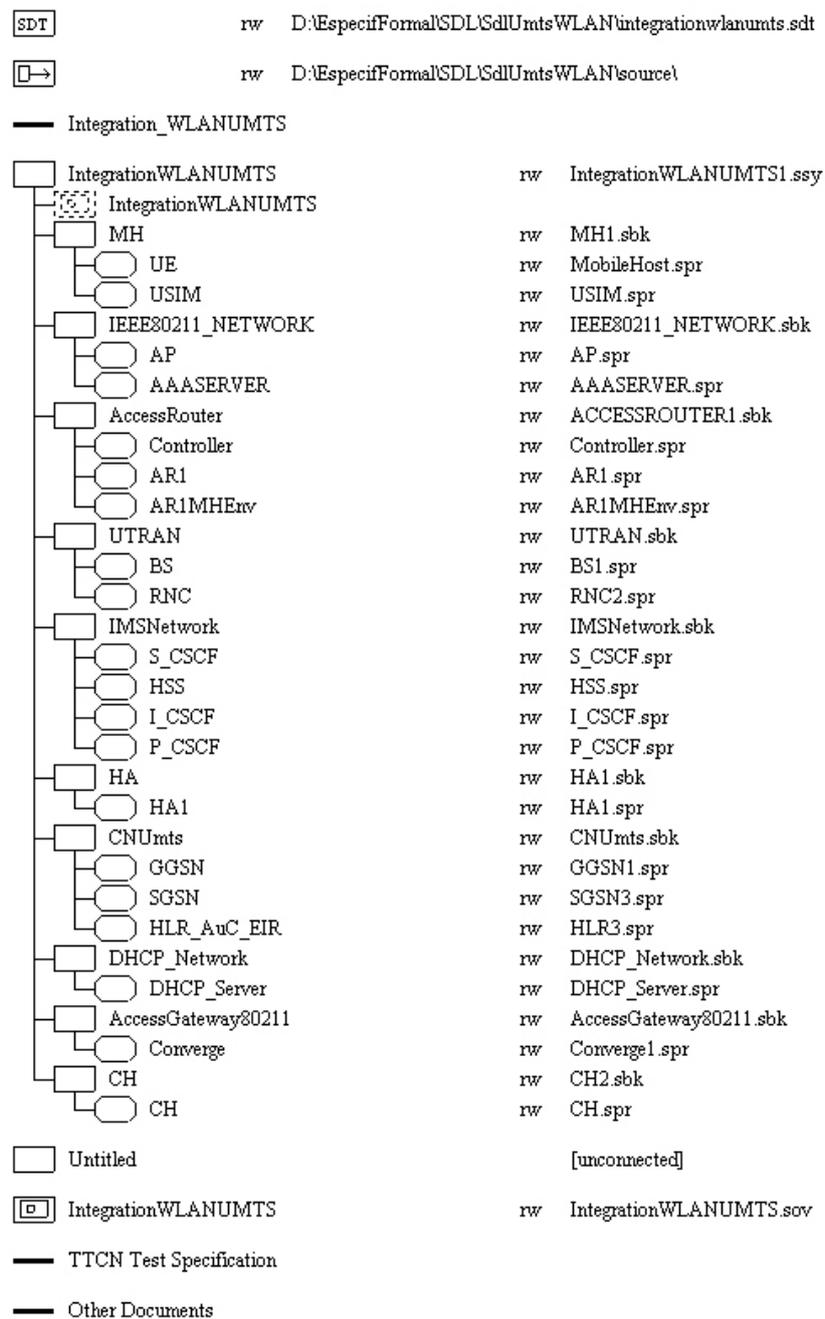


Figura 4.9 Visão Geral do sistema através do Organizer

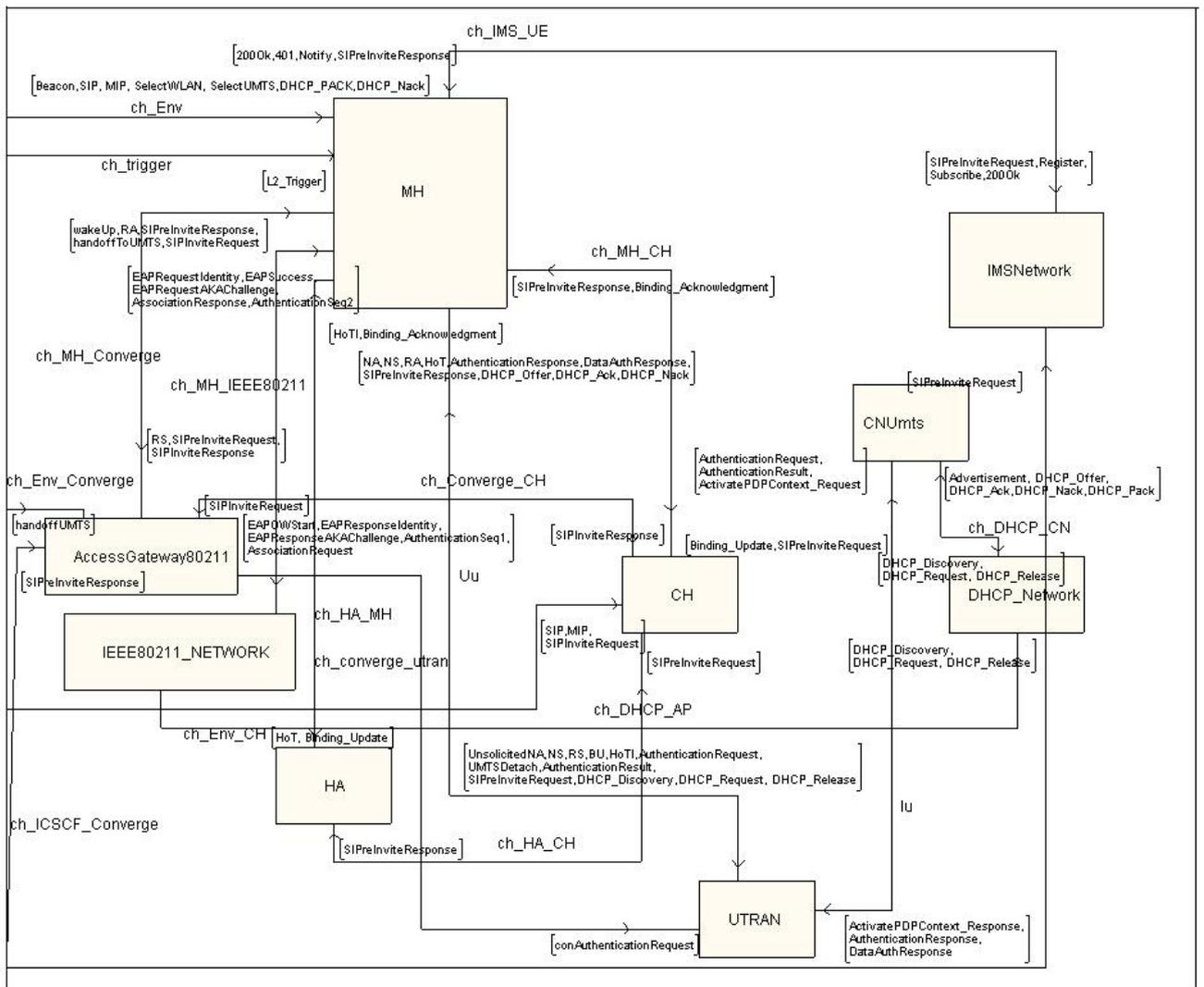


Figura 4.10 Sistema SDL de Integração das redes UMTS e IEEE 802.11

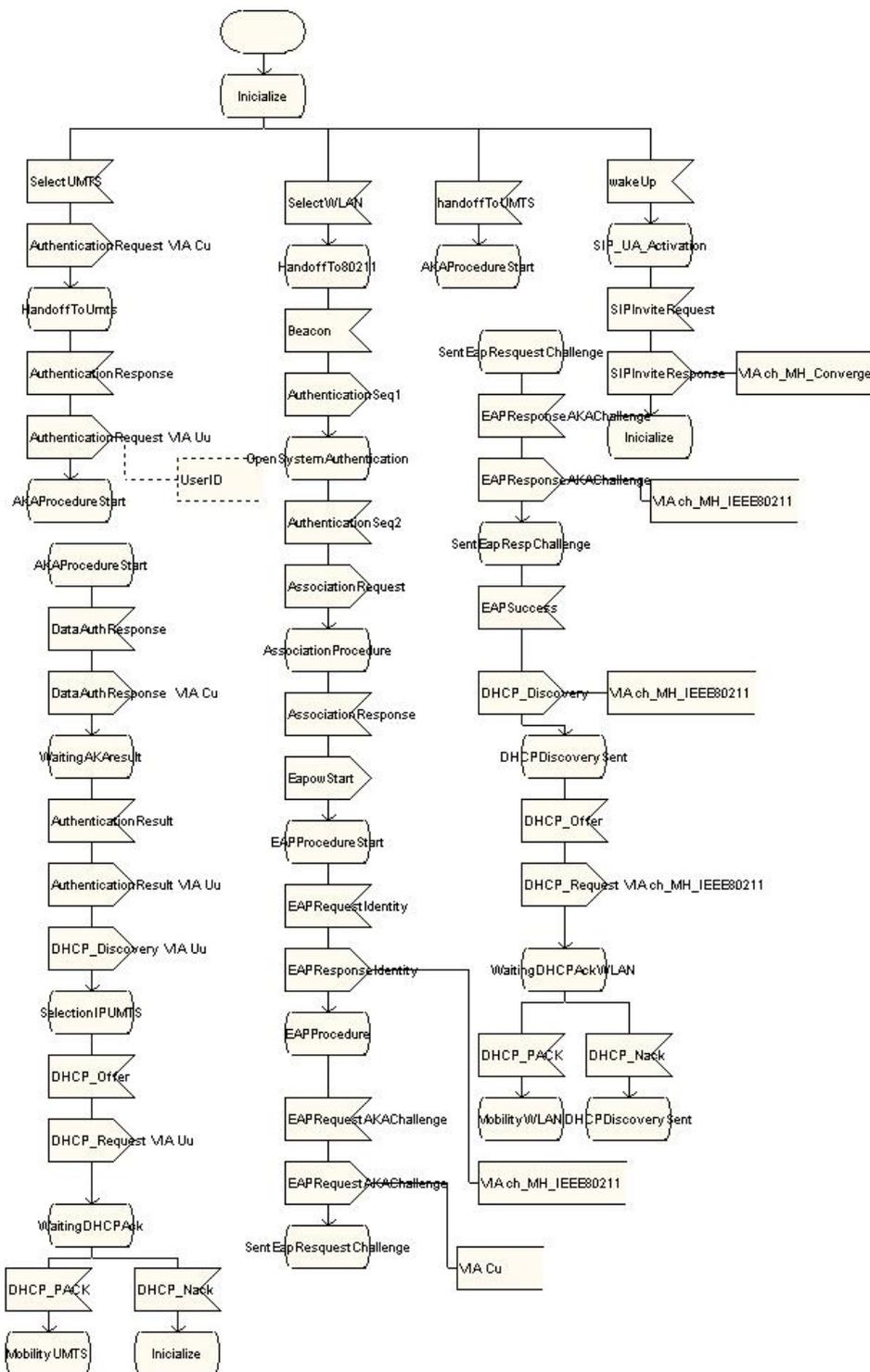
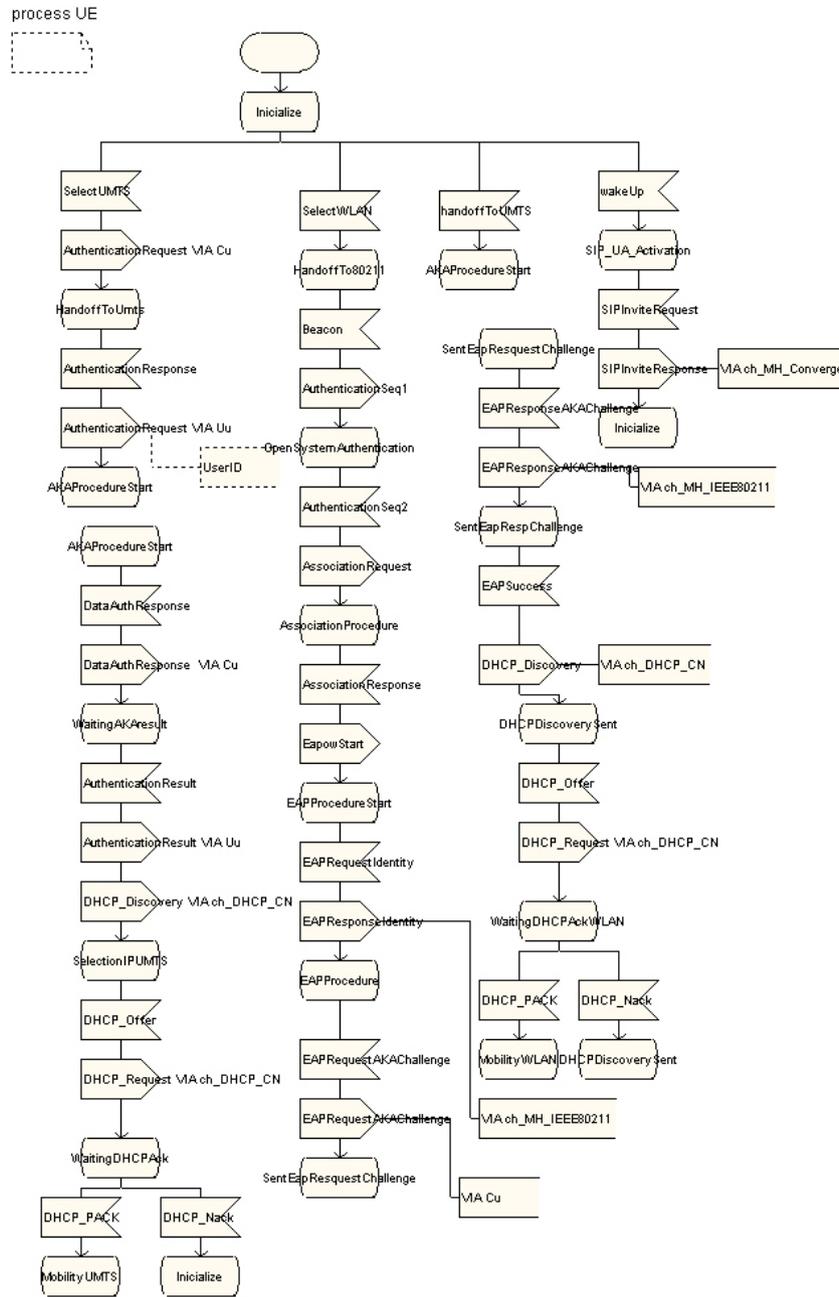
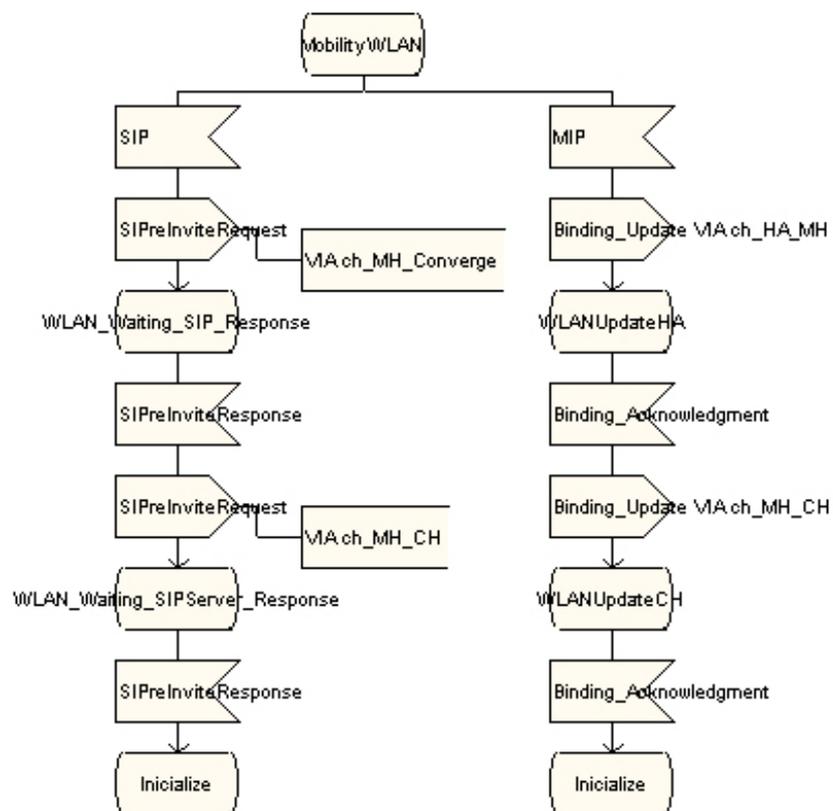


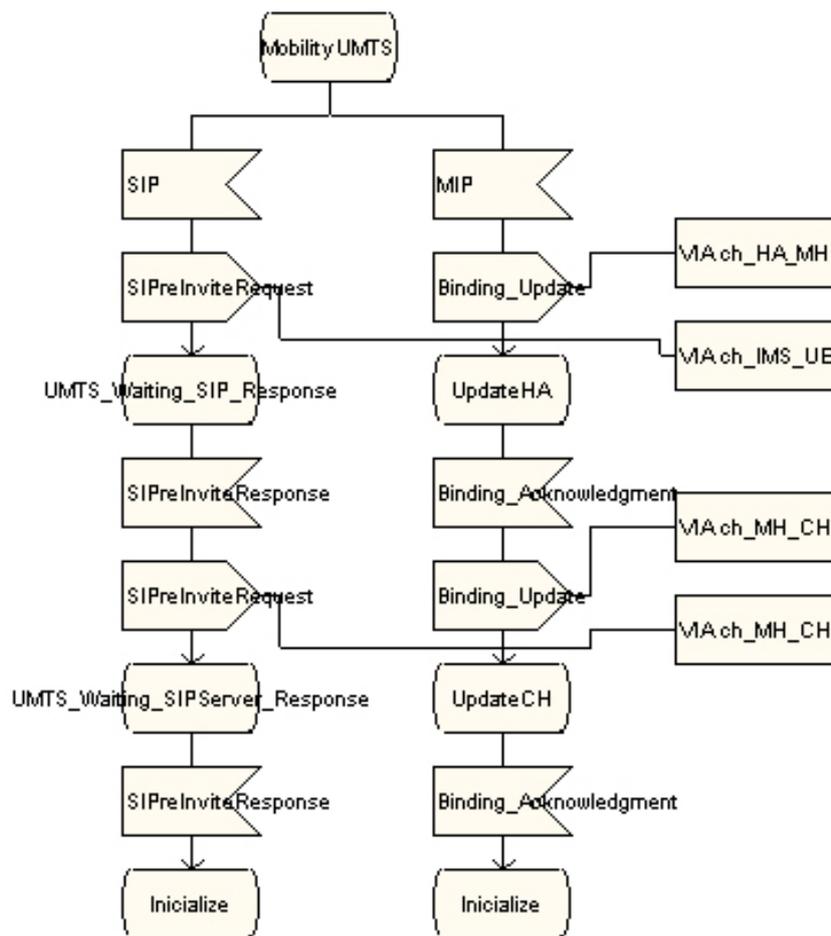
Figura 4.11 Bloco MH



**Figura 4.12** Diagrama de Estados do Bloco MH apresentando o processo de autenticação nas redes UMTS e IEEE 802.11



**Figura 4.13** Diagrama de Estados do Bloco MH apresentando o comportamento SIP e MIP na rede IEEE 802.11



**Figura 4.14** Diagrama de Estados do Bloco MH apresentando o comportamento SIP e MIP na rede UMTS

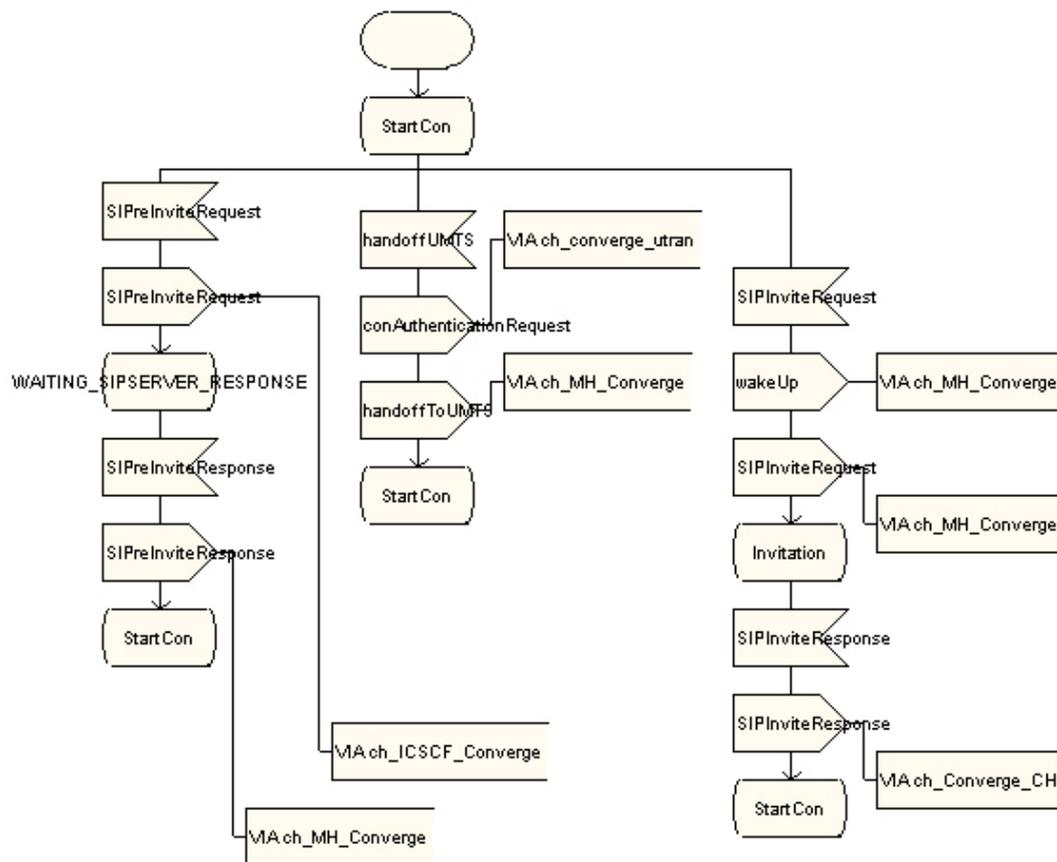


Figura 4.15 Diagrama de estados da entidade Convergence

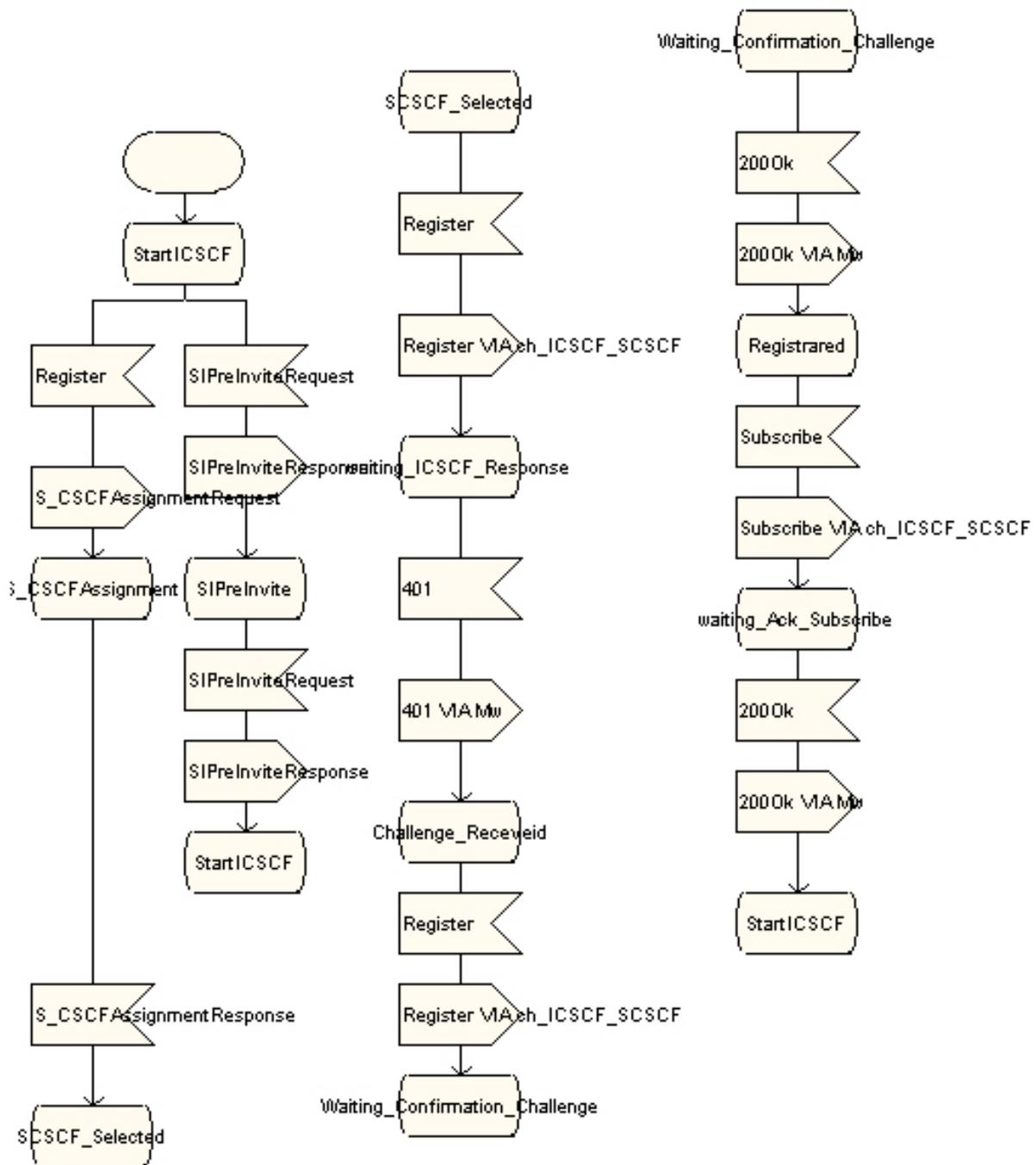


Figura 4.16 Diagrama de estados do servidor IMS: I-CSCF

## CAPÍTULO 5

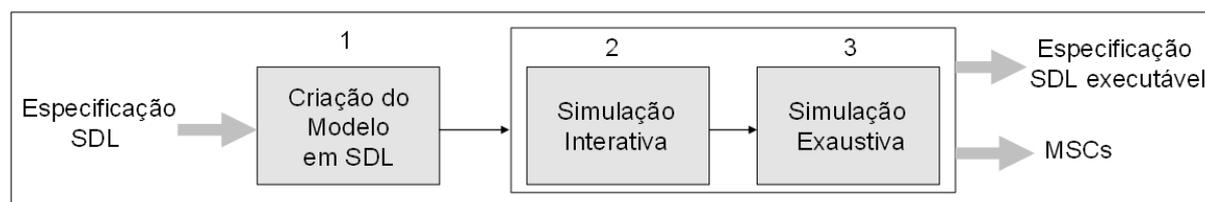
# SIMULAÇÃO E VALIDAÇÃO EM SDL

SDL é bastante útil por representar um modo rápido de avaliar um sistema antes de sua real implementação ou para verificar qual seria o comportamento obtido. Em conjunto com a ferramenta automática, a ferramenta *Telelogic* Tau é usada para a simulação e validação da especificação formal em SDL que modela a proposta desta dissertação.

Este capítulo descreve a simulação e validação da especificação em SDL. Na Seção 5.1 são apresentadas as características relevantes na simulação e validação em SDL. A Seção 5.2 e a Seção 5.3 apresentam os resultados da simulação e validação, respectivamente.

### 5.1 CARACTERÍSTICAS DA SIMULAÇÃO E VALIDAÇÃO EM SDL

É importante mencionar que neste trabalho verificou-se a necessidade da especificação em SDL, devido os sistemas de comunicação utilizados apresentarem características complexas tais como, mobilidade e interoperabilidade. Além disso, o 3GPP também adota o SDL como linguagem para especificar alguns comportamentos dos sistemas celulares.

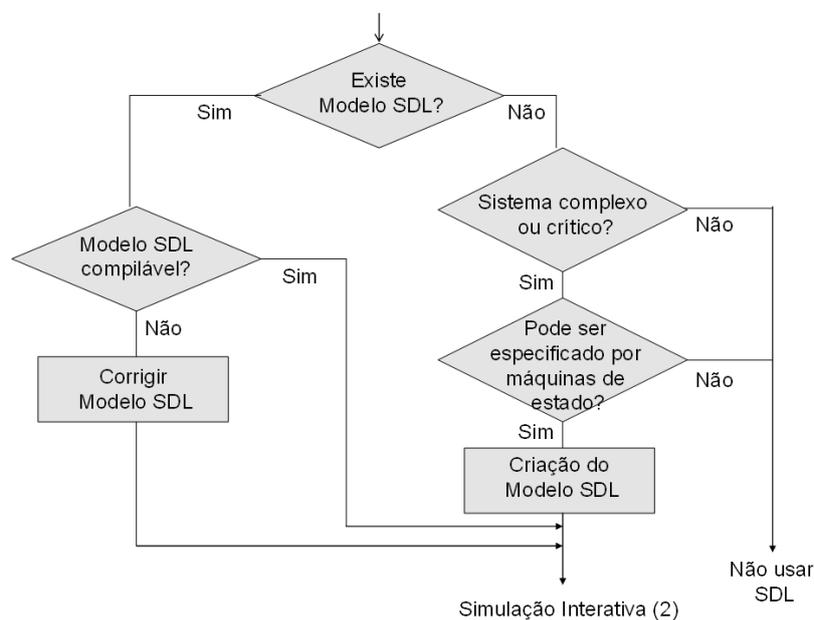


**Figura 5.1** Passos do processo de simulação em SDL (adaptado de [9])

O processo de simulação utilizado pode ser observado na Figura 5.1 e é baseado em três passos definidos em [9], a seguir: Criação do Modelo SDL (1) que possa ser simulado (i.e., um modelo SDL compilado e sem erros); Simulação Interativa (2), que oferece um bom nível de validação e testes automáticos; e Simulação Exaustiva (3), também chamada

de Validação, que fornece um alto nível de corretude. Como resultado desses passos, uma especificação em SDL validada e os respectivos cenários em MSCs são obtidos.

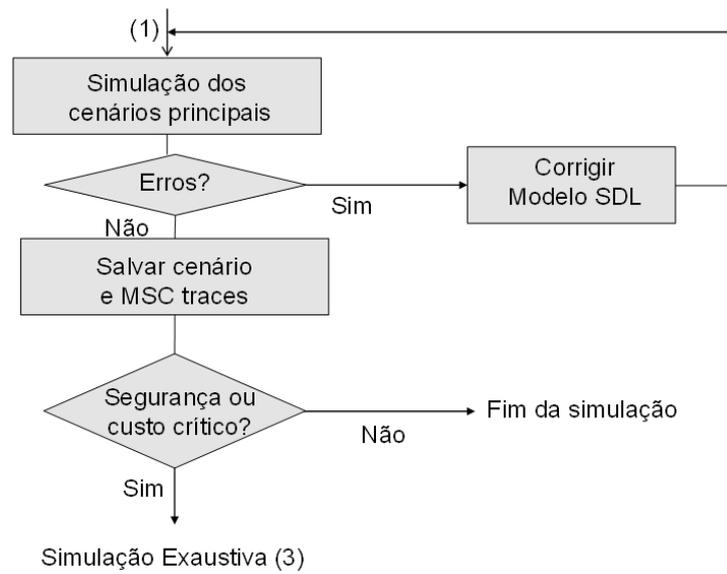
O passo (1) é apresentado na Figura 5.2. O início consiste em verificar se existe uma especificação em SDL, em caso afirmativo, como nesta dissertação, ela deve ser compilada. Se houver erros, eles devem ser corrigidos para antes de iniciar o passo (2) do processo de simulação em SDL. Se não existir uma especificação em SDL, as características do sistema a ser desenvolvido devem ser analisadas para verificar se ele representa um sistema complexo e passível de ser modelado por máquinas de estado.



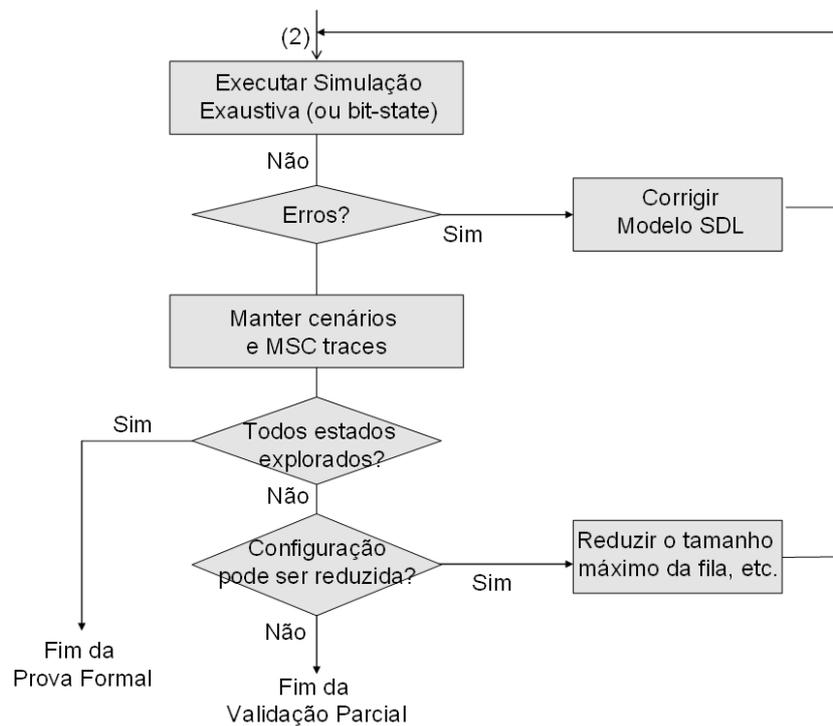
**Figura 5.2** Primeiro passo do processo de simulação em SDL (adaptado de [9])

O passo (2) é apresentado na Figura 5.3, o qual foi simplificado do original para atender as restrições de tempo no desenvolvimento desta dissertação, sem prejuízo para a simulação e validação final. Os principais cenários da especificação são simulados passo a passo. Erros na especificação também podem ocorrer durante essa etapa e eles devem ser corrigidos. Neste trabalho foram encontrados erros neste passo, os quais foram solucionados para então continuar a simulação. O erro mais encontrado nessa fase foi: “descartando um sinal inesperado”, o qual denota que no estado corrente de um processo não existe a especificação de entrada de um determinado sinal na simulação. Esse erro é exibido no *Simulator* UI com a seguinte mensagem: *Signal -signal name- caused an immediate null-transition*.

No passo (3), apresentado na Figura 5.4, é executada a fase de validação, a qual



**Figura 5.3** Segundo passo do processo de simulação em SDL (adaptado de [9])



**Figura 5.4** Terceiro passo do processo de simulação em SDL (adaptado de [9])

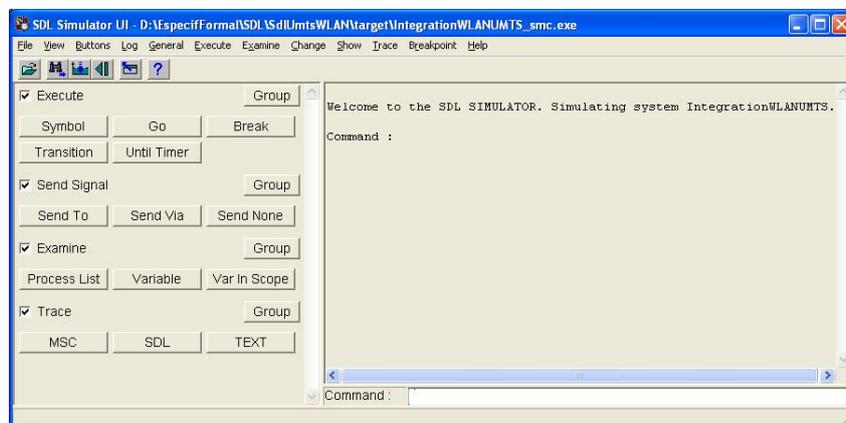
é realizada através de execuções exaustivas da simulação. Quando um erro é encontrado, o modelo SDL deve mais uma vez ser corrigido. Para isso, os cenários e os traces gerados pela simulação devem ser mantidos pelo desenvolvedor. A simulação é finalizada quando

todos os estados alcançáveis do modelo SDL foram explorados. Nesse caso, a corretude do modelo é formalmente provada. Caso contrário, se ocorrer um grande número de estados não explorados, a configuração do modelo deve ser reduzida. Se a simulação não puder ser reduzida, ela é finalizada, mas a validação é apenas parcial, visto que existem estados ainda não explorados. O simulador também detecta símbolos SDL nunca simulados. Eles indicam transições SDL ou ramos que podem ser removidos, ou revelam sinais de testes esquecidos, ou valores do teste para serem transmitidos para o modelo SDL pelo simulador.

## 5.2 SIMULAÇÃO DO SISTEMA DE INTEGRAÇÃO UMTS E IEEE 802.11

O aplicativo *Simulator* UI é utilizado para que sejam simulados os processos de *handoff* vertical entre as redes. O usuário também participa do processo de simulação gerando e recebendo os sinais tratados pelo ambiente. Os sinais trocados entre os processos podem ser visualizados através de diagramas de seqüência.

Na Figura 5.5 pode-se observar o aplicativo *Simulator* UI. A área de texto à direita na figura mostra a entrada de comandos, os resultados e os erros ocorridos.



**Figura 5.5** O aplicativo *Simulator* UI da ferramenta *Telelogic* Tau

Após a execução de todas as transições, pode-se demonstrar o comportamento dinâmico do sistema com o diagrama de seqüência gerado usando o *MSC Trace*. O *MSC Trace* executa os eventos SDL em eventos MSC, com o envio e recebimento de sinais e a criação de processos dinamicamente.

A Figura 5.6 apresenta o processo de *handoff* para a rede IEEE 802.11. O processo

env0 é o ambiente *Environment*, o qual é controlado pelo usuário. Para executar o *handoff* para a rede UMTS, o usuário envia o sinal “SelectWLAN”. O diagrama representa a troca de mensagens durante o processo de seleção, associação, autenticação e configuração do endereço IP na rede IEEE 802.11.

A Figura 5.7 apresenta o processo de *handoff* para a rede UMTS. O processo inicia pelo usuário do sistema ao enviar o sinal “SelectUMTS”. O diagrama representa a troca de mensagens durante o processo de seleção, autenticação e configuração do endereço IP na rede UMTS.

Na Figura 5.8 pode-se observar o diagrama de seqüência gerado pela simulação interativa do sistema UMTS e IEEE 802.11 após os passos apresentados na Figura 5.7. Este diagrama apresenta o processo de *handoff* para a rede UMTS, utilizando o MIP como protocolo de gerenciamento de mobilidade. Por usar o MIP, o usuário deve selecionar através do ambiente *Environment* (env0) o sinal “MIP” para o MH e o CH.

A Figura 5.9 apresenta o processo de *handoff* para a rede UMTS, utilizando o SIP como protocolo de gerenciamento de mobilidade. Neste caso, o usuário deve selecionar através do ambiente *Environment* (env0) o sinal “SIP” para o MH e o CH.

A Figura 5.10 apresenta o processo de *handoff* para a rede IEEE 802.11 após os passos apresentados na Figura 5.6, utilizando o MIP como protocolo de gerenciamento de mobilidade. O processo inicia com o usuário enviando o sinal “MIP”, como mencionado anteriormente.

A Figura 5.11 apresenta o processo de *handoff* para a rede IEEE 802.11, utilizando o SIP como protocolo de gerenciamento de mobilidade. O processo inicia com o usuário enviando o sinal “SIP”.

### 5.3 VALIDAÇÃO DO SISTEMA DE INTEGRAÇÃO UMTS E IEEE 802.11

Conforme mencionado no Capítulo 4, o aplicativo *Validator* UI é utilizado para detectar possíveis erros e inconsistências na modelagem, os quais foram detectados e corrigidos na simulação interativa do sistema, como, por exemplo, *deadlocks*.

Na Figura 5.14 pode-se observar o aplicativo *Validator* UI. A área de texto à direita na figura mostra a entrada de comandos, os resultados da validação e os erros ocorridos.

O *Validator UI* possui cinco algoritmos: *Bit-State*, *Random Walk*, *Tree Walk*, *Exhaustive* e *Tree Search*. Os algoritmos diferem entre si no modo de percorrer os símbolos, possuindo dois parâmetros em comum: *Timeout*, que indica a quantidade de minutos de validação, e *Depth*, que indica a profundidade máxima da árvore de símbolos a ser percorrida. A Tabela 5.1 apresenta os parâmetros relevantes encontrados como resposta na execução dos algoritmos de exploração para validação do sistema.

O algoritmo de exploração *Bit-State* é um algoritmo usado eficientemente para validar grandes sistemas em SDL [26]. Ele pode ser usado de forma simples ou mais avançado, que contém uma configuração adicional.

Parâmetro	Descrição
<b>Search Depth</b>	Limita a exploração, representando a profundidade máxima ou nível da árvore. Se o nível for atingido durante a exploração, o caminho corrente da árvore é truncado e a exploração continua em outro ramo da árvore. O valor deste parâmetro pode ser alterado através do menu <i>Options2</i>
<b>Size of Hash Table (bytes)</b>	Tamanho da estrutura de dados <i>Hash Table</i> . Caso o tamanho seja pequeno, poderá causar risco de colisão. O valor deste parâmetro pode ser alterado através do menu <i>Options2</i>
<b>No of Reports</b>	Quantidade de erros ou <i>warnings</i> encontrados na exploração
<b>Collision Risk</b>	Risco de colisão associada com o tamanho da estrutura de dados <i>Hash Table</i> criada e com os estados gerados no sistema
<b>Max Depth</b>	Maior profundidade atingida na exploração
<b>Symbol Coverage</b>	Representa a porcentagem de estados executados durante a exploração. Se esse resultado não for 100%, a validação não pode ser considerada finalizada

**Tabela 5.1** Parâmetros relevantes após execução dos algoritmos de Exploração

Para executar a maneira mais simples, basta selecionar o botão “Bit-State” na ferramenta *Validator UI* (ver Figura 5.14). O resultado desta exploração é apresentado na Figura 5.15.

Pelos resultados observados na figura, é percebido que a profundidade máxima atingida (*Max Depth*) foi de 200, mas o valor do *Search Depth*, que delimita a profundidade da exploração, representando a profundidade máxima (*Search Depth*) a ser atingida,

estava configurado para 200. Dessa forma, a profundidade máxima da árvore durante a exploração deve ter sido atingida, e é o que demonstra o campo *Truncated paths*. Este parâmetro foi de valor 5, representando que a profundidade máxima (no caso, 200) foi atingida cinco vezes. Esta exploração não apresentou risco de colisão (*Collision Risk*: 0%) e a porcentagem da cobertura dos estados (*Symbol Coverage*) durante a execução foi de 100% (i.e., todos estados explorados foram executados).

O algoritmo *Bit-State* foi novamente executado, entretanto, o parâmetro *Search Depth* teve seu valor aumentado para 300. O resultado desta exploração é mostrado na Figura 5.16.

Pelos resultados observados na figura, é percebido que a profundidade máxima atingida (*Max Depth*) foi de 239, não houve risco de colisão (*Collision Risk*) e a porcentagem da cobertura dos estados (*Symbol Coverage*) durante a execução foi de 100% (i.e., todos estados explorados foram executados). Neste teste não houve utilização do parâmetro *Truncated paths*, pois a profundidade máxima atingida foi menor do que a profundidade máxima para busca.

Para conseguir uma exploração maior foi executado o algoritmo *Bit-State* de forma avançada. Para isso, no menu *Options1* na ferramenta *Validator UI* (ver Figura 5.14), foi selecionado *Advanced*, em seguida, no menu *Options2*, *Bit-State:Depth*, onde foi configurado o valor 800 para a profundidade máxima a ser atingida na árvore.

A Figura 5.17 apresenta o resultado desta exploração. Pelos resultados observados na figura, é percebido que a profundidade máxima atingida (*Max Depth*) aumentou quando comparada com o algoritmo *Bit-State* de configuração simples (ver Figura 5.16). A profundidade alcançada nesse caso foi de 478, houve risco de colisão (*Collision Risk*) de 4% (provavelmente devido ao tamanho da estrutura de dados *Hash Table*) e todos os estados explorados foram executados (i.e., a porcentagem da cobertura dos estados (*Symbol Coverage*) durante a execução foi de 100%).

Para comprovar que o risco de colisão (*Collision Risk*) de 4% foi causado pelo tamanho da estrutura de dados *Hash Table*, foi executado o algoritmo *Bit-State* de forma avançada novamente, entretanto, dessa vez, também foi alterado o tamanho da estrutura de dados. Para isso, no menu *Options1* na ferramenta *Validator UI* (ver Figura 5.14), foi selecionada a opção *Advanced*, em seguida, no menu *Options2*, a opção *Bit-State:Size-Hash*, onde foi configurado o valor 10000000 bytes. A Figura 5.18 apresenta o resultado desta exploração. Pelos resultados observados na figura, é percebido que não houve risco

de colisão (*Collision Risk*) e a porcentagem da cobertura dos estados (*Symbol Coverage*) durante a execução foi de 100%.

Como mencionado anteriormente, a ferramenta *Validator UI* também disponibiliza outros quatro algoritmos para exploração: *Random Walk*, *Tree Walk*, *Exhaustive* e *Tree Search*. Apesar do algoritmo *Bit-State* ser mais eficiente para grandes sistemas em SDL [26], esses algoritmos também foram executados neste trabalho.

As figuras 5.19, 5.20, 5.21 e 5.22 referem-se aos algoritmos *Random Walk*, *Tree Walk*, *Exhaustive* e *Tree Search*, respectivamente. Todos os algoritmos tiveram como resultado a porcentagem 100% da cobertura dos estados (*Symbol Coverage*).

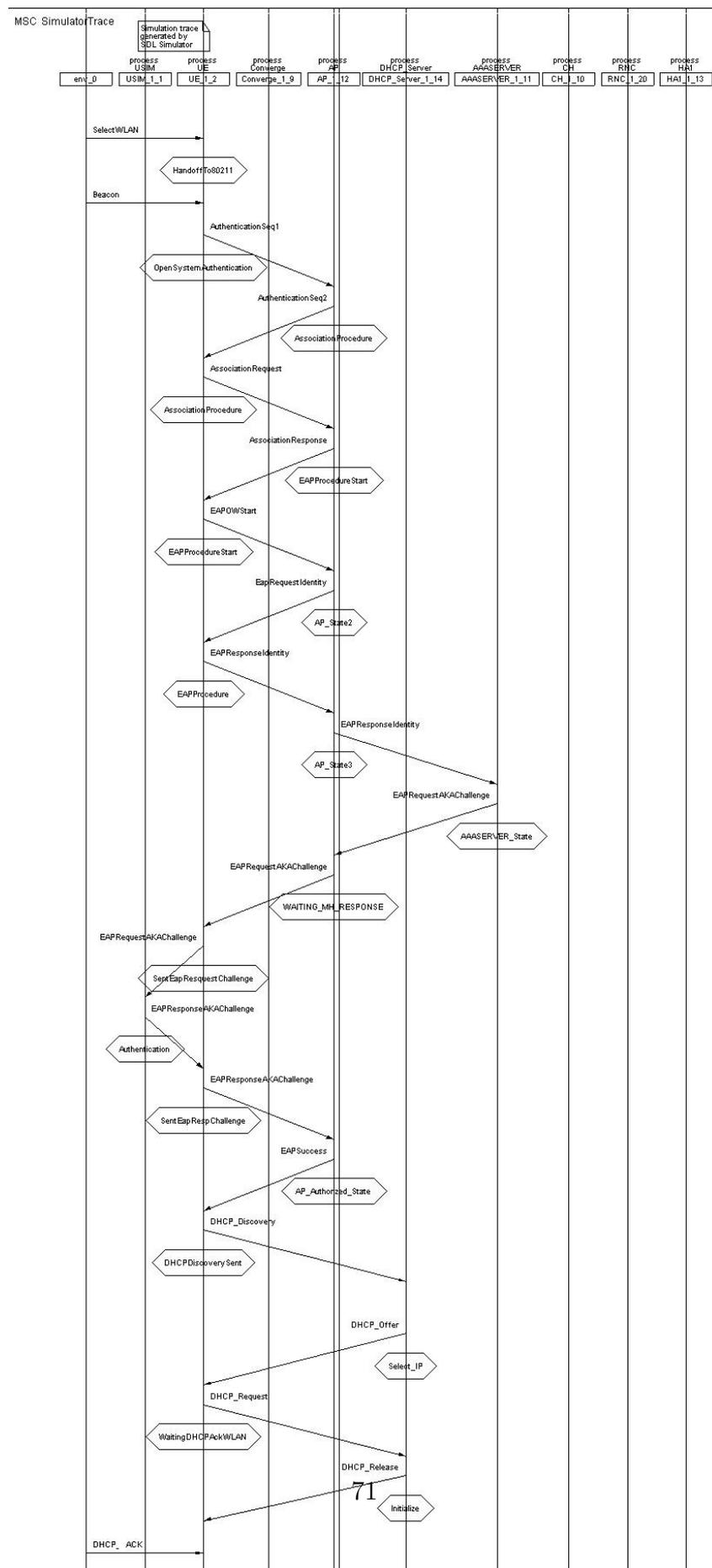
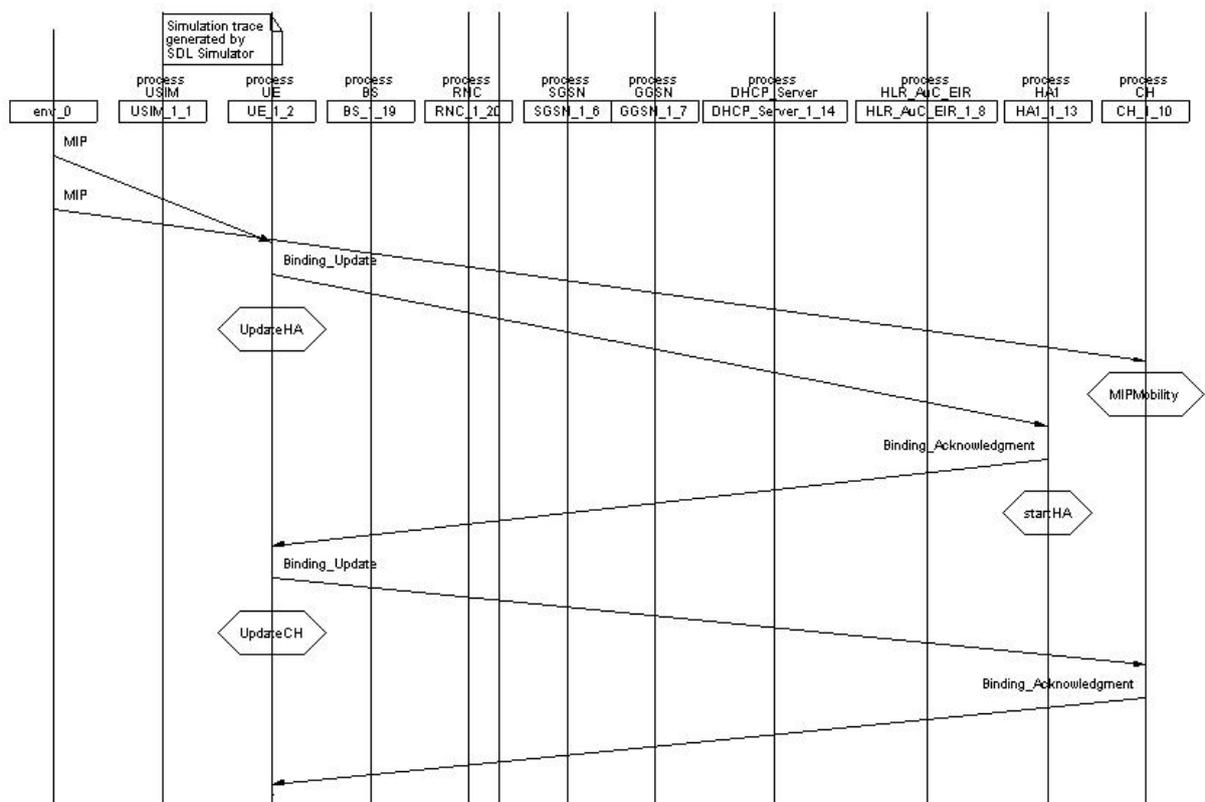
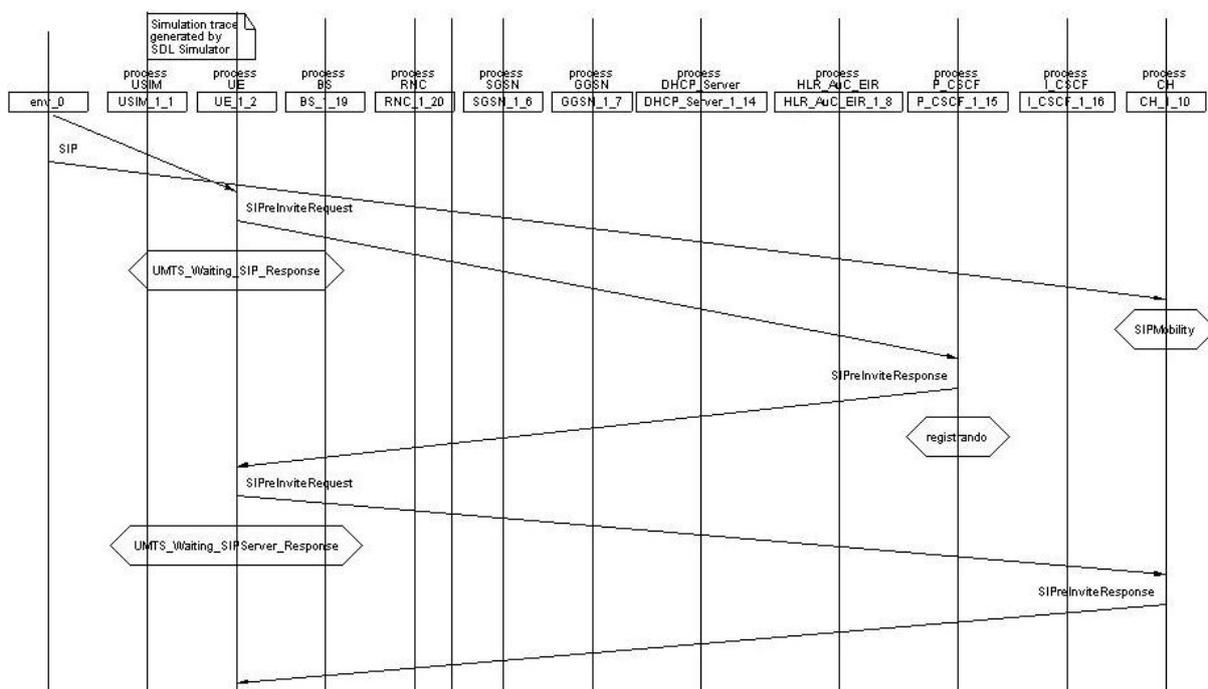


Figura 5.6 Diagrama de Seqüência gerado pelo Simulator UI durante o processo de autenticação à rede IEEE 802.11





**Figura 5.8** Diagrama de Seqüência gerado pelo *Simulator* UI durante o processo de *handoff* para a rede UMTS, utilizando o MIP



**Figura 5.9** Diagrama de Seqüência gerado pelo Simulator UI durante o processo de *handoff* para a rede UMTS, utilizando o SIP

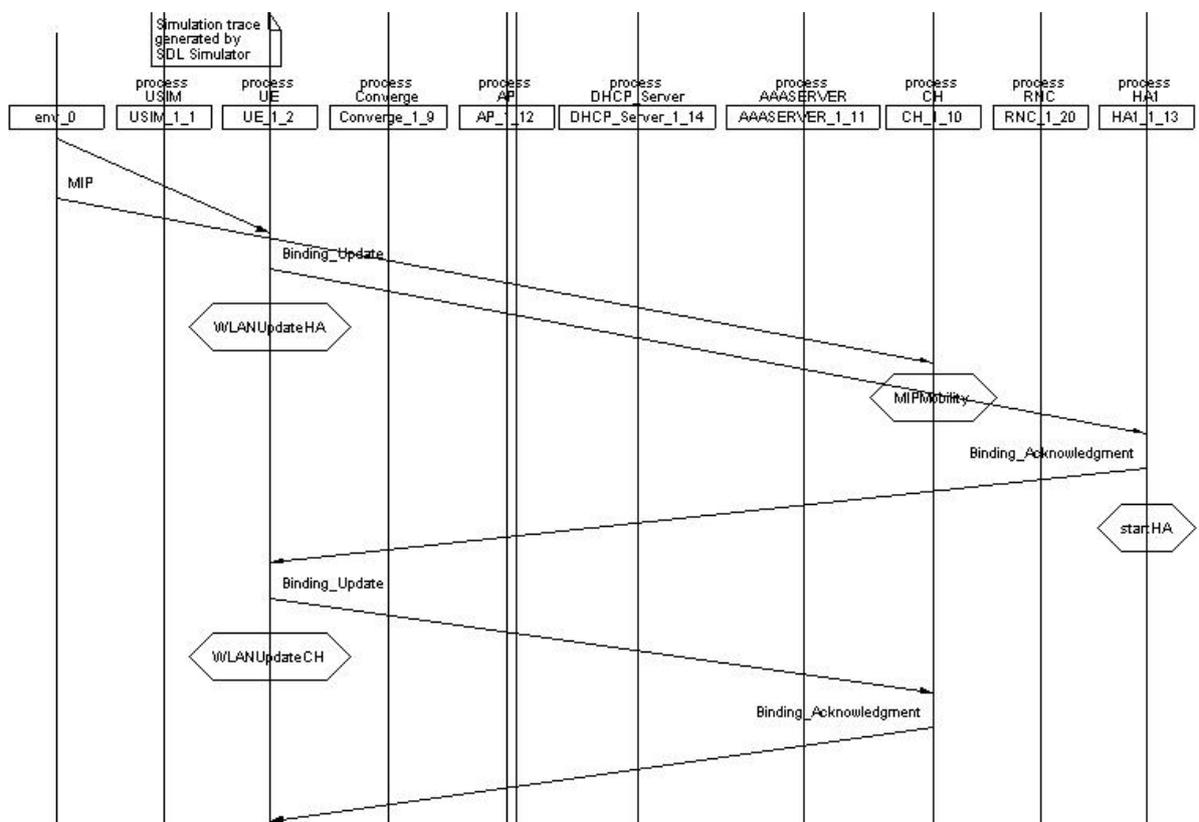
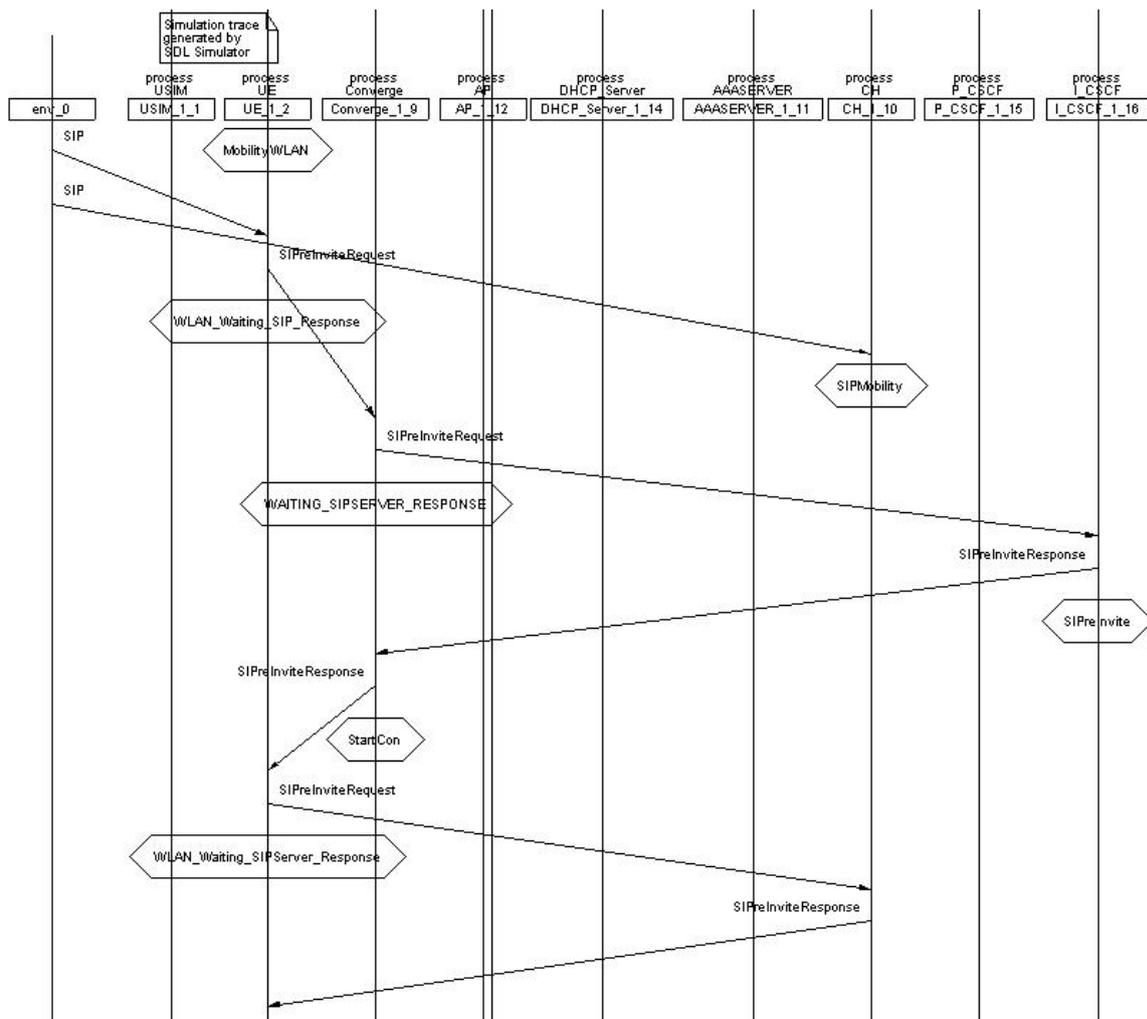
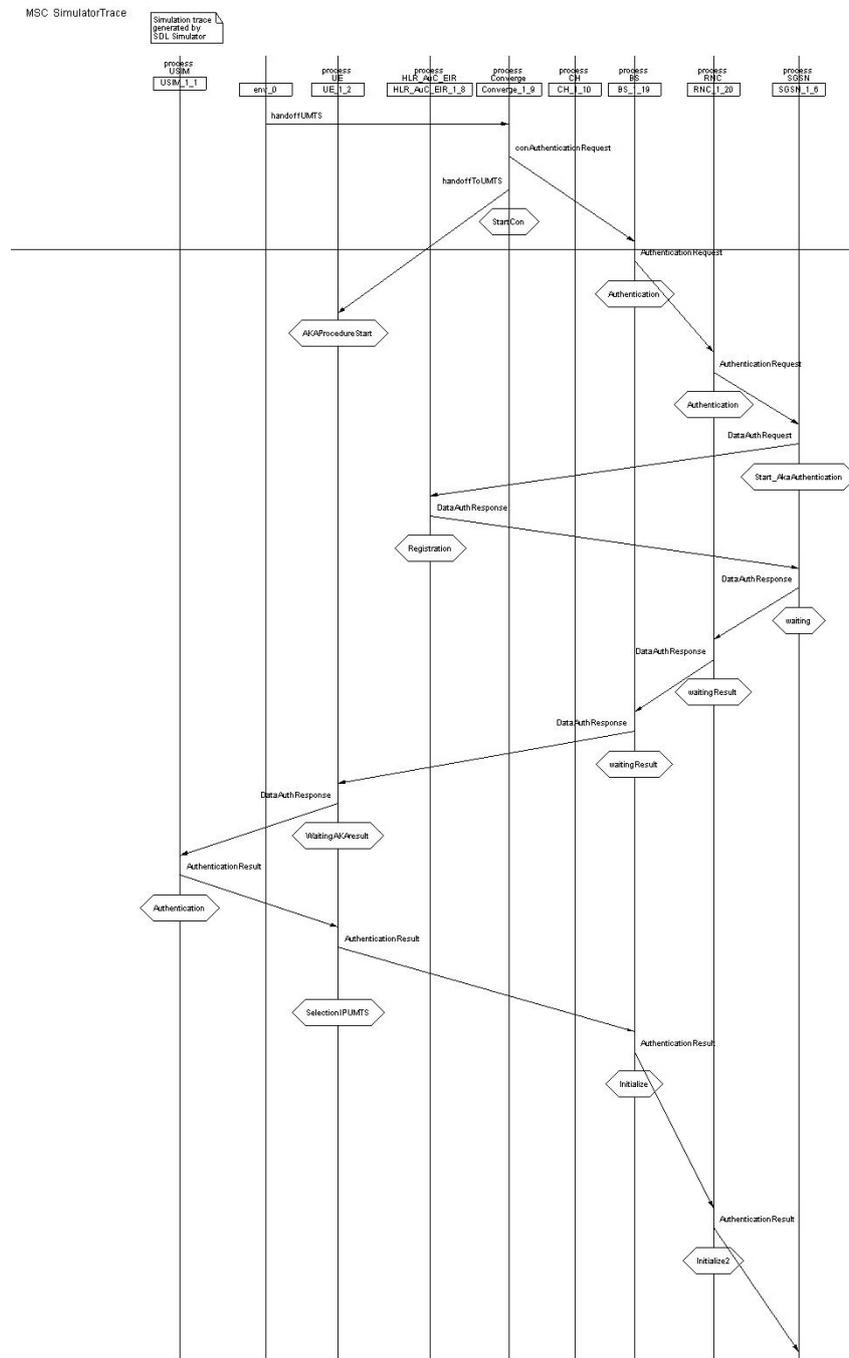


Figura 5.10 Diagrama de Seqüência gerado pelo Simulator UI durante o processo de *handoff* para a rede IEEE 802.11, utilizando o MIP



**Figura 5.11** Diagrama de Seqüência gerado pelo Simulator UI durante o processo de *handoff* para a rede UMTS, utilizando o SIP





**Figura 5.13** Diagrama de Seqüência gerado pelo Simulator UI durante o processo de economia de energia através da *Converge*

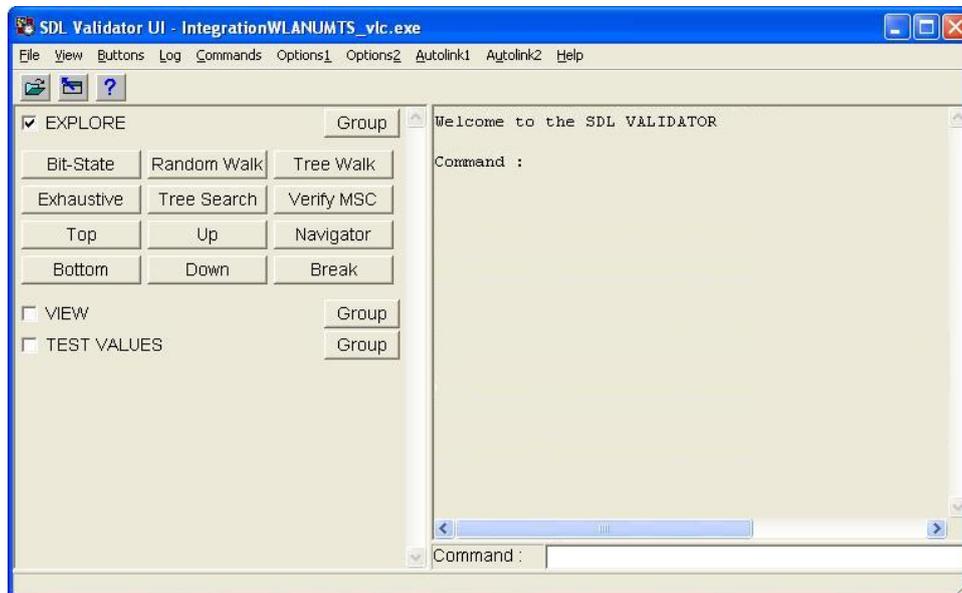


Figura 5.14 O aplicativo Validator UI da ferramenta *Telelogic* Tau

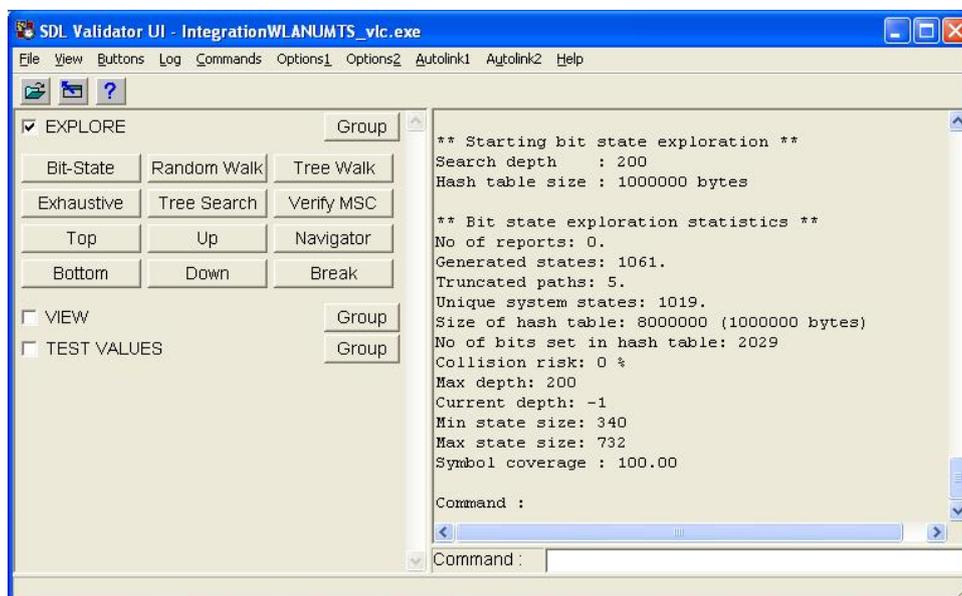
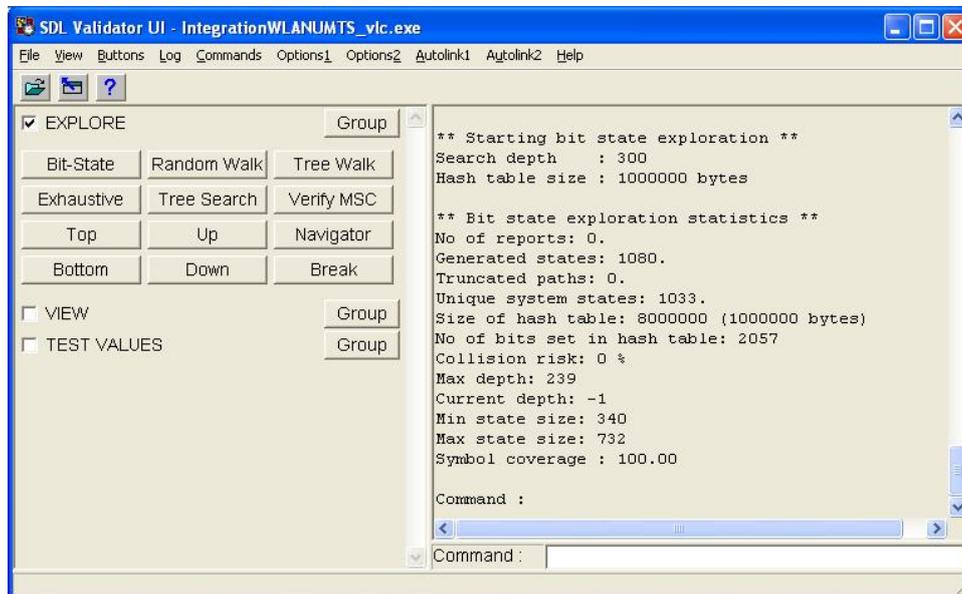
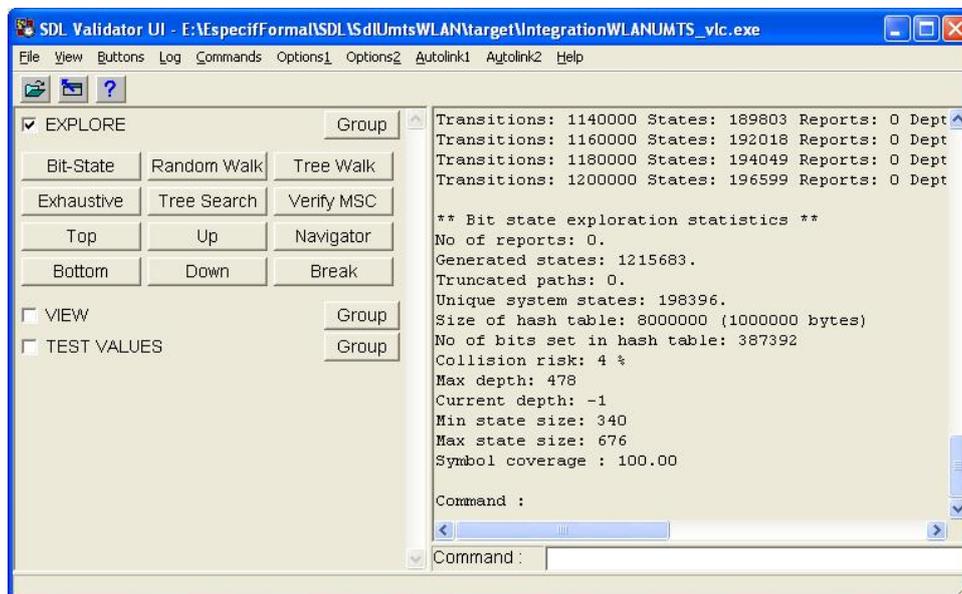


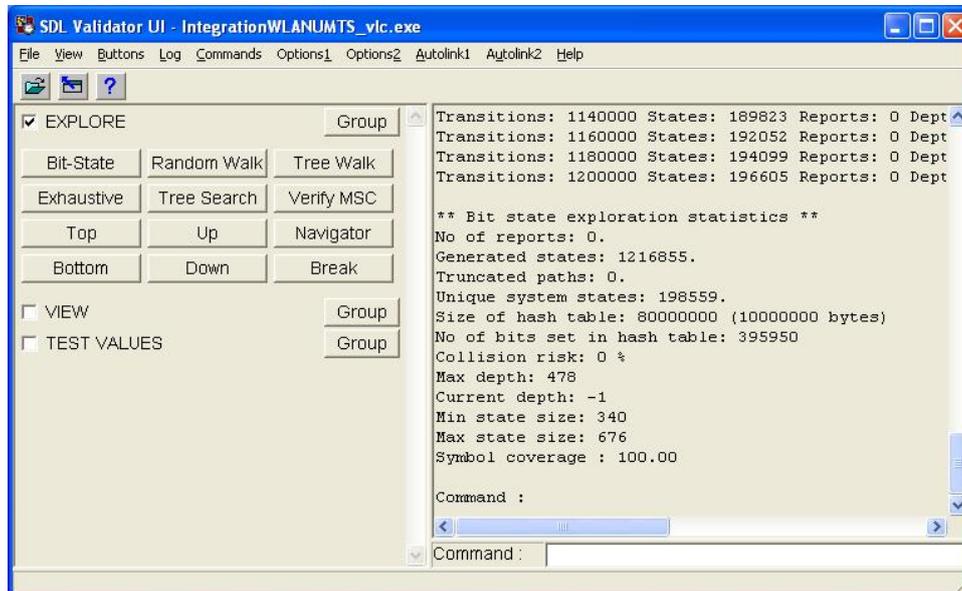
Figura 5.15 Validação utilizando o algoritmo *Bit-State* com profundidade máxima de 200 níveis



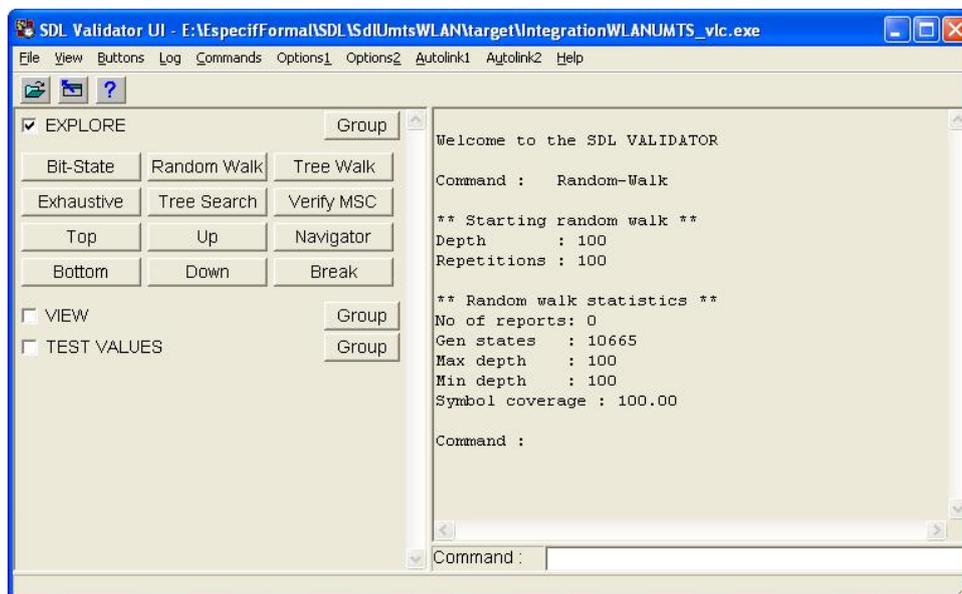
**Figura 5.16** Validação utilizando o algoritmo *Bit-State* simples com profundidade máxima de 300 níveis



**Figura 5.17** Validação utilizando o algoritmo Bit-State avançado com profundidade máxima de 800 níveis



**Figura 5.18** Validação utilizando o algoritmo *Bit-State* configurando o parâmetro tamanho da *Hash-Table* para 100000000 bytes



**Figura 5.19** Validação utilizando o algoritmo *Random Walk*

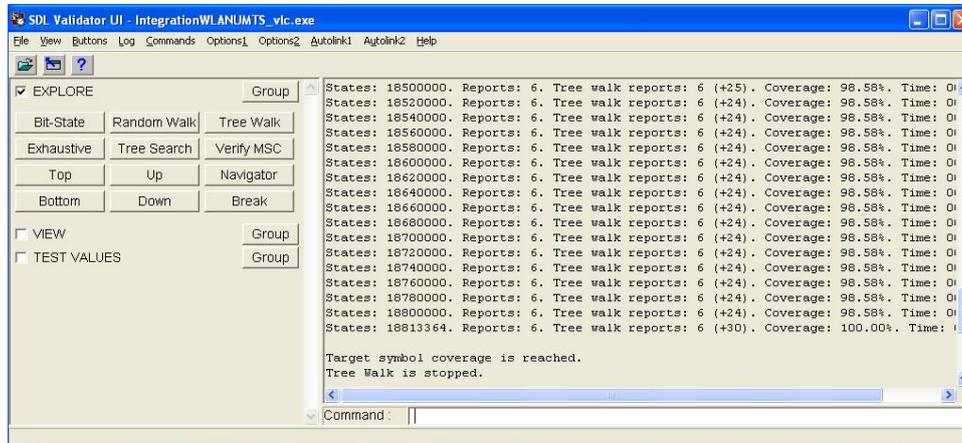


Figura 5.20 Validação utilizando o algoritmo *Tree Walk*

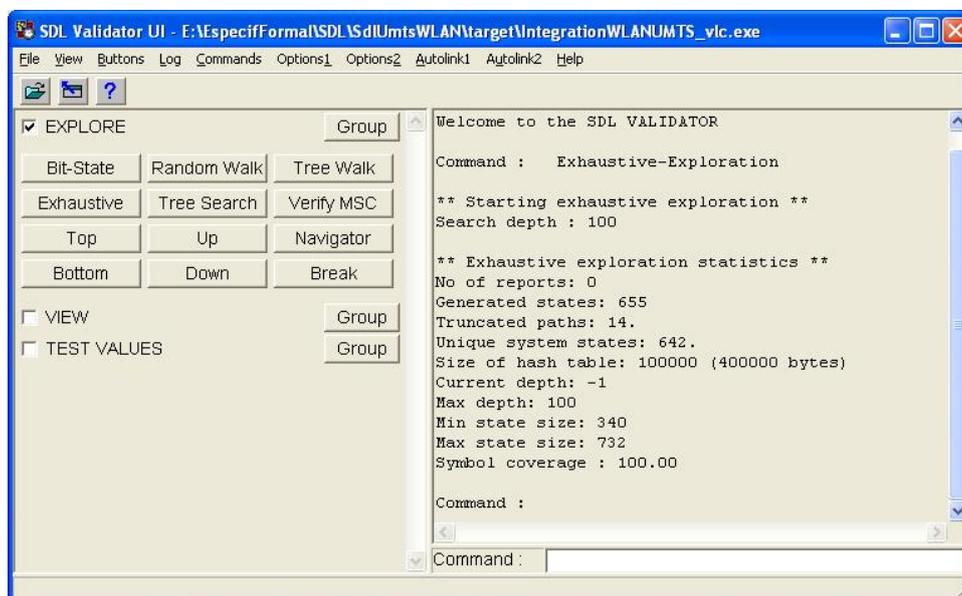


Figura 5.21 Validação utilizando o algoritmo *Exhaustive*

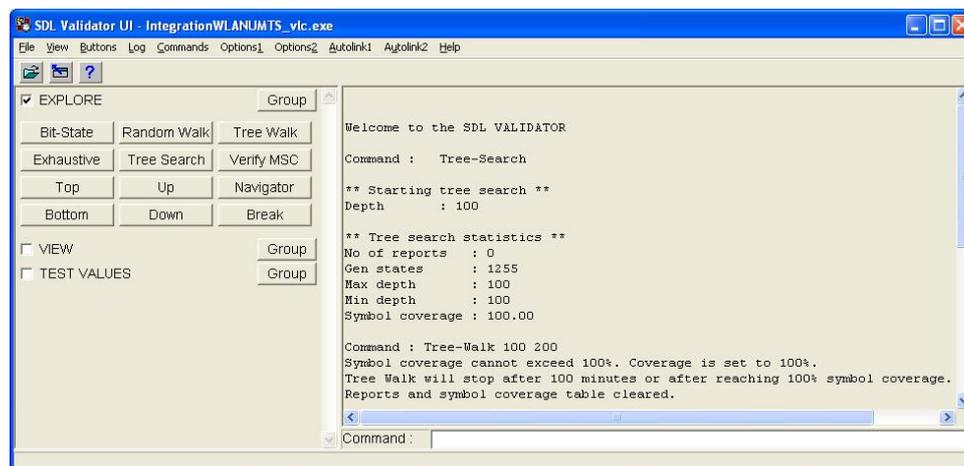


Figura 5.22 Validação utilizando o algoritmo *Tree Search*

## CAPÍTULO 6

# CONSIDERAÇÕES FINAIS

Este capítulo apresenta as considerações finais desta dissertação. A Seção 6.1 descreve as contribuições e os resultados alcançados com a proposta desta dissertação que descreve duas abordagens de gerenciamento de mobilidade para a integração das redes UMTS e IEEE 802.11. Já a Seção 6.2 apresenta os trabalhos futuros que podem ser iniciados a partir das questões motivadas e das observações extraídas da pesquisa desenvolvida.

### 6.1 CONTRIBUIÇÕES E RESULTADOS ALCANÇADOS

Este trabalho propôs duas abordagens para o gerenciamento de mobilidade na integração das redes UMTS e IEEE 802.11: uma baseada no SIP e a outra no MIPv6. A principal contribuição foi a extensão da arquitetura *Loose Interworking*, onde a WLAN não reutiliza os recursos internos da rede celular e, portanto, requer suporte externo para o gerenciamento da mobilidade, o qual neste trabalho foi representado pela utilização dos protocolos MIPv6 e SIP. A inserção do gerenciamento de mobilidade torna esta arquitetura compatível com as recomendações do nível 4 do 3GPP. A arquitetura resultante foi denominado de *Mob4Loose*.

Este trabalho também apresentou uma nova entidade para a arquitetura *Mob4Loose*, a *Converge*, que oferece um melhor serviço ao usuário 3G na rede IEEE 802.11. Os benefícios do uso dessa entidade podem ser descritos em duas etapas do seu comportamento: uma referente à economia de energia do dispositivo; e a outra referente ao nível de serviço prestado pela WLAN, onde o sinal para transmissão de dados passa a ser oferecido em um limite aceitável.

Finalmente, é importante ressaltar que a especificação do processo de *handoff* entre as redes componentes da *Mob4Loose* foi feita utilizando as linguagens formais MSC e SDL. A especificação em SDL e respectivas simulação e validação foram realizadas utilizando a ferramenta Tau SDL *Suite*. Os procedimentos detectaram erros, como perda de

sinais e *deadlocks*, os quais foram prontamente solucionados com a ajuda da ferramenta, resultando em uma especificação em SDL consistente com os cenários gerados em diagramas de seqüência a partir dos requisitos do nível 4 do 3GPP que prevêem o gerenciamento de mobilidade. O processo de *handoff* entre as redes UMTS e IEEE 802.11 de acordo com as duas abordagens propostas nesta dissertação com MIPv6 e SIP foi, portanto, formalmente validado.

## 6.2 TRABALHOS FUTUROS

Como sugestão para trabalhos futuros, o primeiro ponto importante é o mapeamento dos requisitos de QoS a serem oferecidos pelas redes IEEE 802.11 com os requisitos de QoS das redes celulares UMTS, que representa o nível 5 da especificação do 3GPP. Isto pode ser verificado através de uma análise do que as redes IEEE 802.11e podem oferecer, considerando os requisitos de QoS fornecidos ao usuário nas redes 3G.

A integração entre o sistema UMTS e as redes IEEE 802.11 *Ad Hoc* também representa um desafio, pois estas redes, diferentemente das infra-estruturadas, foco desta dissertação, não apresentam uma entidade central (e.g., ponto de acesso) na sua arquitetura para o controle da comunicação.

Outro importante trabalho futuro seria analisar a integração dos sistemas para o acesso aos serviços de comutação por circuitos de uma WLAN (i.e., o usuário poderia fazer uma chamada de voz de uma WLAN), que representa o nível 6 da especificação do 3GPP. Este pode representar um dos maiores desafios nesse processo de integração.

O processo de autenticação também deve ser considerado, já que representa grande parte do atraso gerado no *handoff* entre sistemas heterogêneos. Dessa forma, seria interessante avaliar os passos da autenticação e criar de um técnica visando diminuir o retardo desse processo.

Finalmente, a realização de testes em um ambiente real para avaliar na prática o processo de *handoff* entre redes heterogêneas também seria um trabalho futuro interessante. Atualmente, está sendo implantado um *testbed* na Universidade Federal do Ceará para verificar a validade da proposta deste trabalho em um ambiente real. As métricas de desempenho a serem avaliadas são a latência gerada durante o *handoff* e a perda de pacotes. Desse modo, os desempenhos dos protocolos MIP e SIP também poderão ser comparados.

## REFERÊNCIAS BIBLIOGRÁFICAS

- [1] H. Kaaranen, S. Naghian, L. Laitinen, A. Ahtiainen, and V. Niemi. *UMTS Networks: Architecture, Mobility and Services*. John Wiley and Sons, 2nd edition, 2005. 422 pages.
- [2] M. Abid, S. Sulistyono, and W. Najib. Security in Core Network and UTRAN. *3GWorld Technical Report*, nov 2002. <http://www.geocities.com/warsunnajib/Warsun2file/SecuritSolutioiUMTS-Report.pdf>.
- [3] INTEL. Intel corporation. <http://www.intel.com/>. Last access in June, 2007.
- [4] J. Arkko and H. Haverinen. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (eap-aka). *RFC 4187*, January 2006.
- [5] ETSI TR101.957. Requirements and Architectures for Interworking between Hiper-LAN/2 and 3rd Generation Cellular Systems. August 2001.
- [6] J. Song, S. Lee, and D. Cho. Hybrid Coupling Scheme for UMTS. *Vehicular Technology Conference*, 4:2247–2251, October 2003.
- [7] P. Pinto, L. Bernardo, and P. Sobral. Seamless Continuity of PS-services in WLAN/3G Interworking. *Computer Communications*, 29(8):1055–1064, may 2006.
- [8] M. Poikselka, G. Mayer, H. Khartabil, and A. Niemi. *The IMS IP Multimedia Concepts and Services in the Mobile Domain*. John Wiley and Sons, 2nd edition, 2006. 466 pages.
- [9] L. Doldi. *Validation of Communications Systems with SDL: The Art of SDL Simulation and Reachability Analysis*. John Wiley and Sons, 2003.
- [10] 3GPP TR22.934. Feasibility Study on 3GPP System to WLAN Interworking (Release 6). September 2003.

- 
- [11] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. *IETF RFC 3261*, June 2002.
- [12] F. G. MARQUEZ and et al. Interworking of IP Multimedia Core Networks between 3GPP and WLAN. *IEEE Wireless Communications*, june 2005.
- [13] IEEE. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std*, 1997. IEEE Standard 802.11.
- [14] D. Axiotis, T. Al-Gizawi, K. Peppas, E. Protonotarios, F. Lazarakis, C. Papadias, and P. Philippopoulos. Services in interworking 3G and WLAN environments. *IEEE Wireless Communications*, 11(5):14–20, 2004.
- [15] IEEE. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. *IEEE Std*, 1999. IEEE Standard 802.11b.
- [16] 3GPP. Wireless Local Area Network (WLAN) Interworking Security. *3GPP TS 33.234*, 2005. [http://www.3gpp.org/ftp/tsg\\_sa/WG3\\_Security/TSGS3\\_26\\_Oxford/Docs/PDF/S3-020695.pdf](http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_26_Oxford/Docs/PDF/S3-020695.pdf).
- [17] 3GPP2 X.S0028-200-0. cdma2000 Packet Data Services: Wireless Local Area Network (WLAN) Interworking - Access to Operator Service and Mobility. April 2007. [http://www.3gpp2.org/Public\\_html/specs/X.S0028-200-0\\_v1.0\\_070405.pdf](http://www.3gpp2.org/Public_html/specs/X.S0028-200-0_v1.0_070405.pdf).
- [18] C. Perkins, P. Roberts, and B. Patil. IP Mobility Support for IPv4. *IETF RFC 3220*, August 2002.
- [19] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. *IETF RFC 3775*, 2004.
- [20] S. J. Koh, H. Y. Jung, S. H. Kim, and J. S. Lee. Sctp with mobile ip for ip mobility support. *IETF Internet Draft*, feb 2003. draftsjkoh-mobile-sctp-mobileip-00.txt.
- [21] A. Snoeren and H. Balakrishnan. TCP Connection Migration. *Network and Mobile Systems Group at the MIT Laboratory for Computer Science*, November 2000.
- [22] I. Sommerville. *Software Engineering*. Pearson Education, 8th edition, 2006.

- 
- [23] ITU. Message Sequence Charts - MSC. *ITU-T Recommendation Z.120*, November 1999.
- [24] ITU. International Telecommunications Union. <http://www.itu.int/>, 2006. Last access in December, 2006.
- [25] ITU. Specification and Description Language - SDL. *ITU-T Recommendation Z.100*, August 1992.
- [26] Telelogic. TAU Generation. <http://www.telelogic.com>, 2006. Last access in March, 2006.
- [27] A. D. Nogueira, S. Ramos, B. Góis, M. Castro, and R. Andrade. Integração das Redes UMTS e IEEE 802.11 utilizando os protocolos MIPv6 e SIP. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, XXV, may 2007. SBRC 2007.
- [28] UMTS. UMTS. <http://www.umtsworld.com/>, 2006. Last access in March, 2006.
- [29] C. U. X. Zou, N. A. Hsu, N. M. Chen, R. X. Wei, D. X. Lu, K. C. Jang, and D. M. BCMCS. 3gpp2 cdma2000 tsg-c.
- [30] CDG. Cdma development group. <http://www.cdg.org/>. Last access in June, 2007.
- [31] K. Feher. Modulation and spread spectrum applications. *Wireless Digital Communications*, 1995. Prentice Hall.
- [32] 3GPP. Security architecture. *3GPP TS 33.102*. <http://www.3gpp.org/ftp/Specs/html-info/33102.htm>.
- [33] W. Najib, S. Sulistyono, and M. Abid. UMTS Security in Core Network and UTRAN. *Technical Report from 3World for Tele 3G*, November 2002.
- [34] IEEE. Wireless Personal Area Networks. *IEEE Std*, 2003. IEEE Standard 802.15.
- [35] IEEE. Wireless MAN. *IEEE Std*, 2004. IEEE Standard 802.16.
- [36] IEEE. Mobile Broadband Wireless Access (MBWA). *IEEE Std*, 2003. IEEE Standard 802.20.
- [37] IEEE. Wireless Personal Area Networks. *IEEE Std*, 2003. IEEE Standard 802.15.1.
- [38] ETSI. Hiperman Wireless Standard. <http://portal.etsi.org/radio/hiperman/hiperman.asp>.

- 
- [39] Nortel Networks. Secure network for wireless lans in the enterprise. 2003.
- [40] IEEE. IEEE Standard for Local and Metropolitan Area Network, Port-Based Network Access Control. *IEEE Std*, 2001. IEEE Standard 802.1x.
- [41] Y.K. Kim and R. Prasad. *4G Roadmap and Emerging Communication Technologies*. Artech House, 2006.
- [42] S. Frattasi, H. Fathi, F. H. P. Fitzek, M. Katz, and R. Prasad. Defining 4g technology from the user perspective. *IEEE Network Magazine*, 2006.
- [43] M. Katz and F.H.P. Fitzek. On the definition of the fourth generation wireless communications networks: The challenges ahead. *International Workshop on Convergent Technology (IWCT)*, 2005.
- [44] J. F. Huber. Mobile next-generation networks. *IEEE Computer Society*, 11(1):72–83, 2004.
- [45] E. Gustafsson and A. Jonsson. Always best connected. *IEEE Wireless Communications*, 10(1):49–55, feb 2003.
- [46] Nokia. Nokia. <http://forum.nokia.com/devices/N95>, 2006. Last access in December, 2006.
- [47] Yi Wu. An Improved TCP Migrate Scheme with DNS Handover Assistant for End-to-End Mobility. *NSO3P Network Services and Operations Symposium Po*, June 2007.
- [48] L. Ma, F. Yu, V. Leung, and T. Randhawa. A new method to support umts/wlan vertical handover using sctp. *IEEE Wireless Communications*, 11(4):44–51, Aug 2004.
- [49] Y. Gyekye and J. I. Agbinya. An improved tcp migrate scheme with dns handover assistant for end-to-end mobility. *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies*, 2006.
- [50] S. Faccin, P. Lalwaney, and B. Patil. IP Multimedia services: Analysis of Mobile IP and SIP interactions in 3G networks. *IEEE Communications Magazine*, 42(1):113–120, jan 2004.

- 
- [51] J. C. Chen and Zhang. T. *IP-Based Next-Generation Wireless Networks: Systems, Architectures, and Protocols*. Wiley, 2004. 440p.
- [52] P. MIKKA and et al. *The IMS IP Multimedia Concepts and Services in the Mobile Domain*. Wiley, 2004. 448p.
- [53] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry. The COPS (Common Open Policy Service) Protocol. *RFC 2748*, 2000.
- [54] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko. Diameter Base Protocol. *RFC 3588*, sept 2003. <http://www.ietf.org/rfc/rfc3588.txt>.
- [55] C. Groves, M. Pantaleo, and T. Anderson. Gateway control protocol version 1. *RFC 3525*, jun 2003. <http://www.ietf.org/rfc/rfc3525.txt>.
- [56] 3GPP TS24.229. Internet protocol (IP) multimedia call control protocol based on session initiation protocol (SIP) and session description protocol (SDP). 2005.
- [57] J. Peterson. A Privacy Mechanism for the Session Initiation Protocol (SIP). *RFC 3323*, nov 2002. <http://www.ietf.org/rfc/rfc3323.txt>.
- [58] R. Price, C. Bormann, J. Christoffersson, H. Hannu, Z. Liu, and J. Rosenberg. Signaling compression (sigcomp). Technical report, jan 2003. <http://www.ietf.org/rfc/rfc3320.txt>.
- [59] J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, and T. Haukka. Security mechanism agreement for the session initiation protocol (sip). Technical report, jan 2003. <http://www.ietf.org/rfc/rfc3329.txt>.
- [60] H. Schulzrinne and E. Wedlund. Application-layer mobility using sip". *IEEE Service Portability and Virtual Customer Environments*, pages 1–9, 2001.
- [61] E. GWedlund and H. Schulzrinne. Mobility support using sip. *ACM/IEEE International Conference on Wireless and Mobile Multimedia*, pages 1–7, 1999.
- [62] B. Carpenter and C. Jung. Transmission of IPv6 over IPv4 Domains without Explicit Tunnels. *IETF RFC 2529*, March 1999.
- [63] D. Manolescu, M. Voelter, and J. Noble. *Pattern Languages of Program Design 5*. Software Patterns Series. Addison Wesley, April 2006. 624 pages.

- [64] 3GPP S3-020549. On the Security of EAP/SIM and EAP/AKA and their use in the WLAN-3G Interworking. *3GPP TSG SA WG3 Security*, October 2002.
- [65] D. Amyot, R. Andrade, L. Logrippo, and J. Sincennes. Formal Methods for Mobility Standards. *Wireless Communications and Systems*, 1999.
- [66] ETSI. Methods for Testing and Specification (MTS). *The Testing and Test Control Notation version3. Part1: TTCN-3 Core Language*, aug 2002.
- [67] J. Grabowski, D. Hogrefe, G. Réthy, I. Schieferdecker, A. Wiles, and C. Willcock. An Introduction to the Testing and Test Control Notation (TTCN-3). *Computer Networks*, 42(3):375–403, 2003.