MARCEL STEFAN WAGNER

Influência de Protocolos de Segurança Sobre o
Desempenho de Redes UMTS

Dissertação apresentada à Escola
Politécnica da Universidade de São Paulo
para obtenção do Título de Mestre em
Engenharia.

São Paulo
2009

MARCEL STEFAN WAGNER

Influência de Protocolos de Segurança Sobre o
Desempenho de Redes UMTS

Dissertação apresentada à Escola
Politécnica da Universidade de São Paulo
para obtenção do Título de Mestre em
Engenharia.

Área de concentração: Engenharia de
Sistemas Eletrônicos.

Orientador: Prof. Dr. Wagner Luiz Zucchi

São Paulo
2009

AUTORIZO A REPRODUÇÃO E DIVULGAÇÃO TOTAL OU PARCIAL DESTE TRABALHO, POR QUALQUER MEIO CONVENCIONAL OU ELETRÔNICO, PARA FINS DE ESTUDO E PESQUISA, DESDE QUE CITADA A FONTE.

FICHA CATALOGRÁFICA

Wagner, Marcel Stefan

Influência de protocolos de segurança sobre o desempenho de redes UMTS / M.S. Wagner. -- São Paulo, 2009.

141 p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1.Engenharia elétrica 2.Telecomunicações 3.Telefonia celular 4.Telefonia móvel I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Sistemas Eletrônicos II.t.

DEDICATÓRIA

Dedico este trabalho ao meu irmão Jean e
a meus pais Eldon e Jane.

AGRADECIMENTOS

“Dê o primeiro passo com fé. Você não precisa ver toda a escada. Apenas suba o primeiro degrau”
Martin Luther King Jr.

A Deus, por me oferecer tantas alegrias e disponibilizar sempre um caminho para seguir, mesmo nos momentos mais difíceis.

Aos meus pais Eldon e Jane, por me proporcionarem as condições para crescer, estudar, sonhar e, mais do que isso, realizar os sonhos. À minha mãe pela dedicação nas horas mais complicadas, auxiliando nas decisões e conquistas.

Ao meu irmão Jean, pelo apoio, incentivo e auxílio durante a confecção deste trabalho e, também, à família do meu irmão, por sempre me acolherem com muito carinho.

Ao Dr. Edson, pelo apoio e atenção prestada para a minha evolução educacional.

À ANATEL, em especial ao Dr. Francisco Montoni, por permitir dedicar parte do meu tempo ao estudo referente às disciplinas cursadas no Programa de Mestrado, importantes para obtenção dos créditos necessários e, aos estudos e pesquisas realizadas ao longo deste trabalho.

À UNIP, em especial ao Carlão e Marcão, ambos do laboratório de física, por me proporcionarem mais tempo para me dedicar às pesquisas deste trabalho.

Às pessoas que indiretamente me ajudaram de alguma forma para o sucesso desta obra.

Por fim, mas não menos importante, agradeço ao meu orientador e amigo, Prof. Dr. Wagner Luiz Zucchi, pela oportunidade fornecida de ingressar no Programa de Mestrado da USP, pela orientação, compreensão e ensinamentos. Que este obrigado, que já não é o primeiro, não seja o último, mas sim o início de uma duradoura parceria.

RESUMO

Este trabalho analisa a influência de mecanismos de segurança, incluindo autenticação de assinante, confidencialidade e integridade de dados, sobre o desempenho do sistema celular de terceira geração *Universal Mobile Communication System* (UMTS).

Em função do serviço e do tamanho das chaves utilizadas foram medidos, através de simulação, o nível de potência gasto pelos equipamentos de usuário (UE) e o tempo de resposta em aplicações do tipo Web.

Verificou-se que os efeitos negativos produzidos pelos mecanismos de segurança são pequenos em relação à proteção maior que é obtida nos sistemas UMTS *Terrestrial Radio Access Network* (UTRAN) e *Core Network* (CN).

Palavras-chave: UTRAN; UMTS; Segurança; Algoritmo MILENAGE; *kernel* KASUMI.

ABSTRACT

This work is aimed at analyzing the influence of security mechanisms, including user authentication, data confidentiality and integrity, related to system cellular performance of third generation named Universal Mobile Telecommunication System (UMTS).

By the service and the size of the used keys, there has been measured through simulation, the power level spent by the user equipments and the response time at web applications usage.

It is seen that negative results produced by security mechanisms are small related to the greater protection that is get on UMTS Terrestrial Radio Access Network (UTRAN) systems and Core Network (CN).

Keywords: UTRAN; UMTS; Security; Algorithm MILENAGE; *kernel* KASUMI.

LISTA DE FIGURAS

Figura 1.	Arquitetura do Sistema Móvel GSM.	33
Figura 2.	Exemplo de uma BTS ou ERB.	34
Figura 3.	Canais disponíveis para faixa de 900MHz.	35
Figura 4.	Canais disponíveis para faixa de 1800MHz.	35
Figura 5.	Canais disponíveis para faixa de 1900MHz.	36
Figura 6.	Canais disponíveis para faixa de 2100MHz.	37
Figura 7.	Interface entre canais lógicos e físicos no GSM.	37
Figura 8.	Interfaces da arquitetura GSM.	38
Figura 9.	Interfaces e serviços da arquitetura GSM.	39
Figura 10.	Estrutura de protocolos do SS7.	40
Figura 11.	Fator de reuso 12 (razão de reuso 6,00).	42
Figura 12.	Fator de reuso 7 (razão de reuso 4,58).	42
Figura 13.	Arquitetura do sistema móvel GPRS.	46
Figura 14.	Arquitetura do modelo OSI.	46
Figura 15.	Comparação entre as arquiteturas OSI e TCP/IP.	49
Figura 16.	Classes de endereços IP e máscaras (<i>mask</i>) padrão de subrede.	50
Figura 17.	Demonstração da árvore de nomes do DNS.	51
Figura 18.	Cabeçalhos do IPv4 e IPv6.	52
Figura 19.	Encapsulamento de pacotes IPv6 em IPv4 (<i>tunneling</i>).	53
Figura 20.	Interfaces e serviços da arquitetura GPRS.	54
Figura 21.	Interfaces e serviços da arquitetura EDGE (<i>release 4</i>).	55
Figura 22.	Evolução dos padrões de tecnologias celulares.	57
Figura 23.	Arquitetura do CDMA2000 1xRTT.	59
Figura 24.	Arquitetura do CDMA2000 1xEV-DO.	59
Figura 25.	Evolução do CDMA2000 1xEV-DO para o UMB.	60
Figura 26.	Arquitetura completa do UMTS (sem interligação com o EDGE).	61
Figura 27.	Estrutura dos canais da UTRAN.	63
Figura 28.	Mapeamento dos canais nos enlaces direto e reverso do UMTS.	66
Figura 29.	Distribuição das camadas do WCDMA.	67
Figura 30.	Distribuição das camadas e dos canais do WCDMA.	67
Figura 31.	Exemplo simplificado de recebimento de chamada no UMTS.	68
Figura 32.	Modos de transmissão FDD e TDD do UMTS.	70
Figura 33.	Árvore usada na geração de códigos OVSF.	71
Figura 34.	Ilustração do cálculo do <i>Spreading Factor</i> (SF).	72
Figura 35.	Arquitetura do UMTS com interface GERAN (<i>release 4</i>).	72
Figura 36.	Arquitetura do UMTS com interface GERAN (<i>release 5</i>).	73
Figura 37.	Arquitetura do UMTS com interface VoIP.	74

Figura 38. Arquitetura IMS.....	76
Figura 39. Arquitetura <i>All-IP</i>	77
Figura 40. Arquitetura e modelo de referência WAP1.	78
Figura 41. Comparação entre as arquiteturas WAP1 e WAP2.	79
Figura 42. Evolução até o HSDPA e tendências.....	81
Figura 43. Alocação de banda sugerida pela WRC2000.....	81
Figura 44. Identificação e autenticação do usuário no GSM.	86
Figura 45. Uso do A5 como gerador de chaves.	86
Figura 46. Algoritmos usados na autenticação e encriptação do GSM.....	87
Figura 47. Identificação do IMSI.	87
Figura 48. Troca de informações de segurança no UMTS (camadas internas).	88
Figura 49. Troca de informações de segurança no UMTS (visão geral).	89
Figura 50. Compartilhamento da chave secreta K (de 128bits) entre HN e HE.	89
Figura 51. Visão geral do AKA no UMTS.	91
Figura 52. Segurança de acesso no UMTS.	92
Figura 53. Encriptação dos dados no UMTS.	93
Figura 54. Integridade dos dados no UMTS.	94
Figura 55. Algoritmo KASUMI.....	95
Figura 56. f8 com uso do <i>kernel</i> KASUMI.....	96
Figura 57. f9 com uso do <i>kernel</i> KASUMI.....	96
Figura 58. Estrutura do algoritmo Rijndael (AES).	98
Figura 59. Algoritmo MILENAGE com o uso do <i>kernel</i> AES Rijndael.	100
Figura 60. Visão geral da comunicação e troca de sinalização entre UTRAN e NSS.....	104
Figura 61. Cenário inicial da configuração da rede UMTS com dois UE no software OPNET.	106
Figura 62. Cenário mostrando a UTRAN (apresentando quatro UE, um <i>Node-B</i> e um RNC).	107
Figura 63. Estrutura interna do UE.	108
Figura 64. Estrutura interna do <i>Node-B</i>	108
Figura 65. Estrutura interna do RNC.	109
Figura 66. Estrutura interna do SGSN.	109
Figura 67. Estrutura interna do GGSN.....	110
Figura 68. Estrutura interna do NSS (conjunto MSC, HLR, AuC e EIR, localizados no bloco UTRAN).	111
Figura 69. <i>Finite State Machine</i> (FSM) do módulo MSC (estrutura interna do NSS).	112
Figura 70. <i>task_definition</i> com as configurações internas.	114
Figura 71. <i>task_definition</i> com as configurações internas (função f8 de confidencialidade).	114

Figura 72. <i>task_definition</i> com as configurações internas (função f9 de integridade).....	115
Figura 73. <i>task_definition</i> com as configurações internas (função de autenticação MILENAGE com AES).	115
Figura 74. Cenário UMTS com dois UE.....	116
Figura 75. Cenário UMTS com quatro UE.	116
Figura 76. Cenário UMTS com dez UE.....	116
Figura 77. Cenário UMTS com vinte UE.	116
Figura 78. Cenário UMTS com quarenta UE.....	116
Figura 79. Cenário UMTS com sessenta UE.	116
Figura 80. Comparativo dos cenários de segurança com relação à potência e ao número de UE.	118
Figura 81. Comparativo dos cenários de segurança com relação aos acessos a páginas HTTP.	120
Figura 82. Comparativo dos cenários de segurança com relação às requisições de objetos HTTP.....	121
Figura 83. Comparativo dos cenários de segurança com relação ao atraso de voz fim-a-fim.	122
Figura 84. Comparativo dos cenários de autenticação (atraso de voz fim-a-fim).	123
Figura 85. Comparativo dos cenários de autenticação, confidencialidade e integridade (atraso de voz fim-a-fim).....	123
Figura 86. Comparativo dos cenários de segurança com relação à variação de atraso.....	124
Figura 87. Comparativo dos cenários de segurança com relação à variação de atraso do MILENAGE.	124
Figura 88. Comparativo dos cenários de segurança com relação à variação de atraso do MILENAGE/KASUMI.	125
Figura 89. Elementos da definição da máquina de estados.....	133
Figura 90. Diagrama e tabela de transição de estados.	134
Figura 91. Modelo de Moore.	135
Figura 92. Modelo de Mealy.....	136
Figura 93. Estrutura de camadas ATM.	139

LISTA DE TABELAS

Tabela 1 – Quantidade de acessos e conexões em uso no Brasil.....	27
Tabela 2 – Quantidade de aparelhos celulares por tecnologia no Brasil.	27
Tabela 3 – Padrões de tecnologia celular adotados no mundo.	35
Tabela 4 – Divisão do sinal modulado e <i>slots</i> no GSM.....	37
Tabela 5 – Fator de reuso.....	43
Tabela 6 – Camadas do modelo OSI.	47
Tabela 7 – Camadas do modelo TCP/IP.....	48
Tabela 8 – Classes de endereços IP.	49
Tabela 9 – Blocos de endereços reservados CIDR.	51
Tabela 10 – Comparação entre IPv4 e IPv6.....	53
Tabela 11 – Padrões GSM e UMTS adotados no Brasil e no mundo.....	56
Tabela 12 – Interfaces da arquitetura do UMTS.....	62
Tabela 13 – Componentes da arquitetura do UMTS.	63
Tabela 14 – Canais Lógicos do UMTS (WCDMA).	64
Tabela 15 – Canais de Transporte do UMTS (WCDMA).	64
Tabela 16 – Canais Físicos do UMTS (WCDMA).	65
Tabela 17 – Comparação entre os modos de operação FDD e TDD do WCDMA.	69
Tabela 18 – Tabela de sequência de códigos C_i	71
Tabela 19 – Comparação entre os padrões utilizados em tecnologia celular.	83
Tabela 20 – Comparação entre UMTS WCDMA e CDMA2000 1xRTT.	83
Tabela 21 – Comparação entre UMTS HSDPA e CDMA2000 1xEV-DV.	84
Tabela 22 – Comparação entre variadas tecnologias de transmissão sem fio.	84
Tabela 23 – Simbologia utilizada na segurança do UMTS.....	90
Tabela 24 – Parâmetros de f_8	93
Tabela 25 – Parâmetros de f_9	94
Tabela 26 – Potência de transmissão média no <i>uplink</i> para UE (RLC/MAC) por canal de radiofrequência (dBm).	119
Tabela 27 – Tempo de resposta médio para acesso a páginas HTTP (s).	120
Tabela 28 – Tempo de resposta médio para acesso a objetos HTTP (s).	121
Tabela 29 – Atraso médio na transmissão de voz fim-a-fim (ms).	122
Tabela 30 – Variação de atraso médio na transmissão de voz fim-a-fim (ms).	125

LISTA DE ABREVIATURAS E SIGLAS

16QAM	Quadrature Amplitude Modulation
1G	1ª Geração
1xEV-DO	Single-carrier Evolution-Data Optimized
1xEV-DV	Single-carrier Evolution-Data and Voice
1xRTT	Single-carrier Radio Transmission Technology
2,5G	2ª Geração a caminho do 3G
2,75G	2ª Geração a caminho do 3G
2G	2ª Geração
3DES	Triple Data Encryption Standard
3G	3ª Geração
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
8-PSK	Octagonal Phase Shift Keying
AAL	ATM Adaptation Layer
ACELP	Algebraic Code Excited Linear Prediction
ACK	Acknowledgement
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AF	Autômato Finito
AFD	Autômato Finito Determinístico
AFND	Autômato Finito Não Determinístico
AGCH	Access Grant Channel
AI	Acquisition Indicator
AICH	Acquisition Indicator Channel
AIR	Asynchronous Incremental Redundancy
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMC	Adaptative Modulation and Coding
AMF	Authentication Management Field
AMPS	American Mobile Phone System
AMR	Adaptive Multi Rate
Anatel	Agência Nacional de Telecomunicações
ANSI	American National Standards Institute
AP	Access Point
ARFCN	Absolute Radio Frequency Channel Number
ARIB	Association of Radio Industries and Business
ARP	Address Resolution Protocol
AS	Application Server

ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
ATM/IP	Asynchronous Transfer Mode/Internet Protocol
AuC	Authentication Center
AUTN	Authentication Token
AUTS	Authentication Token in re-Synchronization
AV	Authentication Vector
BCCH	Broadcast Control Channel
BCH	Broadcast Channel
BEMS	Bulk Encryption and MAC Suite
BG	Border Gateway
BLKCNT	Block Count
BMC	Broadcast and Multicast Control
bps	bits por segundo
BS	Base Station
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
BW	Bandwidth
CA	Certification Authority; Call Agent
CAL	Core Access Layer
CAMEL	Customised Application for Mobile network Enhanced Logic
CAP	CAMEL Application Part
CBC-MAC	Cipher Block Chain – Message Authentication Code
CCC	Central de Comutação e Controle
CCCH	Common Control Channel
CCH	Control Channel
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CD/CAICH	Collision Detection/Channel Assignment Indication Channel
CDI	Collision Detection Indicator
CDI/CAI	Collision Detection Indicator/Channel Assignment Indicator
CDM	Code Division Multiplexing
CDMA	Code Division Multiple Access
CDMA2000	Code Division Multiple Access 2000
CDMAone	Code Division Multiple Access de 2ª Geração
CIDR	Classless Inter-Domain Routing
CK	Cipher Key
CN	Core Network
CNG	Comfort Noise Generation
codec	codificador/decodificador
CPCH	Common Packet Channel

CPCS	Common Part Convergence Sublayer
CPICH	Common Pilot Channel
CS	Circuit Switched; Convergence Sublayer
CSCF	Call Session Control Function
CSE	CAMEL Service Environment
CS-GSM	Circuit Switched GSM
CSICH	CPCH Status Indication Channel
CTCH	Common Traffic Channel
D-AMPS	Digital American Mobile Phone System
dB	decibel
DCCH	Dedicated Control Channel
DCH	Dedicated Channel
DCS	Digital Cellular System
DEMUX	Demultiplexação
DES	Data Encryption Standard
DL	Downlink
DNS	Domain Name System
DPCCH	Dedicated Physical Control Channel
DPCH	Downlink Paging Channel
DPDCH	Dedicated Physical Data Channel
DQPSK	Differential QPSK
DS3	Digital Signal 3
DS-CDMA	Direct Sequence Code Division Multiple Access
DSCH	Downlink Shared Channel
DSSS	Direct Sequence Spread Spectrum
DTCH	Dedicated Traffic Channel
DTX	Discontinuous Transmission
E-AGCH	Enhanced Access Grant Channel
E-DCH	Enhanced Dedicated Channel
EDGE	Enhanced Data for GSM Evolution
E-DPCCH	Enhanced Dedicated Physical Control Channel
E-DPDCH	Enhanced Dedicated Physical Data Channel
EFR	Enhanced Full-Rate
E-GPRS	Enhanced General Packet Radio Service
EIA	Electronic Industries Alliance
EIR	Equipment Identity Register
EM	Estação Móvel
ERB	Estação Rádio-Base
E-SCD	Enhanced Circuit Switched Data
ETSI	European Telecommunication Standards Institute
EX-OR	Ou-Exclusivo

FACH	Forward Access Channel
FCC	Federal Communication Commission
FDD	Frequency Division Duplex
FDDI	Fiber Distributed Data Interface
FDMA	Frequency Division Multiple Access
FH	Frequency Hopping
FHSS	Frequency Hopping Spread Spectrum
FIGS	Fraud Information Gathering Services
FPUN	Free Phone and Universal Number
FSK	Frequency Shift Keying
FSM	Finite State Machine
FTP	File Transfer Protocol
GEA	GPRS Encryption Algorithm
GERAN	GSM/EDGE Radio Access Network
GF	Galois Field
GFC	Generic Flow Control
GGSN	Gateway GPRS Support Node
GHz	Giga Hertz
GMM	GPRS Mobility Management
GMSC	Gateway MSC
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GW	Gateway
HARQ	Hybrid Automatic Repeat reQuest
HDLC	High-level Data Link Control
HDR	High Data Rate
HE	Home Environment
HEC	Header Error Control
HLR	Home Location Register
HMAC	Hash Message Authentication Code
HN	Home Network
HPLMN	Home Public Land Mobile Network
HSDPA	High Speed Downlink Packet Access
HS-DPCCH	High Speed Dedicated Physical Control Channel
HS-DSCH	High Speed Downlink Shared Channel
HSPA	High Speed Packet Access
HS-PDSCH	High Speed Physical Downlink Shared Channel
HS-SCCH	High Speed Shared Control Channel
HSUPA	High Speed Uplink Packet Access

HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HW	Hardware
ICMP	Internet Control Message Protocol
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IK	Integrity Key
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IMT-2000	International Mobile Telecommunications – 2000
IN	Intelligent Network
IP	Internet Protocol
IPSec	IP Security Protocol
IPTV	Internet Protocol Television
IPv4	Internet Protocol versão 4
IPv6	Internet Protocol versão 6
IPX	Internetwork Packet Exchange
IR	Incremental Redundancy
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Intermediate Service Part; Internet Service Provider
ISUP	ISDN User Part
ITC	Intervalo de Tempo de Canal
ITU	International Telecommunication Union
ITU-R	International Telecommunication Union – Radiocommunications sector
ITU-T	International Telecommunication Union – Telecommunications sector
IV	Initialization Vector
IWMSC	Inter Working Mobile Switching Center
kbps	Kilo-bits per second
KES	Key Exchange Suite
kHz	kilo Hertz
KM	Key Modifier
KS	Keystream
LAI	Location Area Identity
LAN	Local Area Network
LAPD	Link Access Procedure D
LAPD mobile	Link Access Procedure D mobile
LLC	Logical Link Control

m	metros
MAC	Message Authentication Code; Medium Access Control
MAC-I	MAC Integrity
MAC-S	MAC in re-Synchronization
MAN	Metropolitan Area Network
MAP	Mobile Application Part
MBMS	Multimedia Broadcast/Multicast Service
Mbps	Mega-bits per second
MBWA	Mobile Broadband Wireless Access
MC-CDMA	Multicarrier Code Division Multiple Access
Mcps	Mega-chips per second
MD5	Message Digest 5
ME	Mobile Equipment
MEGACO	Media Gateway Control
MGCF	Media Gateway Control Function
MGCP	Media Gateway Control Protocol
MGW	Media Gateway
MHz	Mega Hertz
MICH	Multimedia Broadcast/Multimedia Service Indicator Channel
MIMO	Multiple-Input and Multiple-Output
MMe	Máquina de Mealy
MMo	Máquina de Moore
MMS	Multimedia Messaging Service
modem	modulador/demodulador
MPLS	Multi Protocol Label Switching
MRF	Multimedia Resource Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
ms	mili-segundos
MS	Mobile Station
MSC	Mobile Switching Center
MSK	Minimum Shift Keying
MTP	Message Transfer Part
MUX	Multiplexação
NACK	Non Acknowledgement
NAS	Non Access Stratum
NAT	Network Address Translator
NCL	Network Control Layer
NGN	Next Generation Network
NIST	National Institute of Standards and Technology
NMC	Network Management Center

NMT	Nordic Mobile Telephone
Node-B	equivalente à ERB ou BTS
NSA	National Security Agency
NSS	Network Subsystem
NW	Network
OC-3	Optical Carrier - 3
OFB	Output Feedback
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OMC	Operation and Management Center
OP	Operator
OQPSK	Offset Quadrature Phase Shift Keying
OSI	Open System Interconnection
OSS	Operator Specific Services
OVSF	Orthogonal Variable Spreading Factor
OWF	One-Way Function
P-CCPCH	Primary Common Control Physical Channel
P-CPICH	Primary Common Pilot Channel
P-TMSI	Packet TMSI
P2P	Point to Point
PA	Paging Area
PABX	Private Automatic Branch Exchange
PBX	Private Branch Exchange
PCCH	Paging Control Channel
PCH	Paging Channel
PCM	Pulse Code Modulation
PCPCH	Physical Common Packet Channel
PCS	Personal Communication System
PCSAC	Prepaid Card Service with Advice of Charge
PCU	Packet Control Unit
PDA	Personal Digital Assistant
PDCP	Packet Data Convergence Protocol
PDH	Plesiochronous Digital Hierarchy
PDN	Packet Data Network
PDP	Packet Data Protocol
PDSCH	Physical Downlink Shared Channel
PDU	Packet Data Unit; Protocol Data Unit
PES	PSTN Emulating Subsystem
PGO	Plano Geral de Outorgas
PHY	Physical layer
PICH	Paging Indicator Channel

PLMN	Public Land Mobile Network
PM	Physical Medium
PN	Pseudo-Noise
POP3	Post Office Protocol 3
PPP	Point-to-Point Protocol
PRACH	Physical Random Access Channel
PS	Packet Switched
PSC	Primary Synchronization Code
PSK	Phase Shift Keying
PSTN	Public Switched Telephone Network
PTM	Point To Multipoint
P-TMSI	Packet TMSI
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RACH	Random Access Channel
RAND	Random number
RARP	Reverse Address Resolution Protocol
RC5	Rivest Cipher 5
RDSI	Rede Digital de Serviços Integrados
RF	Radio Frequency
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RRC	Radio Resource Control
RSA	Rivest Shamir & Adleman
RTP	Real Time Protocol
RTPC	Rede Telefônica Pública Comutada
S/N	Signal/Noise ratio
S-CCPCH	Secondary Common Control Physical Channel
S-CPICH	Secondary Common Pilot Channel
SAP	Service Access Point
SAR	Segmentation and Reassembly
SCCP	Signalling Connection Control Part
SCH	Synchronization Channel
SCM	Serviço de Comunicação Multimídia
SDH	Synchronous Digital Hierarchy
SDMA	Spatial-Division Multiple Access
SDP	Service Data Function; Session Description Protocol
SF	Spreading Factor
SG	Signalling Gateway
SGSN	Serving GPRS Support Node
SHA-1	Secure Hash Algorithm 1

SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SM	Session Management
SMC	Serviço Móvel Celular
SML	Service/Management Layer
SMP	Serviço Móvel Pessoal
SMS	Short Message Service
SMSC	Short Message Service Center
SMS-GMSC	Short Message Service Gateway Mobile Switching Center
SMS-IW MSC	Short Message Service Interworking Mobile Switching Center
SMTP	Simple Mail Transfer Protocol
SN	Serving Network
SNMP	Simple Network Management Protocol
SPNP	Support Private Numbering Plan
SQN	Sequence number
SRES	Signed Response
SS	Spread Spectrum; Supplementary Service
SS7	Signalling System N°. 7
SSC	Secondary Synchronization Code
SSCS	Service Specific Convergence Sublayer
SSL	Secure Socket Layer
SVA	Serviço de Valor Adicionado
SW	Software
TACS	Total Access Communications Systems
TC	Transmission Convergence
TCAP	Transaction Capabilities Application Part
TCH	Traffic Channel
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TD-CDMA	Time Division Code Division Multiple Access
TDD	Time Division Duplex
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TFCI	Transport Format Combination Indicator
TIA	Telecommunication Industry Association
TLS	Transport Layer Security
TMN	Telecommunications Management Network
TMSI	Temporary Mobile Subscriber Identity
TPC	Transmit Power Control
TR	Truncate
TRAU	Transcoder Rate Adapter Unit

TTA	Telecommunications Technology Association
TUP	Telephone User Part
UDP	User Datagram Protocol
UE	User Equipment
UL	Uplink
UMB	Ultra Mobile Broadband
UMTS	Universal Mobile Telecommunication System
UNI	User-to-Network Interface
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
UTRA	Universal Terrestrial Radio Access
UTRA FDD	Universal Terrestrial Radio Access Frequency Division Duplex
UTRA TDD	Universal Terrestrial Radio Access Time Division Duplex
UTRAN	UMTS Terrestrial Radio Access Network
UWB	Ultra Wideband
UWCC	Universal Wireless Communications Consortium
VAD	Voice Activity Detection
VAS	Value Added Service
VC	Virtual Channel
VCi	Virtual Channel Identifier
VHE	Virtual Home Environment
VLR	Visitor Location Register
VLSM	Variable Length Subnet Mask
VMS	Voice Mail System
vocoders	voice codifiers
VoD	Video on-Demand
VoIP	Voice over IP
VP	Virtual Path
VPI	Virtual Path Identifier
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network
WAE	Wireless Application Environment
WAN	Wide Area Network
WAP	Wireless Application Protocol
WARC	World Administrative Radio Conference
WCDMA	Wideband Code Division Multiple Access
WCDMA FDD	Wideband Code Division Multiple Access Frequency Division Duplex
WCDMA TDD	Wideband Code Division Multiple Access Time Division Duplex
WDP	Wireless Datagram Protocol
Wi-Fi	Wireless Fidelity Alliance
WIM	WAP Identity Module

Wi-MAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WLL	Wireless Local Loop
WMAN	Wireless Metropolitan Area Network
WML	Wireless Markup Language
WPT	WAP-Profiled TLS
WRC	World Radiocommunication Conference
WSP	Wireless Session Protocol
WTDMA	Wideband Time Division Multiple Access
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol
WWAN	Wireless Wide Area Network
WWW	World Wide Web
XHTML	Extended HTML
XMAC	Expected MAC
XMAC-I	Expected MAC-I
XML	Extensible Markup Language
XRES	Expected Response
ZE	Zero-Extend

LISTA DE SÍMBOLOS

$\parallel$	Concatenação
$\oplus$	Ou-exclusivo (EX-OR)
$\cap$	bitwise AND operation
$\cup$	bitwise OR operation
A3	Algoritmo 3
A5	Algoritmo 5
A8	Algoritmo 8
E	Entry
f1	função para gerar MAC
f1*	função para gerar MAC-S
f2	função para gerar RES e XRES
f3	função para gerar CK
f4	função para gerar IK
f5	função para gerar AK
f5*	função para gerar AK em re-sincronização
f8	função de encriptação
f9	função de integridade
I	Input
K	Longo termo de chave secreta compartilhada entre o USIM e o AuC
K _c	Cipher Key
K _i	Integrity Key
ROL	rotação circular de bit à esquerda
rot	rotacional
Rx	Recepção
Tx	Transmissão
X	Exit

SUMÁRIO

1. Introdução	27
1.1. Justificativa	28
1.2. Contexto.....	29
1.3. Estrutura do Trabalho	31
2. Evolução até o UMTS	32
2.1. GSM.....	32
2.1.1. Arquitetura do GSM	32
2.1.2. Canalização e Distribuição de Canais	34
2.1.3. Interfaces do GSM.....	37
2.1.4. Capacidade do Sistema.....	41
2.1.5. Espalhamento Espectral.....	41
2.1.6. Fator de Reuso	42
2.1.7. Serviços Disponíveis no GSM.....	43
2.1.8. Considerações do GSM	44
2.2. GPRS	44
2.2.1. Dispositivos do GPRS	45
2.2.2. PLMN	45
2.2.3. Arquitetura do GPRS.....	45
2.2.4. Modelo OSI	46
2.2.5. Modelo TCP/IP.....	48
2.2.6. Interfaces do GPRS	53
2.2.7. Considerações do GPRS	54
2.3. EDGE.....	54
2.3.1. Arquitetura e Interfaces do EDGE	55
2.3.2. Considerações do EDGE	55
2.4. 3ª Geração	56
2.5. IMT-2000.....	57
2.6. CDMA2000	58
2.6.1. CDMA2000 1xRTT.....	58
2.6.2. CDMA2000 1xEV-DO.....	59
2.6.3. CDMA2000 1xEV-DV e UMB.....	60
2.6.4. Considerações do CDMA2000.....	60
2.7. UMTS	61
2.7.1. Arquitetura do UMTS.....	61
2.7.2. Canalização do UMTS WCDMA.....	63
2.7.3. WCDMA	69

2.7.4. Integração entre GERAN e UTRAN	72
2.7.5. IPsec	73
2.7.6. VoIP.....	74
2.7.7. IMS	75
2.7.8. All-IP.....	76
2.7.9. CAMEL	77
2.7.10. WAP	78
2.7.11. HSPA – HSDPA e HSUPA	80
2.7.12. Migração no Brasil	81
2.7.13. Considerações do UMTS.....	82
3. Conceitos e Características de Segurança.....	85
3.1. Mecanismos de Segurança.....	85
3.1.1. Segurança no GSM.....	85
3.1.2. Segurança no GPRS	87
3.1.3. Segurança no UMTS	87
3.1.3.1. Troca de Mensagens no UMTS	88
3.1.3.2. Autenticação – AKA	89
3.1.3.3. Função de Encriptação – f8	93
3.1.3.4. Função de Integridade – f9	93
3.1.3.5. Kernel Algoritmo KASUMI.....	94
3.1.3.6. f8 com KASUMI	96
3.1.3.7. f9 com KASUMI	96
3.1.3.8. Criptografia AES	97
3.1.3.9. Algoritmo MILENAGE.....	99
3.1.4. Considerações de Segurança	100
4. Modelagem dos Mecanismos de Segurança	102
5. Procedimentos e Simulação	106
6. Resultados Obtidos	118
7. Conclusão e Trabalhos Futuros	126
8. Referências	128
8.1. Livros.....	128
8.2. Artigos	129
8.3. Normas e Padrões	131
8.4. Acesso a Website.....	132
APÊNDICE I.....	133
FSM	133
Modelo de Moore	135
Modelo de Mealy.....	135

Considerações dos Modelos de Moore e Mealy	136
APÊNDICE II.....	138
ATM.....	138

1. Introdução

A rede de telefonia móvel teve grande crescimento durante as últimas décadas, evoluindo tão rapidamente que chegou a ultrapassar até mesmo o número de terminais da rede de telefonia fixa no Brasil, o que demonstra o grau e a tendência de evolução na quantidade de usuários dos respectivos serviços (ver Tabela 1). Com base nos dados apresentados e com a informação da Tabela 2, pode-se concluir que a telefonia celular apresenta grande potencial como tecnologia de acesso e, dentre as tecnologias celulares utilizadas ainda hoje no Brasil, o *Global System for Mobile Communication* (GSM) é sem dúvida a melhor opção, podendo ser usado inclusive na migração para o padrão *Universal Mobile Telecommunication System* (UMTS).

Tabela 1 – Quantidade de acessos e conexões em uso no Brasil.

(Dados em Milhões)	2003	2004	2005	2006
Telefones Fixos	39,2	39,6	39,6	38,5
Telefones Celulares	46,4	65,6	86,2	99,9
TV por Assinatura	3,5	3,8	4,2	4,6
Banda Larga	1,2	2,3	3,8	5,6
Usuários de Internet	-	-	32,1	32,8

Fonte: Site <http://www.teleco.com.br/> – Seção de Telecomunicação (consulta em 05/01/2008). Baseado em dados estatísticos do Instituto Brasileiro de Geografia e Estatística (IBGE).

A procura por produtos que oferecem facilidade de mobilidade voltada para comunicação está cada vez mais intensa. Especialmente nesta última década o consumidor passou a exigir mais alcance, mobilidade e tecnologia de softwares para transferência de arquivos e transações financeiras entre diferentes fabricantes de equipamentos móveis (aparelhos celulares, *Personal Digital Assistant* (PDA), etc.) e, também, das diversas operadoras de Serviço Móvel Celular (SMC). O SMC, devido à alteração de denominação feita pela Anatel, passou a chamar-se de Serviço Móvel Pessoal (SMP) [RSMP 07].

Tabela 2 – Quantidade de aparelhos celulares por tecnologia no Brasil.

Tecnologia Celular	Dezembro/2006	Novembro/2007			
		Nº. Celulares		Cresci./mês	Cresci./ano
AMPS	61.462	22.965	0,02%	-437	-62,64%
TDMA	10.308.448	5.557.225	4,78%	-408.929	-46,09%
CDMA	26.004.137	21.505.544	18,49%	-586.358	-17,30%
GSM	63.544.574	89.228.093	76,71%	2.619.247	40,42%
Total	99.918.621	116.313.827	100%	1.623.523	16,41%

Fonte: Site <http://www.teleco.com.br/> – Seção de Telefonia Celular (consulta em 05/01/2008). Baseado em dados estatísticos do Instituto Brasileiro de Geografia e Estatística (IBGE).

Dentro deste cenário, existe a necessidade da proteção das informações de usuário (voz e dados) e mecanismos internos da rede. Para que exista esta proteção, foram aproveitadas no UMTS algumas características de segurança do GSM, que serão mostradas na seção 3.1.

Além do aproveitamento das características de segurança do GSM, o UMTS provém segurança na autenticação de usuários (com o uso de funções de autenticação, troca de desafios, números randômicos e seqüências numéricas), encriptação de dados (utilizando funções de encriptação, inclusive com o algoritmo KASUMI na estrutura interna) e integridade de dados (utilizando funções de integridade, também com o uso do algoritmo KASUMI na estrutura interna).

Na autenticação e geração de chaves, o conjunto de algoritmos que formam o MILENAGE [T205 05], com o uso interno do *Advanced Encryption Standard* (AES) que, por sua vez, é composto pelo algoritmo Rijndael, vem sendo a base de estudos relacionados à segurança no 3G, por tratar-se de um conjunto de algoritmos destinados à encriptação de blocos. A descrição do MILENAGE está no tópico 3.1.3.9.

1.1. Justificativa

Este projeto de pesquisa visa ao estudo de mecanismos e características de segurança presentes no ambiente móvel celular de 3ª Geração (3G), padrão UMTS, relacionados ao desempenho do ponto de vista do usuário, através de análises de atraso fim-a-fim no tráfego de voz e dados e, também, tempo de resposta para requisições de aplicações disponíveis em servidores de informações conectados à rede, utilizando-se, para isto, dispositivos internos da rede UMTS que serão descritos nos próximos tópicos.

O UMTS iniciou sua implantação no Brasil utilizando a planta já instalada da rede GSM com o uso de parâmetros de segurança mais avançados e acréscimo de algumas características que o GSM prevê e não contempla o uso contínuo. A topologia desse novo sistema é baseada em uma arquitetura mista de células, ou seja, células variando o tamanho conforme a necessidade de alcance, sendo, portanto, implementadas com dimensionamento adequado para áreas geográficas específicas e em função das diferentes demandas de tráfego, dando às prestadoras de serviços um leque de ferramentas para o dimensionamento e otimização do sistema.

A pesquisa estende-se às necessidades do mercado nacional no que tange à utilização de celulares cada vez mais incrementados com serviços (*Service Recommender*, *Multimedia*

Messaging Service (MMS), Short Message Service (SMS), Personalized ads, Photo Tagging, Mobile Tagging, Photo Browsing, entre outros) e programas (jogos e aplicativos), bem como, dispositivos operacionais de última geração implementando técnicas de transferência de voz, dados, arquivos de imagem, áudio e vídeo. Vale salientar que os dispositivos serão utilizados cada vez mais para receber ou fornecer informações sigilosas, como transações financeiras, códigos, catálogos, informações pessoais e outros, o que acarreta na necessidade de possuir-se uma rede robusta e prevenida contra ataques ou ameaças de segurança.

Diante dessa gama de motivações e da necessidade de aplicações que possam garantir segurança sem prejudicar o desempenho da rede, deseja-se estudar o comportamento da rede UMTS em diversas situações descritas na modelagem dos mecanismos de segurança, efetuando-se um conjunto de estudos sobre redes de última geração a serem realizados em ambiente de simulação, abrangendo uma região geográfica condizente com a realidade.

1.2. Contexto

A padronização do 3G é feita pelo *International Telecommunication Union – Radiocommunications sector (ITU-R)* e *European Telecommunications Standard Institute (ETSI)*. O objetivo principal é a criação de um sistema móvel de terceira geração com o intuito de universalizar os meios de comunicação móvel com altas taxas de transmissão. Progressos significativos já foram obtidos, como, por exemplo, a reserva de 230MHz (de 1885 a 2025MHz e 2110 a 2200MHz) de espectro para uso no padrão UMTS, com a aprovação de 127 países na *World Administrative Radio Conference (WARC)* em 1992 [WARC 92].

Na visão do ETSI, um sistema de comunicações 3G deverá suportar diversas facilidades como, por exemplo, portadoras realocáveis, banda atribuível sob demanda (2Mbps para comunicações em ambientes *indoor*, 384kbps em ambientes urbanos (pedestres) e pelo menos 144kbps para ambientes externos ou rurais), grande variedade de tipos de tráfego compartilhando o mesmo meio, tarifação adequada do ponto de vista de tráfego de dados, assim como taxa de *download* para aplicações multimídia, serviços personalizados, facilidade de implementação de novos serviços utilizando ferramentas de *Intelligent Network (IN)*¹, *Wireless Local Loop (WLL)*² de banda larga, entre outros.

Segundo [TUDE 04], no UMTS existem três características de primordial importância:

¹ IN é a denominação dada para a rede que fornece serviço agregados à rede, como, por exemplo, serviço telefônico 0800.

² WLL é um sistema utilizado para conectar usuários ao sistema público de telefonia, utilizando sistema de acesso via rádio, substituindo assim a parte final do sistema fixo (acesso ao assinante) de par trançado por rádio.

acesso via rádio de banda larga, *roaming* inteligente e alta capacidade de transmissão/recepção de dados. Os delegados do ETSI reunidos em Paris concordaram com a adoção de um padrão de interface aérea para a 3G que incorpora elementos de duas tecnologias³:

- *Wideband Code Division Multiple Access* (WCDMA);
- Híbrido de *Time Division Multiple Access* (TDMA) e *Code Division Multiple Access* (CDMA), que é o *Time Division Code Division Multiple Access* (TD-CDMA).

A integração da tecnologia de computação com a de telecomunicações, deve constituir-se na base para sistemas multimídia com incríveis poderes de processamento. Dentro de algum tempo, qualquer indivíduo poderá ter acesso às comunicações sem fio em qualquer parte do mundo, inclusive com deslocamento entre áreas, enviando e/ou recebendo *e-mail*, *fax*, *Video on-Demand* (VoD), SMS, foto/vídeo torpedos de alta resolução como o MMS e fazendo conferência de chamadas em 3 ou mais participantes através de seus dispositivos portáteis e, também, com assinantes da rede de telefonia fixa.

Com dispositivos de segurança, a rede torna-se mais confiável para o tráfego de informações, tanto de usuário (voz e dados) quanto de rede (sinalização). No contexto de segurança, aplicado também ao UMTS, apresentam-se a confiabilidade, integridade, disponibilidade e legitimidade [MACH 00], dentre outros aspectos, que serão explicados no capítulo 3.

Referente aos aspectos de segurança, o *3rd Generation Partnership Project* (3GPP), através do TS 33.102 [T102 00], padronizou as características de segurança para o UMTS, inclusive com as que foram aproveitadas do GSM.

No 3GPP TS 35.202 [T202 05] e TS 35.205 [T205 05] foram padronizados os algoritmos KASUMI e MILENAGE, respectivamente. No caso do MILENAGE, o padrão especifica o comprimento de 128bits para entrada, saída e tamanho de chaves, características estas, que foram atendidas pelo algoritmo Rijndael (AES) na composição dos blocos de encriptação.

O UMTS fortaleceu o nível de segurança do GSM, agregando algoritmos e mecanismos de autenticação, integridade e encriptação, possibilitando, desta forma, o oferecimento de serviços diferenciados para o tráfego de qualquer tipo de informação.

³ A versão detalhada da solução europeia foi apresentada à *International Telecommunication Union* (ITU) em junho de 1998 e pode ser visualizada através do site do ITU em: <http://www.itu.int/>.

1.3. Estrutura do Trabalho

Abaixo é apresentada a forma de distribuição do trabalho, que está estruturado em oito capítulos:

- Capítulo 1 – Introdução: são apresentados os objetivos do trabalho, bem como se justifica o mesmo, através de uma visão geral do contexto da dissertação com enfoque no panorama tecnológico e a relevância do assunto desenvolvido;
- Capítulo 2 – Evolução até o UMTS: são apresentados os conceitos referentes à evolução dos sistemas, incluindo respectivas arquiteturas e funcionamentos, que formam a base para a tecnologia celular estudada neste trabalho;
- Capítulo 3 – Conceitos e Características de Segurança: são apresentados conceitos e formas relevantes de efetuar segurança nos sistemas presentes no capítulo 2, bem como conceitos de autenticação de usuários, confidencialidade e integridade de dados;
- Capítulo 4 – Modelagem dos Mecanismos de Segurança: são implementados os cenários de simulação e a estrutura de funcionamento do sistema UMTS, utilizando, para isto, mecanismos de segurança para autenticação de usuários, confidencialidade e integridade de voz e dados;
- Capítulo 5 – Procedimentos e Simulação: são abordados os cenários e construções das simulações realizadas neste trabalho;
- Capítulo 6 – Resultados Obtidos: são apresentados os resultados das simulações dos diversos cenários através de gráficos e tabelas que possibilitam a comparação dos algoritmos de segurança;
- Capítulo 7 – Conclusão e Trabalhos Futuros: são apresentadas as considerações finais deste trabalho, indicando as principais contribuições, o cumprimento dos objetivos propostos e sugestões de continuação do trabalho;
- Capítulo 8 – Referências: referências utilizadas como auxílio para a confecção desta obra.

2. Evolução até o UMTS

Para que haja um bom entendimento sobre a estrutura e funcionamento dos mecanismos móveis celulares 3G envolvidos neste trabalho, neste capítulo serão abordados alguns temas como forma de revisão que posteriormente estarão presentes na modelagem dos dispositivos UMTS e nos modelos de testes.

2.1. GSM

O *Global System for Mobile Communication* (GSM) é um padrão de telefonia celular digital de 2ª Geração (2G), desenvolvido na Europa e padronizado pelo ETSI, sendo adotado na maior parte do mundo. Desenvolvido inicialmente para a faixa de 900MHz, teve posteriormente uma versão adaptada para as faixas de 1800 e 1900MHz. Em poucos anos, foram criados na Europa outros padrões, como o *Nordic Mobile Telephone* (NMT) e *Total Access Communications Systems* (TACS), sendo instalados de forma similar em quase todos os países do oeste europeu. Contudo, problemas foram observados nestes sistemas, como incompatibilidade entre eles (e com o GSM) e a impossibilidade de fazer *roaming* inter-sistemas ou internacional.

Este sistema encontra-se atualmente em uso no Brasil, sendo adotado por várias operadoras de telefonia móvel como a TIM, Vivo, Claro, Oi, dentre outras. Com base nesta informação e visando o progresso do GSM para o UMTS, como já acontecera na Europa e em grande parte dos países no mundo, é importante conhecer sua estrutura e funcionamento.

2.1.1. Arquitetura do GSM

O GSM oferece a estrutura básica dos sistemas móveis celulares, ou seja, as mesmas funcionalidades básicas associadas à mobilidade como, por exemplo, *roaming* entre áreas (*clusters*)¹ e *handover*² entre células. A arquitetura de referência de um sistema GSM é apresentada na Figura 1.

Mobile Station (MS) (ou Estação Móvel (EM)), representada por aparelhos celulares na figura a seguir, é o terminal utilizado pelo assinante (usuário do SMP) que engloba um *Subscriber Identity Module* (SIM), que é um cartão inteligente com as configurações e dados do usuário.

¹ *Clusters* são aglomerados de células (a Figura 2 representa uma célula) nos quais pode existir o uso da gama de frequências destinadas ao sistema celular. Destes, as formações mais utilizadas são de 1, 3, 4, 7 ou 12 células postas com adjacência entre si (Figuras 11 e 12).

² *Handover* é a tecnologia utilizada para que um móvel possa se locomover entre células a fim de que a comunicação em andamento não seja perdida. Também pode ser denominado como *handoff*.

Figura 1. Arquitetura do Sistema Móvel GSM.

(Fonte: <http://www.girodon.com/>, consulta em 10/01/2008)

Sem o SIM, a MS não está associada a um usuário, portanto, não podendo fazer nem receber chamadas. Uma vez contratado o serviço móvel celular junto a uma operadora, o usuário passa a dispor de um *SIM card* que ao ser inserido em qualquer aparelho celular com tecnologia GSM faz com que este aparelho passe a assumir a identidade do proprietário do *SIM card*. O módulo armazena, entre outras informações, um número de 15 dígitos denominado *International Mobile Subscriber Identity* (IMSI) que identifica unicamente uma dada estação móvel. Já o terminal (aparelho celular) é caracterizado por um número também com 15 dígitos, atribuído pelo fabricante, denominado *International Mobile Equipment Identity* (IMEI).

O GSM também utiliza uma identidade temporária para prover o serviço de confidencialidade aos assinantes móveis, denominado *Temporary Mobile Subscriber Identity* (TMSI). O TMSI é formado por 4 octetos, sendo que o *SIM card* utiliza os 32bits, que formam a identidade, todos em 1's para indicar uma TMSI inválida.

Base Station Subsystem (BSS), representado na figura por um retângulo, é a parte do sistema encarregada da comunicação entre o *Core Network* (CN), restante da rede mostrada na figura (ou *Network Subsystem* (NSS)), com as MS em uma determinada área. O BSS é formado por uma ou várias *Base Transceiver Station* (BTS), também chamadas de Estações Rádio-Base (ERB), que constituem as respectivas células (como na Figura 2) e um *Base Station Controller* (BSC) que controla as BTS em termos de configuração, usando uma matriz de comutação digital que faz a conexão dos canais de RF (*Radio Frequency*), controle de chamadas e sinalização, entre outras funcionalidades.

O *Mobile Switching Center* (MSC) ou Central de Comutação e Controle (CCC) é a entidade responsável pelas funções de comutação e sinalização para as estações móveis localizadas em uma área geográfica designada como área do MSC. A diferença principal entre

um MSC e uma central de comutação fixa é que a MSC tem que levar em consideração a mobilidade dos assinantes (locais ou visitantes), inclusive o *handover* da comunicação quando os assinantes se movem de uma célula para outra. O dispositivo do CN encarregado de efetuar o roteamento de chamadas para outros MSC é chamado de *Gateway MSC* (GMSC).

Figura 2. Exemplo de uma BTS ou ERB.
(Fonte: www.wirelessbrasil.org, consulta em 9/12/2007)

O MSC para efetuar corretamente o *handoff* entre células e o *roaming* entre áreas e, ainda, a correta sinalização, depende de outros dois dispositivos chamados *Home Location Register* (HLR), que é a base de dados onde estão contidas as informações sobre os assinantes do GSM, e *Visitor Location Register* (VLR) que é a outra base de dados, porém, contendo a informação sobre os assinantes em *roaming*, ou seja, fora da área de registro.

Ainda no sistema temos a presença importante do *Authentication Center* (AuC), que tem a responsabilidade de efetuar a autenticação dos assinantes para o uso do sistema. O centro de autenticação ou AuC está associado a um HLR e armazena uma chave de identidade para cada assinante móvel registrado naquele HLR, possibilitando a autenticação do IMSI do assinante. É também, responsável por gerar a chave para criptografar os dados que serão trafegados durante a comunicação entre MS e BTS.

O *Equipment Identity Register* (EIR) é a base de dados que armazena os IMEI dos terminais móveis de um sistema GSM. O *Operation and Management Center* (OMC) é a entidade funcional através da qual a operadora monitora e controla o sistema, assim como o *Telecommunications Management Network* (TMN) e *Network Management Center* (NMC).

2.1.2. Canalização e Distribuição de Canais

O GSM foi padronizado para operar os canais físicos nas faixas de frequências apresentadas na tabela a seguir, sendo adotados na Europa o GSM900 e DCS1800 (*Digital Cellular System* na faixa de 1800MHz), e nos Estados Unidos o PCS1900 (*Personal Communication System* na faixa de 1900MHz).

Tabela 3 – Padrões de tecnologia celular adotados no mundo.

(Dados em MHz)	P-GSM900	E-GSM900	R-GSM900	DCS1800	PCS1900
MS → BTS	890 – 915	880 – 915	876 – 915	1710 – 1785	1850 – 1910
BTS → MS	935 – 960	925 – 960	921 – 960	1805 – 1880	1930 – 1990
Banda total (enlaces direto e reverso)	50	70	78	150	160
Espaçamento entre canais Tx e Rx	45	45	45	95	80
Número de canais RF	124	174	194	374	299

Fonte: [SVER 05], pg. 60 a 63.

No Brasil, a administração de frequências está sob a responsabilidade da Agência Nacional de Telecomunicações (Anatel). A Anatel regulamentou, conforme canalização apresentada abaixo, a banda de 900MHz para a operação do GSM.

Figura 3. Canais disponíveis para faixa de 900MHz.

(Fonte: <http://www.wirelessbrasil.org/>, consulta em 20/12/2007)

Verifica-se que existem duas extensões de banda (Ext). Algumas bandas já contam com autorização de operação e outras ainda não foram autorizadas para operação pela Anatel, tendo entre outros motivos, sistemas já operando nestas faixas de frequência. As subfaixas de extensão de 907,5 a 910,0MHz no *uplink* (UL) e 952,5 a 955,0MHz no *downlink* (DL) não foram autorizadas a prestadoras do SMP que estavam operando nas subfaixas D e E. Existe, também, o espaçamento duplex (*offset*) que é de 45MHz. As subfaixas são outorgadas às prestadoras do SMP conforme o Plano Geral de Outorgas (PGO) [PGOu 04].

Figura 4. Canais disponíveis para faixa de 1800MHz.

(Fonte: <http://www.wirelessbrasil.org/>, consulta em 20/12/2007)

Para a Europa e Brasil, foi designada a banda discriminada na Figura 4 para operação do GSM, o que possibilitou uma considerável oferta de capacidade devido ao largo espectro disponível na região de 1800MHz. Esta banda recebeu duas denominações: GSM1800 e DCS1800. Essa proposta de banda foi adotada pela maioria dos países com poucas

modificações, com exceção principalmente dos EUA que adotaram a banda de 1900MHz mostrada na Figura 5. A oferta das bandas D e E, pela Anatel, dentro do modelo SMP, viabilizou a instalação das operadoras com tecnologia GSM no país.

Nos EUA, o *Federal Communication Commission* (FCC), órgão fiscalizador e regulador norte-americano para todos os tipos de comunicações eletrônicas, verificou e relatou não poder utilizar a faixa de 1800MHz para o uso do GSM, pois já era ocupada por outros serviços, inclusive militares, aprovando, desta forma, alterações no sistema GSM para 1900MHz, passando a ser denominado como PCS1900 e ficar disponibilizado não somente para operações com sistemas GSM, mas, também, para CDMA e D-AMPS (TDMA).

Figura 5. Canais disponíveis para faixa de 1900MHz.

(Fonte: <http://www.wirelessbrasil.org/>, consulta em 20/12/2007)

Os blocos A, B e C têm cada um 30MHz (15 para UL e 15 para DL), enquanto que os blocos D, E e F têm cada um 10MHz (5 para UL e 5 para DL). O bloco de extensão, visando também contemplar diferentes operadoras, tem duas formas de subdivisão: em dois blocos, C1 e C2, cada um com 15MHz (7,5 para UL e 7,5 para DL), ou três blocos, C3, C4 e C5, cada um com 10MHz (5 para UL e 5 para DL). Em qualquer caso, o espaçamento duplex (*offset*) é de 80MHz, como mostrado anteriormente na Tabela 3.

A ITU, no ano 2000, lançou as especificações técnicas para a 3ª Geração (3G) de telefonia celular, denominada *International Mobile Telecommunications – 2000* (IMT-2000), descrita na seção 2.5, cuja principal proposta é proporcionar interoperabilidade e interfuncionamento total dos sistemas móveis no mundo, evitando assim a fragmentação que caracterizou as gerações anteriores (1G (*American Mobile Phone System* (AMPS)) e 2G (TDMA e CDMA)). A ITU sugeriu, então, uma alocação de banda a nível mundial, como a apresentada na Figura 6a. No Brasil, a alocação de banda adotada pela Anatel foi a mostrada na Figura 6b.

As Bandas do GSM são divididas em canais de RF, onde cada canal consiste em pares de frequências (Transmissão (Tx) e Recepção (Rx)) com 200kHz de banda cada. Existem, portanto, 124 canais de RF no GSM900 e 374 canais de RF no DCS1800.

Figura 6. Canais disponíveis para faixa de 2100MHz.
(Fonte: <http://www.wirelessbrasil.org/>, consulta em 20/12/2007)

Estes canais de RF receberam uma numeração conhecida como *Absolute Radio Frequency Channel Number* (ARFCN). As frequências portadoras dos ARFCN são moduladas em 0,3GMSK (onde 0,3G descreve a banda do Filtro Gaussiano de pré-modulação utilizado para reduzir o espectro do sinal modulado e MSK (*Minimum Shift Keying*) é um tipo especial de modulação FSK (*Frequency Shift Keying*) na qual 1's e 0's são representados por deslocamentos na frequência da portadora de RF) por um sinal digital com taxa de 270,8333kbps (esta taxa de dados foi escolhida por ser exatamente quatro vezes o valor do deslocamento da frequência de RF ($\pm 67,708\text{kHz}$)). Este sinal digital de 270,8333kbps é dividido no domínio do tempo em 8 *time slots* (intervalos), possibilitando o *Time Division Multiple Access* (TDMA) nas MS. O GSM, assim como o TDMA (IS-136), é uma combinação de *Frequency Division Multiple Access* (FDMA) e TDMA.

Tabela 4– Divisão do sinal modulado e *slots* no GSM.

Característica	Período	Composição
Sinal de 270,8333kbps (<i>Frame</i> TDMA)	4,615ms	8 <i>slots</i> de tempo
<i>Slot</i> de tempo	576,9 μ s	$\pm 156,25\text{bits}$
Bit	3,692 μ s	1 bit

Fonte: Site <http://www.teleco.com.br/> – Seção de Telefonia Celular (outubro/2006).

2.1.3. Interfaces do GSM

O GSM utiliza dois tipos básicos de canais lógicos denominados *Traffic Channel* (TCH), o qual tem a função de transmitir a informação do usuário (voz e dados), e *Control Channel* (CCH) que controla os dados de sinalização. Ambos são transmitidos dentro da estrutura do quadro (*frame*) TDMA. Os canais lógicos são mapeados como segue:

Figura 7. Interface entre canais lógicos e físicos no GSM.

no modo *Full-rate* (de 13kbps) e a de dados no *Half-rate* (de 9.6kbps).

A interconexão entre BTS e BSC se dá através da interface padronizada *Abis* utilizando o protocolo de sinalização ISDN LAPD *mobile*. A BSC se comunica ao GMSC através do *Transcoder Rate Adapter Unit* (TRAU), suportando dois *links*, um para canais de tráfego a 64kbps (levando voz ou dados do usuário) e outro para canais de sinalização a 16kbps. A interface *A* utiliza o protocolo *Signalling System* N°. 7 (SS7), que define a configuração das chamadas e dos serviços trafegados.

A camada física é baseada na norma G.703, do *International Telecommunication Union – Telecommunications sector* (ITU-T) [G703 01], que recomenda a especificação das características elétricas e físicas de interfaces hierárquicas de taxas de bits, como as descritas nas recomendações ITU-T G.702 (*Plesiochronous Digital Hierarchy* (PDH)) [G702 88] e G.707 (*Synchronous Digital Hierarchy* (SDH)) [G707 88]. As interfaces são definidas em termos gerais, especificando portas de entrada e saída, pontos de conexão, regras de codificação e características dos condutores dos meios físicos.

No NSS, o GMSC ou MSC são os nós centrais. Neles, existem níveis de tráfego no enlace e controle de sinalização sobre as interfaces, além do fornecimento de ligação com a rede externa (PSTN, ISDN ou *Packet Data Network* (PDN)). O conjunto formado pelo HLR, AuC e EIR fornece a plataforma para a IN e *Value Added Service* (VAS) ou, conforme a Anatel, Serviço de Valor Adicionado (SVA), que tem como serviços, por exemplo, o *Short Message Service Center* (SMSC) e *Voice Mail System* (VMS).

Figura 9. Interfaces e serviços da arquitetura GSM.

Na interface *A*, entre BSC/TRAU e MSC, a camada física é de 2Mbps padrão da *Comité Consultatif International Téléphonique et Télégraphique* (CCITT) agora ITU-T. As interfaces *C*, *D*, *E*, *F*, *G* foram padronizadas pelo protocolo *Mobile Application Part* (MAP) que, por sua vez, utiliza os serviços de transferência de mensagens do SS7. O MAP é especificado nas normas ETS 300 974 da ETSI [ETSI 00] e IS-41 (também definido como ANSI-41) da *American National Standards Institute* (ANSI), juntamente com a *Electronic Industries Alliance/Telecommunication Industry Association* (EIA/TIA) [IS41 88].

O MAP tem a função de definir a camada de aplicação, protocolos de sinalização, procedimentos de registro dos usuários móveis e manipulação de *handoffs* entre sistemas celulares. O SS7 é um padrão adotado pela ITU e utiliza um canal dedicado para a comunicação de sinalização. Além das aplicações relacionadas ao tráfego telefônico, o SS7 estabeleceu na parte do usuário, camadas que possibilitam a troca de informações entre centrais ou bases de dados, não relacionadas ao estabelecimento de circuitos telefônicos, pois visava-se uma implementação de serviços IN. Estas camadas são: *Signalling Connection Control Part* (SCCP), *Intermediate Service Part* (ISP) e *Transaction Capabilities Application Part* (TCAP), *Mobile Application Part* (MAP), *Message Transfer Part* (MTP), *ISDN User Part* (ISUP) e *Telephone User Part* (TUP).

Figura 10. Estrutura de protocolos do SS7.

A necessidade de sinalização em uma rede celular é maior do que na rede fixa, pois existe outra variável que dificulta bastante a sinalização, localização e segurança, dentre outras características, que é a mobilidade do usuário. Para suprir estas necessidades, foi desenvolvida, para o GSM, a camada MAP que usa como suporte as várias camadas do SS7, conforme Figuras 8 e 10. O modelo de camadas *Open System Interconnection* (OSI) serve como base de comparação para sistemas baseados em camadas e será descrito com mais detalhes na seção 2.2.4.

Diferentes protocolos de sinalização são utilizados nas interfaces. Algumas interfaces NSS envolvem apenas protocolos de controle de sinalização (sem envolvimento com o tráfego), como, por exemplo, não ser gerado tráfego sobre as interfaces entre a GMSC, HLR e VLR. Ao invés disso, estas interfaces transportam apenas sinalização usando o MAP.

O GMSC estabelece o tráfego de chamada a 64kbps para a PSTN através da ISUP. O GMSC e MSC trocam tráfego sobre o LAPD, também a 64kbps, e usam o controle do SS7 (MAP e ISUP). A interconexão entre MSC e redes fixas utiliza o padrão SS7 (TUP ou ISUP). As interfaces *B* (entre MSC e VLR) e *H* (entre HLR e AuC) não estão padronizadas por se referirem normalmente a interfaces internas dos conjuntos MSC/VLR e HLR/AuC.

2.1.4. Capacidade do Sistema

A eficiência de utilização do Espectro de Radiofrequência de um sistema GSM é maior que a do AMPS e menor que a do TDMA (IS-136). Em uma Banda de 30kHz o AMPS tem capacidade para uma chamada telefônica e o TDMA para três. Já o GSM em 200kHz tem capacidade para oito chamadas.

Por apresentar menos interferência co-canal (interferência entre canais de mesma frequência), os sistemas GSM utilizam um reuso de frequência de 9 ou 12, enquanto no AMPS e TDMA o normal é de 7. Ainda, com o recurso de setorização, ou seja, divisão dos hexágonos por 3, são gerados padrões 4/12 (ou mais) no GSM e 7/21 no AMPS e TDMA, propiciando melhor utilização do espectro, menos tráfego por célula e melhoria na qualidade do sinal por parte do GSM (ver Figuras 11 e 12). Se o GSM utilizar um recurso de saltos em frequência (ou *Frequency Hopping* (FH)), previsto nas especificações e descrito na próxima seção, é possível utilizar esquemas de reuso de frequências mais eficientes.

2.1.5. Espalhamento Espectral

Para a transmissão em radiofrequência podem ser utilizadas técnicas de *Spread Spectrum* (SS) ou espalhamento espectral, como, por exemplo, *Direct Sequence Spread Spectrum* (DSSS) e *Frequency Hopping Spread Spectrum* (FHSS). Nessas técnicas, a transmissão dos quadros de dados é feita enviando-os por vários canais disponíveis dentro de uma faixa de frequência ao invés de usar um único canal, possibilitando, desta forma, a transmissão simultânea de vários quadros.

A técnica DSSS distribui o sinal sobre uma gama extensiva de faixa de frequência, reorganizando os pacotes no receptor. A FHSS, também conhecido como salto em frequência, por sua vez, envia segmentos curtos de dados que são transmitidos através de frequências específicas (79 canais de 1MHz distribuídos em 20 saltos), possibilitando o controle de fluxo com o receptor, que pode negociar velocidades menores comparadas às velocidades oferecidas pela técnica DSSS, porém, menos susceptíveis a interferências e gerando mais confiabilidade na entrega de quadros. Para um receptor não desejado, o sinal modulado em FHSS aparece como ruído de pulso de curta-duração. O FHSS é mais lento que o DSSS, pois a idéia é garantir alta segurança na transmissão.

Devido ao FHSS fornecer controle de fluxo, canais diferenciados e maior quantidade de segurança na transmissão é o modelo adotado pelo GSM. Mas para os sistemas 3G, que provêem recursos de segurança e exigem maiores velocidades, a melhor escolha é o DSSS.

2.1.6. Fator de Reuso

O fator de reuso é baseado na forma dos *clusters*, que podem ser visualizados nas figuras abaixo através de conjuntos de células hexagonais destacadas em grupos de cores diferentes.

Figura 11. Fator de reuso 12 (razão de reuso 6,00).
Uso no padrão GSM.

Figura 12. Fator de reuso 7 (razão de reuso 4,58).
Uso nos padrões AMPS e TDMA.

A idéia inicial era baseada na forma circular (Figura 2), porém, a melhor representação para a área de cobertura celular é o hexágono, pois devido ao padrão de irradiação, que usa a transmissão de ondas eletromagnéticas, o círculo torna-se irregular. Na geometria celular hexagonal, a unidade de distância entre células é representada por $\sqrt{3}r$. Portanto, a distância a ser utilizada entre células com canais RF idênticos é dada pela expressão:

$$d^2 = i^2 + ij + j^2 \quad (1)$$

A área da célula é dada por:

$$a = \frac{3\sqrt{3}r^2}{2} \quad (2)$$

Supondo-se, então, que a distância entre os centros de duas células adjacentes seja igual a d , tem-se que a área (A) do *cluster* é dada pela seguinte expressão:

$$A = 3\sqrt{3} \left[\frac{\left(\frac{d}{2}\right)}{\cos 30^\circ} \right]^2 \frac{1}{2} = A = \frac{\sqrt{3}d^2}{2} \quad (3)$$

Fazendo-se agora o número de células por cluster (N) igual a A/a , temos que:

$$N = \frac{A}{a} = d^2 \quad (4)$$

ou equivalente, usando a expressão (1):

$$N = i^2 + ij + j^2 \quad (5)$$

Finalmente, substituindo-se (2) e (3) em (4), consegue-se a expressão final da razão

d/r , mais conhecida como razão de reuso de co-canal:

$$N = \frac{\frac{\sqrt{3} d^2}{2}}{\frac{3\sqrt{3} r^2}{2}} = \frac{\sqrt{3} d^2}{2} \cdot \frac{2}{3\sqrt{3} r^2} = \frac{d^2}{3r^2} \quad \boxed{\frac{d}{r} = \sqrt{3N}} \quad (6)$$

Da expressão (6), podemos realizar os cálculos para obter o fator de reuso relacionado à quantidade de células do *cluster*, gerando a tabela abaixo.

Tabela 5 – Fator de reuso.

Padrão de Reuso (N) (Células por Cluster)	Razão de Reuso (d/r)	Quantidade de Canais por Célula	Tráfego por Célula	Qualidade do Sinal
1	1,73	360	Alto	Baixa
3	3,00	120	↑	↓
4	3,46	90		
7	4,58	51		
9	5,19	40		
12	6,00	30	Baixo	Alta

Fonte: [SVER 05], pg. 40.

Da tabela, percebemos que quanto menos células formando um *cluster*, maior é a quantidade de canais e mais alto é o tráfego de voz e sinalização por célula, gerando baixa qualidade no sinal em termos de interferência co-canal, atraso e desempenho ruim do sistema. Portanto, o correto é termos mais células por cluster, aumentando, assim, a razão de reuso, gerando baixo tráfego de voz, dados e sinalização por célula, melhorando assim, a qualidade do sinal percebido pela MS.

2.1.7. Serviços Disponíveis no GSM

As especificações do GSM procuraram de início reproduzir na rede móvel os serviços que estariam disponíveis na rede fixa através da ISDN, padronizada pela *International Telecommunication Union* (ITU) [I120 93]. A estrutura flexível dos canais físicos do GSM, bem como a utilização do padrão SS7, facilitou a introdução destes serviços que foram divididos em grupos, como apresentados a seguir.

- *Bearer Services*: são serviços de transporte de dados utilizados para conectar dois elementos de uma rede com taxas de dados de 2,4 a 9,6kbps como, por exemplo, o acesso ao X.25³;

³ X.25 é um conjunto de protocolos padronizado pela ITU para redes de longa distância, que usam o sistema telefônico ou ISDN como meio de transmissão. Fonte: <http://www.itu.int/>.

- *Location Services*: são serviços padronizados para o GSM, que permitem estimar com precisão a localização de uma estação móvel, servindo de base para vários serviços oferecidos ao assinante, como o *Global Positioning System* (GPS)⁴;
- *Supplementary Services* (SS): são serviços acrescidos para o assinante final, tais como identificação do número chamador, chamada em espera, siga-me, conferência de chamadas (como os utilizados no *Private Branch Exchange* (PBX)) e outros proporcionados pela estrutura IN (Figura 9).

2.1.8. Considerações do GSM

O GSM é o padrão de telefonia celular com maior número de usuários no mundo, tendo atingido em 2005 a marca de 1709,2 milhões de assinantes⁵ e está presente em praticamente todos os continentes. A presença mundial e o volume de assinantes de redes GSM é o grande trunfo deste sistema, pois se traduz em facilidades de *roaming* mundial e custos mais baixos para rede e terminais.

O GSM foi introduzido no Brasil em 2002 com a licitação das Bandas D e E feita pela Anatel [LSMP 02], estando em operação em quase todo o território nacional e sendo adotado pela maioria das operadoras que utilizavam o TDMA.

A adoção do GSM pelas operadoras no Brasil, teve impacto não apenas na interface rádio, o que exige novos terminais GSM, mas, também, na rede nacional de *roaming* que era baseada no IS-41 para os sistemas AMPS, TDMA e CDMA. A sinalização de *roaming* do GSM é feita através do protocolo MAP com suporte do SS7. Este padrão possibilitou a disponibilidade de novos serviços como *Bearer Services*, *Teleservices*, *Location Services* e *Supplementary Services*, além de serviços diferenciados com a presença da plataforma IN (modelo adotado pela ITU-T) [I312 92].

2.2. GPRS

O *General Packet Radio Service* (GPRS) é um serviço para comunicação de dados que permite à estação móvel (MS) conexão com a Internet sem a necessidade de estabelecer uma chamada telefônica. Este serviço pode utilizar até 8 *time slots* de um canal GSM de 200kHz, o que implica em uma taxa que teoricamente poderia chegar a 115kbps ou mais.

⁴ GPS é um sistema de posicionamento por satélite (uso de satélite americano), utilizado para a determinação da posição de um receptor na superfície da Terra ou em órbita. Fonte: <http://pt.wikipedia.org/>.

⁵ Dados extraídos do site <http://www.teleco.com.br/>, baseados em informações da *Wireless Intelligence* (Ovum/GSM Association). Acessível através de <https://www.wirelessintelligence.com/Index.aspx>.

2.2.1. Dispositivos do GPRS

Os dispositivos utilizados na arquitetura do GPRS são os mesmos da arquitetura GSM, com exceção do *Serving GPRS Support Node* (SGSN) e *Gateway GPRS Support Node* (GGSN). É através do SGSN que existe a entrega de pacotes de dados entre a MS e sua área geográfica de serviço (área onde a MS tem registro no HLR) e é no GGSN que ocorre a interface entre o *backbone* GPRS e a PDN, que é uma rede de pacotes como a Internet, ou a outra *Public Land Mobile Network* (PLMN).

2.2.2. PLMN

A *Public Land Mobile Network* (PLMN) é uma rede móvel de mesma estrutura GSM, tendo como objetivo geral, fornecer o serviço móvel de telecomunicações em redes terrestres. A PLMN, da mesma forma como na IN, é estruturada em planos funcionais e usa interfaces abertas de sinalização além dos mesmos protocolos e blocos de implementação básicos do SS7. Ao conjunto de células agrupadas dentro de uma área geográfica da PLMN é dado o nome de *Location Area Identity* (LAI).

Tipicamente uma LAI é composta por 30 células e o VLR é a entidade responsável pelo controle e atualização de dados de cada LAI. Esta atualização é necessária conforme ocorre o deslocamento da MS entre as LAI. Quando o usuário move-se de um VLR para outro, a informação é atualizada pelo HLR, através de interfaces com os MSC (e GMSC).

A PLMN fornece além dos serviços de estabelecimento, supervisão e liberação de chamadas (que utiliza os serviços de supervisão de circuitos), os serviços de *roaming* e *handoff* (ou *handover*), que consistem em determinar, a cada momento, a melhor BTS para a MS, e a realização da migração, caso necessário, independentemente de existirem chamadas em curso ou estabelecidas. Enfim, a PLMN é essencial para o funcionamento de quaisquer sistemas *wireless*, assim como, para redes cabeadas (PSTN), proporcionando ao GSM melhoria na performance da rede, auxiliando no controle das MS quando em ambientes de registro local (HLR) ou visitante (VLR) e, inclusive, em situações de transição entre elas.

2.2.3. Arquitetura do GPRS

A rede GPRS suporta tanto a comutação de circuito como a de pacote. A comutação por circuitos é suportada pelos elementos de rede BTS, BSC e MSC, vistos no capítulo anterior. A comutação por pacotes realiza a transferência de dados por pacotes em uma interface wireless, proporcionada pelo SGSN e GGSN, provendo mobilidade aos usuários e permitindo acesso à PDN.

Figura 13. Arquitetura do sistema móvel GPRS.
(Adaptado de: <http://www.girodon.com/>, consulta em 10/01/2008)

Ainda, para a proteção da Intra-PLMN contra ataques de intrusos, existe o *Border Gateway* (BG), que é uma caixa lógica contendo dois (ou mais) operadores juntos via *backbone* Inter-PLMN. É utilizado na conexão entre diferentes PLMN, interligando a rede GPRS.

2.2.4. Modelo OSI

Primeiramente, para facilitar a compreensão dos dispositivos a serem utilizados neste trabalho, foi utilizado o modelo *Open System Interconnection* (OSI) [X210 93] como referência, pois suas camadas são muito bem definidas e de fácil entendimento. Este modelo é padronizado pela *International Organization for Standardization* (ISO) e para melhor descrever as camadas do modelo OSI, foi gerada a Tabela 6, apresentada adiante. Este padrão é muito utilizado para comparações por estar isento de conexões com quaisquer tecnologias específicas, sendo adotado pela maioria dos fabricantes de equipamentos da área de telecomunicações para a implementação de produtos.

Figura 14. Arquitetura do modelo OSI.
(Fonte: <http://www.seekfordsolutions.com/>, consulta em 17/01/2008)

O modelo é distribuído em camadas sendo que as camadas inferiores fornecem serviço às camadas superiores, transmitindo-se, portanto, a informação através da rede até alcançar o destino (por exemplo, de um *host A* para um *host B* e vice-versa), como na Figura 16. Um destes serviços é o encapsulamento das *Packet Data Unit* (PDU), ou seja, informação fornecida pelas camadas superiores para serem transportadas pelas camadas inferiores, às quais acrescentam em suas respectivas PDU (ou *Protocol Data Unit*) os seus cabeçalhos.

Tabela 6– Camadas do modelo OSI.

Camada	Descrição
Aplicação	Esta camada faz a interface entre o protocolo de comunicação e o aplicativo que solicitou ou que irá receber a informação através da rede. Por exemplo, ao solicitar a recepção de e-mails através do aplicativo de e-mail, este entrará em contato com a camada de Aplicação do protocolo de rede, efetuando tal solicitação. Tudo nesta camada é direcionado aos aplicativos. Unidade: dados.
Apresentação	Esta camada converte o formato do dado recebido pela camada de Aplicação em um formato comum a ser utilizado na transmissão. Faz também a compressão de dados e criptografia. Um padrão que pode ser utilizado nesta camada é o <i>Abstract Syntax Notation One</i> (ASN.1) descrito através da norma [X680 02]. Unidade: dados.
Sessão	Esta camada disponibiliza serviços como, por exemplo, pontos de controle periódicos a partir dos quais a comunicação pode ser restabelecida em caso de pane na rede. Unidade: dados.
Transporte	Esta camada é responsável por pegar os dados enviados pela camada de Sessão e dividi-los em segmentos que serão transmitidos para a camada de Rede. No receptor, a camada de Transporte é responsável por pegar os pacotes recebidos da camada de Rede, remontar o dado original e assim enviá-lo à camada de Sessão. Ele pode operar de duas formas, orientado a conexão (é o modo no qual existe um sincronismo inicial (<i>three-way-handshake</i>) e estabelecimento de uma conexão fim-a-fim com confirmação de recebimento de pacotes) e não orientado a conexão (é o modo em que a transmissão é feita assincronamente e sem confirmação de recebimento de pacotes). Algumas funções desta camada são: controle de fluxo e congestionamento, ordenação dos pacotes e a correção de erros. Unidade: segmentos.
Rede	Esta camada é responsável pelo endereçamento dos pacotes, convertendo endereços lógicos em endereços físicos (por exemplo, o IP ou IPX), de forma que os pacotes consigam chegar corretamente ao destino. Essa camada também determina a rota que os pacotes irão seguir para atingir o destino, baseada em fatores como condições de tráfego da rede e prioridades. Os pacotes podem chegar ao destino através de múltiplos caminhos. Algumas funções desta camada são: encaminhamento, endereçamento, interconexão de redes, tratamento de erros, fragmentação de pacotes e controle de congestionamento de pacotes. Unidade: pacotes.
Enlace	Esta camada detecta e, opcionalmente, corrige erros que possam acontecer no nível físico. É responsável pela transmissão, recepção e delimitação de quadros, além de fazer o controle de fluxo. Ela também estabelece um protocolo de comunicação entre sistemas diretamente conectados. Esta camada subdividiu-se em <i>Logical Link Control</i> (LLC) e <i>Medium Access Control</i> (MAC). Unidade: quadros.
Física	Esta camada define as características técnicas dos dispositivos elétricos do sistema, nos quais existe a transmissão de bits. No caso de transmissão de voz, utiliza-se como meio de condução a interface aérea ou física, transmitindo-se ondas eletromagnéticas. Os dados podem ser transmitidos através de feixes de luz sobre meios físicos como a fibra-óptica. Unidade: bits.

Adaptado de: (<http://pt.wikipedia.org/>, consulta em 13/01/2008).

2.2.5. Modelo TCP/IP

Como o GPRS dá acesso à rede de dados ou PDN, é necessário entender o funcionamento do *Internet Protocol* (IP), pois será utilizado, principalmente em serviços mais atuais como o *IP Multimedia Subsystem* (IMS) no contexto de serviços e IPSec na parte de segurança, descritos nas seções 2.7.7 e 2.7.5, respectivamente.

Baseando-se na forma como são dispostas as funções na rede de pacotes, foi gerado o modelo *Transmission Control Protocol/Internet Protocol* (TCP/IP) que pode ser visto através da Figura 15, adotando-se uma estrutura de 5 camadas para melhor visualização dos processos envolvidos, porém, também existe uma abstração do modelo com 4 camadas não abordado neste trabalho. As descrições detalhadas das camadas encontram-se na Tabela 7.

Tabela 7 – Camadas do modelo TCP/IP.

Camada	Descrição
Aplicação	Os processos que rodam nesta camada são específicos da aplicação. O dado (informação) é passado do programa de rede, no formato usado internamente por essa aplicação, e é codificado dentro do padrão de um protocolo da camada de Transporte. Alguns protocolos que pertencem a esta camada são: HTTP, SMTP, FTP, RTP, Telnet, SIP, SNMP, POP3, IMAP e DNS. Unidade: dados.
Transporte	Tem as mesmas funções e tarefas que foram descritas no modelo OSI. Alguns protocolos que pertencem a esta camada são: <i>Transmission Control Protocol</i> (TCP) (orientado a conexão) e <i>User Datagram Protocol</i> (UDP) (não orientado a conexão). Unidade: segmentos.
Internet	Equivalentemente à camada de Rede do modelo OSI, esta camada é responsável pelo endereçamento dos pacotes, encaminhamento e determinação de rotas, fragmentação e controle de congestionamento de pacotes, e ainda, pelo fornecimento do serviço de melhor esforço na entrega de pacotes a um destino. Alguns protocolos que pertencem a esta camada são: IP (IPv4 e IPv6), ARP, RARP, ICMP e IPsec. Unidade: pacotes.
Acesso a Rede	Nesta camada pode ser estabelecido um <i>Virtual Private Network</i> (VPN) ou túnel, onde pacotes da camada de Internet, ao invés de serem enviados através de uma interface física, são enviados usando um protocolo de tunelamento da suíte de protocolos. Alguns protocolos que pertencem a esta camada são: Ethernet (802.3), Wi-Fi (802.11), IEEE 802.1Q, 802.11g, HDLC, Token Ring, FDDI, PPP e Frame Relay. Unidade: quadros.
Física	Assim como no modelo OSI, esta camada faz a interface física entre os equipamentos, utilizando quaisquer meios de condução para a transmissão dos bits. Alguns protocolos que pertencem a esta camada são: Modem, RS-232, EIA-422, RS-449, RDSI, <i>Bluetooth</i> e USB. Unidade: bits.

Adaptado de: (<http://pt.wikipedia.org/>, consulta em 13/01/2008).

Para o transporte dos dados através da rede utiliza-se o padrão IP. O endereço IP, na versão 4 (IPv4), é um número de 32 bits escrito com quatro octetos no formato decimal (por

exemplo: 129.66.45.57). Devemos notar que um endereço IP não identifica uma máquina individual, mas sim uma conexão à rede. Deste modo, um *gateway* conectado a n redes tem n endereços IP diferentes, sendo um para cada conexão.

Figura 15. Comparação entre as arquiteturas OSI e TCP/IP.

(Fonte: <http://www.pucsp.br/>, consulta em 05/01/2008)

Os endereços IP podem ser usados tanto para se referir às redes quanto a um *host* específico. Por convenção, um endereço de rede tem o campo identificador de *host* com todos os bits iguais a 0 (zero). Podemos nos referir a todos os *hosts* de uma rede através de um endereço por difusão, ou seja, o campo identificador de *host* deve ter todos os bits iguais a 1. Um endereço com todos os 32bits iguais a 1 é considerado um endereço de *broadcast* para a rede do *host* que originou o pacote (ou datagrama). O endereço 127.0.0.1 é reservado para teste de comunicação entre processos da mesma máquina (*loopback*).

O IP utiliza cinco classes diferentes de endereços (conforme Tabela 8). A definição de classes de endereços deve-se ao fato do tamanho das redes que compõem o sistema, sendo estas, desde redes locais de computadores de pequeno porte (redes privadas) até redes públicas interligando milhares de *hosts*, incluindo equipamentos como roteadores, *switch routers*, *Access Points* (AP), servidores e outros.

Tabela 8 – Classes de endereços IP.

Classe	Gama de Endereços			Nº. de Endereços por Rede ou Finalidade	Tipo de Endereço
A	1.0.0.0	–	9.255.255.255	16.777.216	Público
A	10.0.0.0	–	10.255.255.255	-	Privado
A	11.0.0.0	–	126.255.255.255	16.777.216	Público
A	127.0.0.0	–	127.255.255.255	<i>Loopback</i>	-
B	128.0.0.0	–	172.15.255.255	65.536	Público
B	172.16.0.0	–	172.31.255.255	-	Privado
B	172.32.0.0	–	191.255.255.255	65.536	Público
C	192.0.0.0	–	192.167.255.255	256	Público
C	192.168.0.0	–	192.168.255.255	-	Privado
C	192.169.0.0	–	223.255.255.255	256	Público
D	224.0.0.0	–	239.255.255.255	<i>Multicast</i>	-
E	240.0.0.0	–	247.255.255.255	Uso futuro	-

Os endereços de rede privada podem ser utilizados em muitas redes *Local Area Network* (LAN), inclusive repetidamente, pois para obter acesso à *Wide Area Network* (WAN) ou *Metropolitan Area Network* (MAN) existe um *Network Address Translator* (NAT) que faz a tradução de endereços IP privados em endereços IP públicos. Na WAN o endereço IP é único, não podendo existir duplicidade, isto para que haja o correto direcionamento dos pacotes IP.

Das classes apontadas na Tabela 8, as que são utilizadas mais comumente pelos usuários e empresas são as classes A, B e C. A parte de 127.0.0.0 a 127.255.255.255 não é usada para compor endereços de usuários, tendo como finalidade a execução de testes.

O endereço de uma rede IP deve ser composto pelo seu endereço (cujo último octeto tem o valor zero no modo padrão) e respectiva máscara de rede (*netmask*). Exceção para redes “subnetadas”, ou seja, cuja gama de endereços de rede foi subdividida, formando subredes. As máscaras *default* de rede das classes A, B e C, têm a seguinte formatação:

Figura 16. Classes de endereços IP e máscaras (*mask*) padrão de subrede.
(Fonte: <http://www.answers.com/>, consulta em 18/01/2008)

Os endereços da Internet são mais conhecidos pelos nomes associados aos endereços IP (como, por exemplo, www.3gpp.org, onde WWW significa *World Wide Web* e .org o domínio). A Internet é padronizada pelo *Internet Engineering Task Force* (IETF) que é uma comunidade internacional formada por técnicos, agências, fabricantes, fornecedores e pesquisadores com a missão de identificar e propor soluções a questões ou problemas relacionados à utilização da Internet, além de sugerir padronização das tecnologias e protocolos envolvidos na arquitetura.

Para que seja possível a navegação pela *Web*, é necessário traduzir os nomes em endereços IP. O *Domain Name System* (DNS) é o mecanismo que converte nomes em endereços IP e vice-versa, como pode ser visto na Figura 17. Assim como acontece no

endereçamento *Classless Inter-Domain Routing* (CIDR), os nomes DNS são hierárquicos e permitem que faixas de espaços de nomes sejam delegados a outros DNS.

O CIDR é uma forma de flexibilizar o uso de endereços IP, dividindo margens de endereços IP em redes separadas, conforme mostra a Tabela 9, promovendo, deste modo, o uso mais eficiente dos endereços IP.

Tabela 9– Blocos de endereços reservados CIDR.

Blocos de Endereços	Descrição	Referência
0.0.0.0/8	Rede corrente (só funciona como endereço de origem)	RFC 1700
10.0.0.0/8	Rede Privada	RFC 1918
14.0.0.0/8	Rede Pública	RFC 1700
39.0.0.0/8	Reservado	RFC 1797
127.0.0.0/8	<i>Localhost</i>	RFC 3330
128.0.0.0/16	Reservado (IANA)	RFC 3330
169.254.0.0/16	<i>Zeroconf</i>	RFC 3927
172.16.0.0/12	Rede Privada	RFC 1918
191.255.0.0/16	Reservado (IANA)	RFC 3330
192.0.0.0/24	-	-
192.0.2.0/24	Documentação	RFC 3330
192.88.99.0/24	IPv6 para IPv4	RFC 3068
192.168.0.0/16	Rede Privada	RFC 1918
198.18.0.0/15	Teste de <i>benchmark</i> de redes	RFC 2544
223.255.255.0/24	Reservado	RFC 3330
224.0.0.0/4	<i>Multicast</i> (antiga rede Classe D)	RFC 3171
240.0.0.0/4	Reservado (antiga rede Classe E)	RFC 1700
255.255.255.255	<i>Broadcast</i>	-

Fonte: (<http://pt.wikipedia.org/>, consulta em 18/01/2008).

A tabela acima ajuda na divisão dos endereços IP em blocos CIDR. O CIDR está definido no RFC 1519.

Figura 17. Demonstração da árvore de nomes do DNS.

(Fonte: <http://www.juliobattisti.com.br/>, consulta em 18/01/2008)

Recentemente, outra versão do IP, a versão 6 (IPv6), que utiliza um endereço composto por 128bits, possibilitou um aumento extraordinário na possibilidade de distribuição de endereços de rede e *host*.

O endereço do IPv6 está no formato hexadecimal e é composto por 8 grupos de 4 algarismos hexadecimais separados por dois pontos (:), como abaixo:

300F:FAB2:FFA1:12AE:3245:03B1:7781:8ABC

No caso de haver endereços IPv6 com grupos formados por zeros, como no endereço abaixo, adotaram-se as três regras a seguir.

300F:0000:FFA1:0000:0000:03B1:7781:8ABC

- Zeros podem ser omitidos se estiverem no início do grupo. Deste modo, 03B1 pode ser escrito como 3B1;
- Um ou mais grupos com 4 bytes em 0 podem ser omitidos, sendo substituídos por um par de dois pontos. Desta forma, o endereço do exemplo acima poderia ser escrito da seguinte forma:

300F::FFA1::3B1:7781:8ABC

- Endereços IPv4 podem ser escritos e transitados pela rede IPv6, colocando-se um par de dois pontos (::) seguido da notação do endereço IP na versão 4, como abaixo:

::133.25.12.52

O IPv6 tem um cabeçalho base seguido de zeros ou cabeçalhos de extensão. O IPv4 tem o cabeçalho formado por 20bytes (20 octetos) ou 5 *longwords* e o IPv6, o cabeçalho composto por 40bytes ou 10 *longwords*, conforme Figura 18.

Figura 18. Cabeçalhos do IPv4 e IPv6.
(Adaptado de: <http://www.cisco.com/>, consulta em 17/01/2008)

O IPv6 prevê o aparecimento de novos serviços sobre a plataforma IP, como, por exemplo, *Voice over IP* (VoIP), *streaming* de vídeo em tempo real, etc. Este protocolo suporta

intrinsecamente classes de serviço diferenciadas em função das exigências e prioridades dos serviços. Para que o IPv6 tenha um bom convívio com o IPv4, utiliza-se o *tunneling* ou tunelamento do IPv6 dentro de pacotes IPv4, usando-se para a transição, o encapsulamento, como na figura a seguir.

Figura 19. Encapsulamento de pacotes IPv6 em IPv4 (*tunneling*).
(Fonte: <http://w3.ualg.pt/>, consulta em 05/01/2008)

Para maximizar os números IP destinados aos usuários em geral, agregou-se a técnica *Variable Length Subnet Mask* (VLSM), aproveitando-se, deste modo, a gama de endereços IP, através da sumarização de rotas para o tráfego de pacotes pela rede.

Para melhor visualizar as diferenças entre o IPv4 e IPv6, consultar a tabela a seguir:

Tabela 10 – Comparação entre IPv4 e IPv6.

Características	IPv4	IPv6
Espaço de Endereço	32bits	128bits
Suporte para IP móvel	Precário	Bom
Segurança	Nenhuma	Cabeçalhos para inserção
Auto Configuração	Não existe	Padrão

Fonte: (<http://www.wirelessbrasil.org/>, consulta em 14/01/2008).

O uso do IP em redes celulares já é uma realidade. Com a inclusão deste protocolo, obtêm-se novas funcionalidades e serviços, como por exemplo, VoIP, IMS, WAP, etc. Os serviços de Internet são prestados ao assinante final através de provedores de serviço, ou *Internet Service Providers* (ISP), que no Brasil devem ter licença e autorização da Anatel para exploração do Serviço de Comunicação Multimídia (SCM) [R272 01] [R328 03].

2.2.6. Interfaces do GPRS

Para a parte relacionada a dados, ou seja, nas interfaces do GPRS, são utilizados endereçamentos com respectivas classes e subclasses IP, o que possibilita a correta transição e entrega de pacotes de dados fim-a-fim, inclusive com conexão a outras redes de pacotes.

O GPRS oferece interfaces complementares ao GSM, pois utiliza serviços voltados à rede comutada a pacotes. A interface que interliga a BSS ao CN GPRS é a interface *Gb*, como ilustrado na Figura 20.

A interface *Gb* faz a ligação entre a *Packet Control Unit* (PCU), localizada na BSS e conectada à BSC, e o SGSN no *Core GPRS*. A PCU provê à BSS as interfaces físicas e lógicas para o tráfego de dados por pacotes no sistema (BTS, BSC e TRAU).

É através do *Core GPRS*, formado pelo SGSN e GGSN, que a rede celular GSM tem interação com a Internet, outra *network* (NW) ou outras PDN. Todo este processo é feito com a comutação de pacotes IP que, por sua vez, carregam dados oriundos de aplicativos celulares que rodam nas MS ou dados de sinalização e controle.

Figura 20. Interfaces e serviços da arquitetura GPRS.

2.2.7. Considerações do GPRS

O GPRS oferece ao GSM a possibilidade de aumentar a taxa dos canais e, ainda, a implementação de interfaces com a Internet e PDN, ou mesmo, com outras PLMN. Acrescenta, também, mais segurança ao sistema. Este padrão 2,5G teve um substituto para a transmissão de dados com velocidades mais altas, sendo este o EDGE.

2.3. EDGE

O *Enhanced Data for GSM Evolution* (EDGE) é um padrão desenvolvido com a finalidade de aumentar a taxa de dados para serviços oferecidos pela rede GSM. Este aumento é obtido através do uso de outro tipo de modulação para a portadora dos canais de RF, em substituição a usada anteriormente no GSM (0,3GMSK), que é o 8-PSK (*Octagonal Phase*

Shift Keying). Esta solução mantém a estrutura básica de canalização do GSM implicando na instalação de transceptores com modulação 8-PSK para canais de RF.

O EDGE agrega ainda, novas facilidades no protocolo de acesso à interface aérea *Um* e novos esquemas de codificação de canal.

2.3.1. Arquitetura e Interfaces do EDGE

Como pode-se observar através da Figura 21, os mecanismos e interfaces do GSM e GPRS foram mantidos, possibilitando uma taxa de transmissão maior alterando-se apenas a forma de modulação do sinal GSM, protocolo de acesso à interface aérea e esquemas de codificação de canal.

Para tal, foram modificadas as estruturas de *hardware* (HW) e *software* (SW) na GSM/EDGE *Radio Access Network* (GERAN), que é o nome dado pelo *3rd Generation Partnership Project* (3GPP) para o acesso rádio GSM/EDGE, ou à área correspondente aos elementos que compõem a conexão com a interface aérea.

Os pacotes EDGE aumentam para 69.2kbps a taxa de dados que trafega em cada um dos 8 *time slots*, somando um total teórico de largura de banda (BW) de 473.6kbps.

Figura 21. Interfaces e serviços da arquitetura EDGE (release 4).

2.3.2. Considerações do EDGE

O EDGE melhora o desempenho do GPRS, aumentando as capacidades, tanto para a parte comutada a pacotes *Enhanced General Packet Radio Service* (E-GPRS) quanto para a comutada a circuito *Enhanced Circuit Switched Data* (E-SCD), sendo uma atualização de HW e SW para o GPRS. Por sua vez, o EDGE acabará sendo substituído pelo *Wideband Code Division Multiple Access* (WCDMA), que é a interface aérea preferencial adotada pelo UMTS.

2.4. 3ª Geração

As primeiras gerações de sistemas celulares foram desenvolvidas visando-se principalmente o tráfego de voz. A exemplo do que ocorre com a rede de telefonia fixa, usada cada vez mais para tráfego de dados, na década de 90 surgiu uma série de esforços para ampliar o tráfego de dados nas redes celulares.

A evolução do GSM para serviços de terceira geração com taxas de dados de 2Mbps vem sendo padronizada pelo *3rd Generation Partnership Project* (3GPP). Esta evolução exigiu a definição de um novo padrão para a interface entre MS e BTS com canais RF de 5MHz (no UMTS). Ao mesmo tempo, outro padrão surgiu para substituir o CDMAone (2G), o CDMA2000, que é padronizado pelo *3rd Generation Partnership Project 2* (3GPP2), com canais RF de 1,25MHz.

O novo padrão de interface aérea, denominado *Wideband Code Division Multiple Access* (WCDMA), implica em mudanças na estrutura de canalização do GSM, exigindo uma banda adicional de frequências para implementação do serviço, oferecendo transmissão de imagens e tarefas multimídia, mantendo, no entanto, a compatibilidade com as arquiteturas existentes GSM, GPRS e EDGE. A tabela a seguir apresenta os principais padrões até o UMTS.

Tabela 11 – Padrões GSM e UMTS adotados no Brasil e no mundo.

(Dados em MHz)	P-GSM900	E-GSM900	R-GSM900	DCS1800	PCS1900	UMTS2100 (ITU)	UMTS2100 (Anatel)
MS → BTS	890 – 915	880 – 915	876 – 915	1710 – 1785	1850 – 1910	1885 – 2025	1920 – 1980
BTS → MS	935 – 960	925 – 960	921 – 960	1805 – 1880	1930 – 1990	2110 – 2200	2110 – 2170
Banda total (enlaces direto e reverso)	50	70	78	150	120	230	120
Espaçamento entre canais Tx e Rx	45	45	45	95	80	190	190
Tamanho do canal RF	0,2	0,2	0,2	0,2	0,2	5	5
Número de canais RF	124	174	194	374	299	23	12

Adaptado de: (<http://www.teleco.com.br/>, consulta em 15/01/2008).

Os EUA vieram com mais uma proposta, além do CDMA2000, através da TIA TR45.3, que é baseado no *Wideband Time Division Multiple Access* (WTDMA), descrito nas recomendações do *Universal Wireless Communications Consortium* (UWCC) que, por sua vez, havia desenvolvido o padrão TDMA (IS-136). Outros padrões foram desenvolvidos em várias partes do mundo, como a idéia da *Association of Radio Industries and Business* (ARIB), do Japão, que apresentava propostas baseadas nos esquemas WCDMA, TDMA e

Orthogonal Frequency Division Multiplexing (OFDM). Porém, no final, adotou-se a plataforma WCDMA e esta foi enviada como proposta à ITU.

Figura 22. Evolução dos padrões de tecnologias celulares.

(Fonte: <http://dictionary.zdnet.com/definition/>, consulta em 10/01/2008)

Outra entidade é a coreana *Telecommunications Technology Association* (TTA), que propôs duas padronizações, porém, uma delas era similar ao CDMA2000 e a outra ao UMTS. Além destes, o próprio ETSI havia enviado duas propostas, sendo uma delas o UMTS com o WCDMA FDD (como o ARIB) e a outra no TD-CDMA, formando o WCDMA TDD. Ambas serão explicadas com mais detalhes adiante.

2.5. IMT-2000

Os esforços levaram ao projeto *International Mobile Telecommunications – 2000* (IMT-2000), que definiu os requisitos de um sistema celular 3G como sendo:

- Altas taxas de dados: 144kbps em todos os ambientes, 384kbps em ambientes urbanos (pedestres) e 2Mbps em ambientes *indoor* e de baixa mobilidade;
- Transmissão de dados nas formas simétrica e assimétrica;
- Serviços baseados em comutação de circuitos (*Circuit Switched* (CS)) e pacotes (*Packet Switched* (PS));
- Qualidade de voz comparável ou superior à fornecida pela telefonia fixa;
- Melhor eficiência no uso do espectro;
- Vários serviços simultâneos para usuários finais, inclusive serviços multimídia;
- Incorporação suave dos sistemas celulares 2G;
- *Roaming* global;
- Arquitetura aberta para a rápida introdução de novos serviços e tecnologias.

O IMT-2000 é recomendado através da ITU-R M.1457 [IMTe 00], que adotou vários

padrões de interfaces aéreas para os sistemas 3G, sendo os principais: CDMA2000, WCDMA e EDGE. A migração de uma operadora 2G para sistemas 3G envolve grandes investimentos. A escolha do sistema e a estratégia de migração dependem da análise sobre a situação atual da operadora, devendo-se considerar aspectos como a estrutura de rede atual (se é GSM, GPRS ou EDGE), espectro disponível (conforme leis de outorga e obtenção de licença do país ou região) e serviços a serem oferecidos.

Em conformidade com o uso do espectro de RF no Brasil, a operadora deve obter a autorização ou concessão para atuar no respectivo serviço (no caso SMP) e possuir a licença para que possa colocar em operação os dispositivos da rede e disponibilizar os serviços contratados aos assinantes (usuários). De modo a minimizar os custos nesta transição, buscou-se desenvolver padrões de 3G que facilitassem a evolução dos padrões 2G existentes. Isto deu origem a duas grandes linhas de evolução: CDMA2000 e UMTS, como apresentados a seguir.

2.6. CDMA2000

O *Code Division Multiple Access* 2000 (CDMA2000) é um padrão 3G, idealizado e construído para aperfeiçoar os sistemas celulares baseados no IS-95 (CDMAone). O *3rd Generation Partnership Project* 2 (3GPP2), criado pelo ETSI, é a organização responsável pelas especificações deste padrão. O CDMA2000 conserva o comprimento da largura de banda, ou *bandwidth* (BW) da portadora do CDMAone, que é de 1,25MHz. Baseando-se nesta BW e na interoperabilidade entre os padrões 2G e 3G, o CDMA2000 utilizou ferramentas de transição como o IS-95B, mostrado na Figura 22.

2.6.1. CDMA2000 1xRTT

O CDMA2000 manteve a banda por portadora em 1,25 MHz de modo a manter a compatibilidade com os sistemas CDMA (IS-95) ainda existentes. É padronizado pela TIA, na TR45.5. Este padrão trabalha sobre a tecnologia DSSS e somente no modo *Frequency Division Duplex* (FDD), descrito na seção 2.7.3.

Este sistema pode operar com uma ou mais portadoras (conceito de multi-portadoras) e sua estrutura permite a compatibilidade com o sistema 2G (CDMAone).

Neste padrão, é utilizado o *Direct Sequence Code Division Multiple Access* (DS-CDMA) que é o uso do método de acesso CDMA, juntamente com a tecnologia de espalhamento espectral *Direct Sequence Spread Spectrum* (DSSS), no qual vários usuários, utilizando códigos diferentes, compartilham a mesma banda de frequências. O CDMA2000 tem um modo de operação, o *Single-carrier Radio Transmission Technology* (1xRTT), que

especifica um único canal de 1,25MHz para a transferência de dados (sua primeira versão).

Figura 23. Arquitetura do CDMA2000 1xRTT.
(Fonte: <http://ru.infocom.uz/>, consulta em 20/01/2008)

2.6.2. CDMA2000 1xEV-DO

A evolução para o CDMA2000 foi o *Single-carrier Evolution-Data Optimized* (1xEV-DO) que é um padrão de banda larga no qual pode-se alcançar velocidades mais altas do que as atingidas pelo GPRS ou EDGE. Este padrão foi desenvolvido pela Qualcomm em 1999, para suprir as exigências do IMT-2000, atingindo velocidades de 400 a 700kbps em média e acima de 2Mbps em ambientes *indoor*.

Figura 24. Arquitetura do CDMA2000 1xEV-DO.
(Fonte: <http://www.zte.com.cn/>, consulta em 20/01/2008)

Este modelo pode capacitar zonas de computação pervasiva, ou seja, zonas em que múltiplos dispositivos portáteis estão conectados à Internet com uma velocidade alta e constante. Possibilitando ao usuário acesso e uso de serviços, como *Internet Protocol Television* (IPTV) e VoIP. Em contradição ao *High Speed Downlink Packet Access* (HSDPA), que habilita a transmissão de voz e dados simultaneamente, o 1xEV-DO disponibiliza somente a transmissão de dados. Pode ser utilizado, também, no esquema *Multicarrier Code*

Division Multiple Access (MC-CDMA).

Este padrão também implementa outra forma de modulação, a 16QAM (*Quadrature Amplitude Modulation*) e a tecnologia para enlace reverso *Hybrid Automatic Repeat reQuest* (HARQ), melhorando o *throughput* (taxa de dados instantânea) do sistema.

2.6.3. CDMA2000 1xEV-DV e UMB

Por último, o CDMA2000 teve a evolução para o *Single-carrier Evolution-Data and Voice* (1xEV-DV), suprimindo a falta de simultaneidade na transmissão de voz e dados. Utiliza a tecnologia de alta velocidade *High Data Rate* (HDR) do 1xEV-DO com o padrão 1xRTT. Integra mecanismos similares ao 1xRTT, provendo também compatibilidade com padrões anteriores.

Ultra Mobile Broadband (UMB) é a tecnologia 3G, apresentada em 2007, que introduz o *Orthogonal Frequency Division Multiple Access* (OFDMA), *Multiple-Input and Multiple-Output* (MIMO), *Spatial-Division Multiple Access* (SDMA) e técnicas de cancelamento de interferência para aumentar a taxa de transmissão do DL em 280Mbps e, então, melhorar o *throughput* do sistema.

2.6.4. Considerações do CDMA2000

Figura 25. Evolução do CDMA2000 1xEV-DO para o UMB.

(Fonte: <http://www.zte.com.cn/>, consulta em 20/01/2008)

Baseando-se nas tecnologias de acesso apresentadas no CDMA2000, nota-se uma evolução passo a passo abrangendo aspectos como aumento na taxa de transmissão de dados, por duas vezes e após, a evolução para uma transmissão de alta velocidade para voz e dados simultaneamente. Os planos de evolução para o 1xEV-DO prevêem a inserção do UMB, com novos modelos de acesso múltiplo, na esperança de alcançar taxas de dados altíssimas (280Mbps), melhorando ainda mais o desempenho do sistema padronizado pelo 3GPP2, assim como mostra a figura acima.

arquitetura desenvolvida para o UMTS baseou-se nos mecanismos já existentes da plataforma GSM/GPRS, agregando mecanismos e interfaces de alta velocidade, além da interoperabilidade e facilidade de evolução modular, como demonstra a Figura 28.

Fundamentadamente na arquitetura apresentada, foram descritas as interfaces envolvidas na estrutura do UMTS (ver Tabela 12) e os mecanismos de conexão ou dispositivos que compõem o sistema (ver Tabela 13). As interfaces *Iu*, *Iub* e *Iur*, trabalham baseadas nos princípios do *Asynchronous Transfer Mode* (ATM)⁶.

Tabela 12 – Interfaces da arquitetura do UMTS.

Componentes	Descrição
<i>Uu</i>	A interface aérea é dividida em três camadas, sendo estas, a camada Física (L1), de Enlace de Dados (L2) e de Rede (L3). É neste <i>link</i> que ocorre a interação entre o UE e o <i>Node-B</i> , transportando tráfego de voz e dados. É nesta interface que trabalha o WCDMA.
<i>Iu</i> (<i>Iu CS</i> e <i>Iu PS</i>)	É a interface localizada entre a UTRAN e CN (NSS), sendo especificada para suportar interconexão do <i>Radio Network Subsystem</i> (RNS), formado pelo RNC e <i>Node-B</i> com pontos de acesso a uma única PLMN. Oferece apoio a todos os serviços UMTS (PS e CS), interfuncionamento entre UMTS e GSM (<i>release 5</i>) e, por fim, permite a evolução tecnológica entre as CN, RNS e redes de transporte.
<i>Iub</i>	É a interface que conecta o <i>Node-B</i> ao RNC. É neste enlace que trafegam todas as informações trocadas entre o UE e o NSS.
<i>Iur</i>	Interface que permite a troca de informação de sinalização entre duas RNC dentro de uma mesma UTRAN. Suporta a interconexão de RNC de diferentes fabricantes, oferece apoio aos serviços oferecidos pela RNS e UTRAN (via <i>Iu</i>) e separa as funcionalidades entre as redes de RF e transporte, facilitando a implementação de novas tecnologias.
<i>Gc</i>	Interface que interliga o GGSN ao HLR, sendo opcional e utilizada pelo GGSN para requisitar informações de localização ao HLR. A interface principal é a <i>Gr</i> .
<i>Gd</i>	Interface que conecta o SGSN ao GMSC, provendo acesso ao SMS (SMS-GMSC). Ou seja, provê o acesso ao serviço de mensagens curtas através do <i>Inter Working Mobile Switching Center</i> (IWMSC) denominado SMS-IWMSC.
<i>Gi</i>	Interface entre a GGSN e redes de pacotes de dados (PDN), como, por exemplo, Internet, acesso a e-mails (via <i>browser</i> de Internet ou aplicativo específico), DNS e DHCP.
<i>Gn</i>	Interface entre SGSN e GGSN localizadas em um mesmo PLMN (ou entre dois SGSN), que tem a finalidade de transmitir tráfego de dados (pacotes).
<i>Gp</i>	O mesmo que o descrito para a interface <i>Gn</i> , porém, para interligações entre SGSN e GGSN de diferentes PLMN. Provê também a função de segurança (requisito para a comunicação entre diferentes PLMN).
<i>Gr</i>	Interface utilizada pelo SGSN para acessar dados residentes no HLR (por exemplo, perfil do assinante UMTS). Esta é a interface principal, enquanto que a <i>Gc</i> é opcional.
<i>Gs</i>	Interface opcional usada pelo SGSN para enviar informação de localização ao conjunto MSC/VLR. O SGSN pode receber requisição de busca (<i>paging</i>) da MSC através desta interface.
<i>B</i>	Interface responsável pela interconexão do MSC e VLR, usada no gerenciamento da base de dados dos assinantes que utilizam os serviços da área controlada pela MSC que está associada ao VLR. Oferece os serviços de localização, atualização de registro da UE e de dados associados aos <i>Supplementary Services</i> (SS).
<i>C</i>	Interface que faz a interconexão entre o MSC e HLR, usada quando o GMSC precisa interrogar o HLR associado ao assinante para a obtenção de informações necessárias ao roteamento de chamadas ou envio de SMS. Utiliza procedimentos específicos de sinalização especificados pelo <i>Mobile Application Part</i> (MAP).
<i>D</i>	Interface que interconecta o HLR e VLR, para troca de dados relacionados à localização da UE ou ao gerenciamento do assinante. O principal serviço oferecido é a capacidade de o UE originar e receber chamadas dentro da área de serviço. Utilizada na maioria dos procedimentos de sinalização (também usa o MAP).
<i>E</i>	Interface que conecta duas MSC (ou MSC com GMSC). Utilizada no procedimento de <i>handover</i> entre MSC diferentes. Também utiliza o MAP na sinalização.
<i>F</i>	Interface usada na conexão de MSC e EIR, sendo utilizada na verificação do estado do IMEI do UE. Visa apontar se o UE está habilitado ou não a acessar e usar os recursos da rede. Também usa o MAP na sinalização.

Adaptado de: [SVER 05].

⁶ ATM é uma arquitetura de rede de alta velocidade orientada a conexão e baseada na comutação de pacotes de dados. Utiliza para isto, o modo de transmissão assíncrono, sendo que através de seu protocolo ATM, encapsula os dados em pacotes de tamanho fixo de 53bytes (48bytes de dados e 5bytes de cabeçalho), criando as denominadas células ATM. Acessível através de <http://pt.wikipedia.org/>.

Tabela 13 – Componentes da arquitetura do UMTS.

Componentes	Descrição
UE	<i>User Equipment</i> ou equipamento do usuário é o terminal móvel (aparelho celular) juntamente com seu <i>Universal Subscriber Identity Module</i> (USIM) equivalente ao <i>SIM card</i> dos terminais GSM.
UTRAN	UMTS <i>Terrestrial Radio Access Network</i> ou rede terrestre de acesso via rádio baseada no <i>Wideband Code Division Multiple Access</i> (WCDMA).
<i>Node-B</i>	<i>Node-B</i> é o equipamento equivalente à BTS descrita no GSM. É neste dispositivo que se concentra o tráfego aéreo.
RNC	<i>Radio Network Controller</i> ou controlador de rede aérea é o mecanismo inteligente da rede, que coordena os <i>Node-B</i> , assim como a BSC controlava as BTS no GSM.
CN	<i>Core Network</i> ou núcleo da rede, é o ambiente que suporta serviços baseados em comutação de circuitos (CS) e comutação de pacotes (PS). Como no GSM/GPRS.
MSC	<i>Mobile Switching Center</i> ou centro de comutação móvel é o mecanismo por onde trafega a informação comutada a circuito. Como no GSM.
GMSC	<i>Gateway MSC</i> é o dispositivo que faz a interface com a PSTN, ISDN ou outras MSC.
HLR	<i>Home Location Register</i> ou registro de localização primário é o banco de dados no qual o UE está cadastrado (base de dados principal).
VLR	<i>Visitor Location Register</i> ou registro de localização visitante é o banco de dados temporário necessário para quando o UE está fora da sua área de registro. Ele, através da MSC, tem interação com o HLR.
EIR	<i>Equipment Identity Register</i> ou registro de identidade do equipamento é o banco de dados com as informações do UE. Da mesma forma que no GSM.
AuC	<i>Authentication Center</i> ou centro de autenticação é a entidade responsável pela guarda de informações de registro, permitindo o acesso do usuário ao sistema. Tem interatividade com o HLR.
SGSN	<i>Serving GPRS Support Node</i> ou nó de suporte a serviços GPRS é um dos elementos responsáveis pela operação da rede comutada a pacotes no UMTS.
GGSN	<i>Gateway GPRS Support Node</i> ou nó de suporte entre a rede UMTS e a PDN (ou a outra PLMN).

A *UMTS Terrestrial Radio Access Network* (UTRAN) [U401 00], composta pelos dispositivos *Node-B* (que faz interface com a UE) e RNC (que faz o controle de chamadas e sinalização), utiliza três tipos de canais para a comunicação, conforme mostra a Figura 27.

Os canais usados na UTRAN são: Canais Lógicos (que são mapeados nos Canais de Transporte), Canais de Transporte (que transportam diferentes fluxos de informação) e Canais Físicos (que compõem a interface *Uu* e alocam diferentes tipos de banda para diferentes finalidades). Os canais e as interações entre eles, serão vistos na próxima seção.

2.7.2. Canalização do UMTS WCDMA

Figura 27. Estrutura dos canais da UTRAN.
(Fonte: <http://www.teleco.com.br/>, consulta em 18/01/2008)

Os canais estão especificados nas Tabelas 14 (Canais Lógicos), 15 (Canais de Transporte) e 16 (Canais Físicos). O *downlink* (DL) é no sentido *Node-B* → UE e o *uplink* (UL) é no sentido UE → *Node-B*. Esta convenção pode ser utilizada tanto para a técnica FDD quanto para TDD.

O UMTS utiliza a tecnologia WCDMA na interface aérea (ou interface *Uu*). Esta interface está no contexto da *Universal Terrestrial Radio Access* (UTRA), que é o padrão 3G para serviços de comunicações móveis especificado pelo 3GPP [U105 99].

Tabela 14 – Canais Lógicos do UMTS (WCDMA).

Tipo de Canal	Sigla do Canal	Descrição do Canal	Uso (<i>downlink</i> / <i>uplink</i>)
Canais de Controle	BCCH	<i>Broadcast Control Channel</i> carrega as informações específicas do sistema e da célula através de <i>broadcasting</i> .	DL
	PCCH	<i>Paging Control Channel</i> é usado para enviar mensagens aos celulares (na <i>Paging Area</i> (PA)) e quando a rede não tem informação sobre a célula em que está localizada a UE ou quando a UE está no <i>sleep mode</i> .	DL
	DCCH	<i>Dedicated Control Channel</i> é o canal bidirecional que transfere informação de controle entre a rede e uma UE específica (dedicado). É alocado durante o procedimento de estabelecimento de conexão RRC.	DL / UL
	CCCH	<i>Common Control Channel</i> é o canal bidirecional P2P que transfere informação de controle entre a rede e as UE (comum). É usado quando as UE não têm conexão RRC com a rede ou quando a UE está utilizando os canais de transporte comuns durante o procedimento de re-seleção de nova célula.	DL / UL
Canais de Tráfego	DTCH	<i>Dedicated Traffic Channel</i> é o canal bidirecional P2P usado para transmissão de dados entre a rede e uma UE específica.	DL / UL
	CTCH	<i>Common Traffic Channel</i> é um canal do enlace direto ponto-multiponto (<i>multicast</i>) ou <i>Point to Multipoint</i> (PTM) unidirecional usado na transferência de informação de usuário entre a rede e um grupo específico de UE (por exemplo, o serviço <i>Cell-Broadcast</i>).	DL

Adaptado de: [SVER 05] e <http://www.umtsworld.com/>.

Tabela 15 – Canais de Transporte do UMTS (WCDMA).

Tipo de Canal	Sigla do Canal	Descrição do Canal	Uso (<i>downlink</i> / <i>uplink</i>)
Canais Dedicados	DCH	<i>Dedicated Channel</i> é o canal bidirecional P2P dedicado a uma UE específica na área de cobertura da célula.	DL / UL
	E-DCH	<i>Enhanced Dedicated Channel</i> é um canal P2P dedicado a uma UE específica na área de cobertura da célula. As mesmas funções melhoradas do DCH.	UL
Canais Comuns	BCH	<i>Broadcast Channel</i> é o canal do enlace direto PTM usado no transporte de informação de sistema, tendo taxa fixa e sendo sempre transmitido na área de cobertura de uma célula.	DL
	FACH	<i>Forward Access Channel</i> é o canal do enlace direto PTM que envia informações a muitas UE ou a uma específica, quando a rede tem conhecimento da localização do UE.	DL
	DSCH	<i>Downlink Shared Channel</i> é o canal de <i>downlink</i> compartilhado por várias UE. Associado a um ou mais DCH.	DL
	HS-DSCH	<i>High Speed Downlink Shared Channel</i> é um canal de <i>downlink</i> compartilhado por várias UE, o mesmo que o DSCH, porém, com alta velocidade. Está associado a um canal físico DPCH ou um ou mais HS-SCCH.	DL
	PCH	<i>Paging Channel</i> é o canal de procura e atualização da localização de UE.	DL
	RACH	<i>Random Access Channel</i> é o canal que leva informação proveniente da UE.	UL
	CPCH	<i>Common Packet Channel</i> é o canal aleatório aberto para a UE estabelecer contato com o <i>Node-B</i> , visando prover o controle de potência. Usado em conjunto com o DCH.	UL

Adaptado de: [SVER 05] e <http://www.umtsworld.com/>.

Tabela 16 – Canais Físicos do UMTS (WCDMA).

Tipo de Canal	Sigla do Canal	Descrição do Canal	Uso (downlink / uplink)
Canais do Enlace Direto	P-CCPCH	<i>Primary Common Control Physical Channel</i> é o canal usado para transmitir o canal de transporte BCH. Taxa fixa igual a do canal CPICH. SF=256.	DL
	S-CCPCH	<i>Secondary Common Control Physical Channel</i> é o canal usado para transmitir os canais de transporte FACH e PCH. Suporta combinações de formatos múltiplos implementados com a utilização do parâmetro <i>Transport Format Combination Indicator</i> (TFCI). Taxa fixa igual a do canal CPICH. SF=256.	DL
	SCH	<i>Synchronization Channel</i> é o canal de sincronização usado pela UE na procura de células em uma determinada área de cobertura. Formado por dois subcanais (primário e secundário). O primário é formado por um código modulado de comprimento 256chips denominado <i>Primary Synchronization Code</i> (PSC) e o segundo é formado por uma transmissão cíclica de 15 seqüências de códigos modulados com comprimento 256chips cada, chamado de <i>Secondary Synchronization Code</i> (SSC).	DL
	CPICH	<i>Common Pilot Channel</i> é o canal que transporta uma seqüência de bits predefinida com uma taxa fixa (30kbps, SF=256 (<i>Spreading Factor</i>)). <i>Primary Common Pilot Channel</i> (P-CPICH) (canal piloto com os mesmos códigos de canalização) e <i>Secondary Common Pilot Channel</i> (S-CPICH) (canal piloto com código de canalização arbitrário).	DL
	AICH	<i>Acquisition Indicator Channel</i> é o canal usado para transportar o <i>Acquisition Indicator</i> (AI) que corresponde à assinatura do canal PRACH. SF=256.	DL
	CD/CAICH	<i>Collision Detection/Channel Assignment Indication Channel</i> é o canal de taxa fixa utilizado para carregar o <i>Collision Detection Indicator</i> (CDI) ou o <i>Collision Detection Indicator/Channel Assignment Indicator</i> (CDI/CAI) ao mesmo tempo.	DL
	PICH	<i>Paging Indicator Channel</i> é o canal usado para transportar o indicador de busca (<i>paging</i>). Está sempre associado a um S-CCPCH, que por sua vez, é mapeado no canal de transporte PCH. SF=256.	DL
	HS-SCCH	<i>High Speed Shared Control Channel</i> é o canal utilizado para transportar sinalização relacionada com a transmissão do canal de transporte HS-DSCH. Taxa fixa de 60kbps e SF=128.	DL
	PDSCH	<i>Physical Downlink Shared Channel</i> é o canal usado para transportar o DSCH.	DL
	HS-PDSCH	<i>High Speed Physical Downlink Shared Channel</i> é o canal usado para transportar o canal de transporte HS-DSCH. Este canal pode utilizar os esquemas de modulação QPSK ou 16QAM. No QPSK temos M=2 e M=4 para o 16QAM (M = número de bits por símbolo).	DL
	AGCH	<i>Access Grant Channel</i> é usado para apontar recursos às requisições de acesso do usuário à rede. Os recursos incluem canais dedicados para serem utilizados ao longo da transmissão.	DL
	E-AGCH	<i>Enhanced Access Grant Channel</i> é o canal usado para transportar o canal de enlace reverso E-DCH. SF=256.	DL
	MICH	<i>Multimedia Broadcast/Multimedia Service Indicator Channel</i> é usado para transportar a notificação de indicação <i>Multimedia Broadcast/Multicast Service</i> (MBMS). Está sempre associado a um S-CCPCH no qual é mapeado o canal de transporte FACH.	DL
	DPCH	<i>Downlink Paging Channel</i> é o canal onde ocorre a multiplexagem dos canais dedicados DPDCH e DPCCCH. Efetua o controle de potência do transmissor através do parâmetro <i>Transmit Power Control</i> (TPC) e a sincronização do quadro WCDMA com o parâmetro <i>pilot</i> .	DL
	CSICH	<i>CPCH Status Indication Channel</i> é um canal utilizado para carregar a informação de status do CPCH. SF=256.	DL
Canais do Enlace Reverso	PRACH	<i>Physical Random Access Channel</i> é o canal usado para transportar o canal RACH. A transmissão do acesso randômico é baseada no protocolo <i>Slotted ALOHA</i> , no qual a UE pode iniciar a transmissão a partir de intervalos de tempo <i>access slots</i> ou Intervalo de Tempo de Canal (ITC).	UL
	DPCCCH	<i>Dedicated Physical Control Channel</i> é usado para transportar as informações de controle geradas pela camada 1 do WCDMA.	UL

Continua

Tipo de Canal	Sigla do Canal	Descrição do Canal	Uso (downlink / uplink)
Canais do Enlace Reverso	E-DPCCH	<i>Enhanced Dedicated Physical Control Channel</i> é o canal usado para transporte de informações geradas pela camada 1 do WCDMA. O mesmo do DPCCH, porém, com a interface melhorada em termos de conexão.	UL
	HS-DPCCH	<i>High Speed Dedicated Physical Control Channel</i> é o canal usado para transportar sinalização de retorno relacionada à transmissão do canal HS-DSCH, assim como no DPCCH, porém, com velocidade superior.	UL
	DPDCH	<i>Dedicated Physical Data Channel</i> é usado para transportar o canal DCH. A quantidade de DPDCH é variável em cada enlace de RF.	UL
	E-DPDCH	<i>Enhanced Dedicated Physical Data Channel</i> é o canal utilizado para transportar o canal E-DCH. Quantidade variável de E-DPDCH em cada enlace RF.	UL
	PCPCH	<i>Physical Common Packet Channel</i> é usado para transportar o CPCH. Em cada código de embaralhamento celular, são alocados possíveis códigos de 64 PCPCH.	UL

Adaptado de: [SVER 05] e <http://www.umtsworld.com/>.

Os canais destacados em azul nas tabelas acima são canais mais atuais, implantados no EDGE (E-DCH, E-AGCH, E-DPCCH e E-DPDCH), HSDPA (HS-DSCH, HS-SCCH, HS-PDSCH) e HSUPA (HS-DPCCH), com interfaces que oferecem maiores velocidades, e os demais são canais essenciais ao funcionamento do sistema, conforme mostra a Figura 28 e o exemplo da Figura 30.

Os componentes de acesso via rádio da UTRA são baseados no *Direct Sequence Code Division Multiple Access* (DS-CDMA) e em métodos de acesso híbrido como o *Time Division Code Division Multiple Access* (TD-CDMA). Estes componentes têm sido projetados para atender os requisitos da padronização 3G relativos à eficiência no uso do espectro de radiofrequência, mobilidade e *Quality of Service* (QoS).

A interface de rádio UTRA FDD é constituída dos canais mostrados nas Figuras 28 e 29. A conversão dos canais lógicos para os de transporte acontece na camada *Medium Access Control* (MAC) que é a subcamada localizada na camada de Enlace do modelo OSI (descrito na seção 2.2.4). Os canais são mapeados da camada superior para a inferior, ou seja: Camada Lógica para Camada de Transporte e esta para a Camada Física, como expõe a Figura 28.

Figura 28. Mapeamento dos canais nos enlaces direto e reverso do UMTS.

(Adaptado de: <http://www.umtsworld.com/>, consulta em 22/01/2008)

Radio Link Channel (RLC) é o enlace que interliga o UE ao BSS (*Node-B* e RNC), por onde trafega protocolos trocando informações de retransmissão e outros elementos referentes à interface rádio. O *Logical Link Control (LLC)* é a subcamada de protocolos entre o UE e a SGSN. A subcamada *Medium Access Control (MAC)* é o acesso rádio que aloca o controle e encaminhamento dos protocolos que circulam através dos Canais Físicos (nas Figuras 28 e 29, como PHY) descritos anteriormente. O modelo de camadas do UMTS é exposto na figura abaixo.

Figura 29. Distribuição das camadas do WCDMA.
(Fonte: <http://lee-1.com/>, consulta em 26/01/2008)

Packet Data Convergence Protocol (PDCP) é utilizado no UMTS para formatar os dados dentro de uma estrutura de camadas por prioridade para serem transferidos sobre a interface aérea e o *Broadcast and Multicast Control (BMC)* é o protocolo que adapta serviços de *broadcast* e *multicast* na interface aérea.

Figura 30. Distribuição das camadas e dos canais do WCDMA.
(Fonte: <http://wireless.agilent.com/>, consulta em 26/01/2008)

O *Radio Resource Control* (RRC) é a entidade que provém o serviço de transferência de informação para o *Non Access Stratum* (NAS) e está localizado em uma subcamada da camada 3 do WCDMA (Figura 32), estando somente no plano de controle. É responsável pelo controle da configuração das camadas 1 e 2, conforme a figura acima.

GPRS *Mobility Management* (GMM) e a pilha de protocolos *Session Management* (SM), entre o UE e SGSN, fazem anexação e desanexação do GPRS, ativação e desativação do *Packet Data Protocol* (PDP) como o IP ou X.25, dentre outras funções. A seguir é apresentado um esquema, exemplificando o modo de operação dos canais em uma rede UMTS.

Figura 31. Exemplo simplificado de recebimento de chamada no UMTS.
(Fonte: <http://www.gta.ufrj.br/>, consulta em 22/01/2008)

Neste exemplo, existe a interação entre os componentes da rede (UE, *Base Station* (BS) ou *Node-B*, RNC e CN ou NSS) e os canais descritos nas Tabelas 14 a 16, pelos quais ocorrem as comunicações.

Neste exemplo um usuário recebe uma chamada, porém, antes do recebimento, a RNC faz o sincronismo com o UE e troca informações com a finalidade de identificação do UE através do IMSI, que se encontra no *Universal Subscriber Identity Module* (USIM). Depois da conferência do IMSI, pelo *Node-B*, o UE interage com a CN para obter as configurações do canal de comunicação (BW, nível de potência, entre outras) que será alocado para a conversação entre origem e destino.

Por fim, quando o usuário atende à chamada, existe então uma sinalização na rede referente ao atendimento e, posteriormente, já com a conversação, existe o tráfego de voz e a sinalização da chamada em curso, trocados entre o UE e CN.

O UMTS utiliza o *Adaptive Multi Rate* (AMR) para compressão de voz, que se baseia no oferecimento de oito diferentes taxas de bits conforme as condições do enlace. O uso do AMR requer uma adaptação otimizada do enlace para selecionar o melhor modo *codec*, conforme os requisitos de capacidade e canal de RF. Ou seja, se as condições do canal de RF forem ruins, a codificação na fonte é reduzida e a codificação no canal é melhorada. O AMR pode trabalhar com diferentes técnicas, como *Algebraic Code Excited Linear Prediction* (ACELP), *Discontinuous Transmission* (DTX), *Voice Activity Detection* (VAD) e *Comfort Noise Generation* (CNG). Todas estas técnicas são utilizadas na transmissão, visando melhorar algumas características inerentes do sistema.

2.7.3. WCDMA

A interface rádio *Uu*, descrita anteriormente como parte dos canais físicos, situada entre o UE e a UTRAN, é baseada no *Wideband Code Division Multiple Access* (WCDMA). O WCDMA é um padrão de interface rádio desenvolvido para o UMTS e padronizado pela ITU [M687 97]. Por estar implantando uma interface completamente nova, o WCDMA pode ampliar a BW do canal de RF para 5MHz, podendo operar de duas formas distintas:

- *Frequency Division Duplex* (FDD): neste modo, os enlaces de subida e descida utilizam canais de 5 MHz diferentes e separados por uma faixa de frequência de 190MHz;
- *Time Division Duplex* (TDD): neste modo, os enlaces de subida e descida compartilham a mesma banda de 5MHz, porém, alternadamente no tempo.

Tabela 17 – Comparação entre os modos de operação FDD e TDD do WCDMA.

	FDD	TDD
Método de Acesso Múltiplo	DS-CDMA	DS-CDMA
Alocação de Banda	1920 – 1980MHz (UL) 2110 – 2170MHz (DL)	1900 – 1920MHz (UL) 2010 – 2025MHz (DL)
Fator de Reuso de Frequência	1	1
Banda por Portadora	5MHz	5MHz ~ 1,6MHz
<i>Chip Rate</i>	3,84Mcps	3,84Mcps ou 1,28Mcps
Comprimento do <i>Frame</i>	10ms (38400chips)	10ms
Tipo de Modulação	QPSK	QPSK
Codificação de Voz	AMR SID <i>codecs</i> (Frame tipo 8)	AMR GSM EFR <i>codecs</i> (Frame tipo 7)
Nº. de <i>Slots/Frame</i>	15	15
Máxima Taxa de bits em um Canal RF	2,3Mbps	3,3Mbps
Controle de Potência (<i>range</i>)	80dB UL e 30dB DL	65dB UL e 30dB DL
Fator de Espalhamento (UL)	4 a 256	1, 2, 4, 8 e 16
Fator de Espalhamento (DL)	4 a 512	1, 2, 4, 8 e 16

Adaptado de: (<http://www.umtsworld.com/>, consulta em 15/01/2008).

Os sistemas iniciais utilizavam o UTRA FDD (ou WCDMA FDD). Porém, nas faixas de frequência de 1900 a 1920MHz (UL) e 2010 a 2025MHz (DL), a tecnologia UTRA TDD (ou WCDMA TDD) [HAAR 00] que é semelhante à UTRA FDD, exceto pelo modo como utiliza o canal de RF (*Radio Frequency*). O UTRA TDD apresenta-se como uma boa solução para aproveitar o espectro. Estuda-se o uso da UTRA TDD em ambientes de pico-célula [GERL 02]. Ambas podem ser vistas através da figura a seguir:

Figura 32. Modos de transmissão FDD e TDD do UMTS.

(Fonte: <http://paginas.fe.up.pt/>, consulta em 10/01/2008)

Em um sistema CDMA, existe o espalhamento do sinal com as devidas codificações. Estes códigos não são feitos para obter-se uma chamada segura e sim para criar uma identificação única no sistema. Os códigos de espalhamento são ruídos como códigos pseudo-randômicos (*Pseudo-Noise* (PN)). Os códigos de canal são projetados para que tenham a máxima separação entre si e os códigos de identificação de célula estão balanceados para que não haja igualdade de códigos.

O WCDMA utiliza como método de acesso o CDMA, juntamente com a tecnologia de espalhamento espectral *Direct Sequence Spread Spectrum* (DSSS), formando o DS-CDMA. Neste modo de operação, os terminais compartilham a mesma banda de frequências, porém, com cada UE obtendo e utilizando um código diferente. Este processo é feito através da combinação de informação banda-base e alta taxa de chips de código binário.

O *Spreading Factor* (SF) é obtido pela razão entre chips e taxa de informação de banda-base (o UMTS tem 3,84Mcps). Os SF variam de 4 a 512 no modo UTRA FDD. O processo de espalhamento tem ganho que pode ser expresso em dB⁷, como SF=128 → ganho de 21dB. O mais baixo SF é o que possui a maior taxa de dados. No SF, o *Orthogonal Variable Spreading Factor* (OVSF) é um código usado no processo de espalhamento e desordenação.

⁷ dB ou decibel é uma medida da razão entre duas quantidades, sendo usada para uma grande variedade de medições em acústica, física e eletrônica. É uma unidade de medida adimensional semelhante à porcentagem. A definição do dBW refere-se a 1W. No caso de uso em medição de potência, tem-se que 3dB corresponde ao dobro de potência em Watts. Site para consulta: <http://pt.wikipedia.org/wiki/Decibel>.

Os OVSF podem ser definidos através da árvore OVSF, ilustrada abaixo:

Figura 33. Árvore usada na geração de códigos OVSF.
(Fonte: <http://www.mathworks.com/>, consulta em 24/01/2008)

O código OVSF é dado por $C_{N,K}$, onde N é o fator de espalhamento do código (no caso do modo UTRA FDD o SF é de 4 a 512) e K é o número do código para o intervalo discriminado por $0 \leq K \leq N-1$. Cada nível da árvore de código define o comprimento do fator de espalhamento e o método para a obtenção é mostrado através da matriz:

$$C_{2N} = \begin{bmatrix} C_N(0) & C_N(0) \\ C_N(0) & -C_N(0) \\ C_N(1) & C_N(1) \\ C_N(1) & -C_N(1) \\ \dots & \dots \\ C_N(N-1) & C_N(N-1) \\ C_N(N-1) & -C_N(N-1) \end{bmatrix} \quad (7)$$

onde C_N tem as variações em C_i para as decisões de caminho ($x_i = 0$ ou $x_i = 1$):

$$C_{i+1} = \begin{cases} C_i C_i & \text{if } x_i = 0 \\ C_i (-C_i) & \text{if } x_i = 1 \end{cases} \quad (8)$$

A tabela abaixo mostra um exemplo para a conversão de 6_{10} (6 na base 10) para o correspondente 110_2 (110 em binário). Neste caso adiciona-se um zero à esquerda (0110), pois o comprimento é dado por $4 = \log_2 16$.

Tabela 18 – Tabela de seqüência de códigos C_i .

i	x_i	C_i
0		$C_0 = [1]$
1	0	$C_1 = C_0 C_0 = [1] [1]$
2	1	$C_2 = C_1 C_{-1} = [1 1] [-1 -1]$
3	1	$C_3 = C_2 C_{-2} = [1 1 -1 -1] [-1 -1 1 1]$
4	0	$C_4 = C_3 C_3 = [1 1 -1 -1 -1 -1 1 1] [1 1 -1 -1 -1 -1 1 1]$

Fonte: (<http://www.mathworks.com/>, consulta em 24/01/2008).

Como dito anteriormente, o SF é calculado através da razão entre a taxa de chips (ou taxa do canal) pela taxa de dados (ou taxa de símbolos a serem enviados pelo canal), assim como mostra a Figura 34.

Figura 34. Ilustração do cálculo do *Spreading Factor* (SF).
(Fonte: <http://www.umtsworld.com/>, consulta em 20/01/2008)

Como visto anteriormente, o WCDMA é subdividido em camadas, sendo elas a L1 (camada Física), L2 (camada de Enlace de Dados) e L3 (camada de Rede). As camadas foram ilustradas através das Figuras 29 e 30.

2.7.4. Integração entre GERAN e UTRAN

Durante o processo de passagem do 2G/2,5G/2,75G para o 3G, haverá uma convivência de CN GSM/UMTS, como na Figura 35, sendo duas opções para o acesso rádio:

- GSM/EDGE – através da GSM/EDGE *Radio Access Network* (GERAN);
- WCDMA – através da UMTS *Terrestrial Radio Access Network* (UTRAN).

Figura 35. Arquitetura do UMTS com interface GERAN (release 4).

Até o *release 4*, as especificações do GERAN desenvolvidas pelo 3GPP estavam baseadas na hipótese de que existiam duas interfaces separadas entre BSC e CN, denominadas: *A* – interface entre BSC e MSC para serviços CS, como gerenciamento do BSS e mobilidade; e *Gb* – entre BSC e nós de suporte para os serviços PS do GPRS e EDGE.

As camadas 1 e 2 da interface *A* são baseadas nos níveis 2 e 3 do SS7, ou seja, no MTP. Esta camada foi modificada para a operação em velocidades mais altas, como dito anteriormente. A interface *Iur-g* permite o interfuncionamento (conectividade) entre as redes UTRAN e GERAN.

Figura 36. Arquitetura do UMTS com interface GERAN (*release 5*).

A partir do *release 5*, o GERAN passou adotar a interface *Iu* entre a GERAN e NSS, já utilizada pelo UMTS, garantindo que um conjunto similar aos serviços CS e PS do UMTS pudessem ser fornecidos através das duas opções de acesso rádio: GSM/EDGE e WCDMA. Com esta adoção, serviços desenvolvidos para o núcleo do UMTS puderam ser utilizados pelas duas interfaces rádio, além de outras tecnologias como o *Wireless Local Area Network* (WLAN), que serão incorporadas na universalidade do modelo [WONG 03].

2.7.5. IPsec

IPSec ou *IP Security Protocol* é uma extensão do IP, que visa a padronizar o

fornecimento de: privacidade do usuário (aumentando a confiabilidade das informações fornecidas pelo usuário para um determinado local na PDN, por exemplo, como bancos), integridade dos dados (garantindo que o conteúdo recebido seja da origem verdadeira), autenticidade das informações (ou *identity spoofing*, é a garantia de que uma pessoa é quem diz ser) e não repudição (quando uma informação transmitida e recebida por um destino, tem sua autenticidade e o seu envio não pode ser negado pela origem).

Este protocolo opera sob a camada de Rede (camada 3) do modelo OSI. Outros protocolos de segurança da Internet como *Secure Socket Layer* (SSL) e *Transport Layer Security* (TLS) operam desde a camada de Transporte (camada 4) até a camada de Aplicação (camada 7) do modelo OSI. Isto torna o IPsec mais flexível, pois pode ser utilizado na proteção dos dados transferidos pelos protocolos TCP e UDP, porém, aumentando a complexidade e mecanismos gerais de processamento.

2.7.6. VoIP

Figura 37. Arquitetura do UMTS com interface VoIP.

Voice over IP (VoIP) é o nome dado aos serviços utilizados para carregar voz sobre protocolo IP, ou seja, possibilitando o tráfego de voz pela rede de pacotes. A telefonia baseada em redes de pacotes já dá passos de plena maturidade, sendo que muitos fornecedores

de telefonia IP e serviços 0800 estão incorporando-se neste novo paradigma. Com o VoIP existe a provisão de melhor qualidade no transporte da voz e, ao mesmo tempo, economia em banda passante.

A Figura 37 ilustra a interconexão do VoIP ao UMTS. Na figura é apresentada a conexão de dispositivos através da Internet. O UE, de sua *Home Public Land Mobile Network* (HPLMN), se comunica com a CN até alcançar a Internet, para então, ser encaminhada a sessão até o PABX VoIP da Empresa 2, que encaminhará a chamada até o destino.

Dentro do contexto VoIP, dois padrões principais fazem parte da telefonia IP: o H.323 (da ITU-T), que está presente em muitos equipamentos e softwares VoIP, e o *Session Initiation Protocol* (SIP) (proposto pelo IETF), que tem mobilizado muitos fabricantes das áreas de telefonia e dados, devido à flexibilidade, aderência a padrões genuinamente Internet e arquitetura aberta.

O VoIP utiliza protocolos como o *Media Gateway Control* (MEGACO) que é usado para criar, modificar e excluir cadeias de mídia através do *Media Gateway* (MGW) e ainda, negociar os formatos de mídia a serem empregados no sistema. O MGW dá suporte ao tráfego de sinalização e *bearer*, e o MEGACO é padronizado através do H.248, tendo colaboração do ITU-T e IETF.

Na arquitetura VoIP, o *Media Gateway Control Protocol* (MGCP) faz a integração do SS7 em redes VoIP e é composto por um *Call Agent* (CA), no mínimo um *Media Gateway* (MGW) e um *Signalling Gateway* (SG) quando conectado à PSTN.

O SIP é um protocolo de sinalização de telefonia IP usado para estabelecer, modificar e finalizar chamadas telefônicas VoIP, sendo desenvolvido pela IETF (RFC 3261). O SIP se assemelha ao HTTP, pois é baseado em texto, sendo, portanto, bastante flexível e aberto. O SIP utiliza o *Session Description Protocol* (SDP), que é padronizado pelo IETF (RFC 4566), sendo um formato para descrição dos parâmetros de inicialização de *streaming* de mídia, ou seja, de conteúdo visto ou ouvido pelo usuário durante uma transmissão de dados.

2.7.7. IMS

O *IP Multimedia Subsystem* (IMS) tem tornado-se a base para avanços na arquitetura *Next Generation Network* (NGN) das operadoras de telefonia móvel, fixa e a cabo. Com esta tecnologia obtêm-se menores custos, diferenciação de serviços e convergência entre as redes móveis e fixas. O IMS, como definido pelo 3GPP, habilita provedores de serviço a desenvolverem arquiteturas comuns de entrega para qualquer tipo de serviço, utilizando qualquer meio e alcance a qualquer tipo de consumidor, independentemente de conhecerem o

caminho pelo qual seguirão os pacotes ou conexões na rede.

Servidores de mídia (ou *Application Servers (AS)*) são importantes partes do IMS nas redes sem fio (*wireless*) oferecendo serviços multimídia e de voz. Na arquitetura 3G e em geral, um servidor de mídia IP suporta o *Multimedia Resource Function Processor (MRFP)* na área correspondente ao PS. O MRFP faz integração com o GGSN e SGSN via RTP. *Multimedia Resource Function Controller (MRFC)* é o mecanismo coordenado pelo *Call Session Control Function (CSCF)* em conjunto com um AS. A mixagem de várias cadeias de mídia é passada ao *Multimedia Resource Function (MRF)* que compreende o MRFC e MRFP. O MRFC controla as cadeias de mídia estabelecidas pelo MRFP, baseando-se na informação fornecida pelo CSCF e o AS envolvido.

Similarmente ao que ocorre com o MGCP, acontece com o *Media Gateway Control Function (MGCF)* e MGW, que fazem a conversão dos sinais entre circuitos (CS) e pacotes (PS). Ambos utilizam a evolução do MGCP, que é o H.248 (ou o MEGACO), que pode ser utilizado entre MRFP e MRFC, através da interface *Mp*, para estabelecimento de conexão IP e, se necessário, *bearers* do SS7 garantem o suporte às cadeias de mídia mixadas.

Figura 38. Arquitetura IMS.

(Fonte: <http://www.radisys.com/>, consulta em 20/01/2008)

2.7.8. All-IP

O 3GPP propôs como padrão a junção entre o UMTS e uma arquitetura IP (*All-IP*), com o objetivo de integrar as tecnologias IP e *wireless*. Esta arquitetura está em desenvolvimento desde o padrão GSM, passando pelo GPRS e então ao UMTS (nos *releases* 99 e 00, sendo que o *release* 00 incorpora os *releases* 4 e 5). No *release* 4 introduz-se a

arquitetura NGN para o CS e no release 5 o IMS no PS.

A *Core Access Layer* (CAL), ou núcleo da camada de acesso, é a parte da rede que encaminhará os serviços IP para os níveis de controle, como o *Network Control Layer* (NCL) e *Service/Management Layer* (SML), ou de usuário (PSTN, PLMN, Internet, UMTS, WLAN, etc.). Para as interfaces na CAL, utilizam-se as tecnologias IP no endereçamento, ATM no transporte e *Multi Protocol Label Switching* (MPLS) para diferenciação dos serviços. O MPLS define prioridades incluindo um *label* no cabeçalho de pacotes encaminhados pela rede, este *label* informa ao ATM a prioridade e o ATM examina e comuta os pacotes em alta velocidade, por exemplo, como os pacotes de mídia em tempo real.

Figura 39. Arquitetura All-IP.

(Fonte: <http://www.huawei.com/>, consulta em 25/01/2008)

2.7.9. CAMEL

Um dos maiores melhoramentos realizados no GSM fase 2 é a integração entre rede móvel e a *Intelligent Network* (IN). Neste contexto aparece o *Customised Application for Mobile network Enhanced Logic* (CAMEL) que é uma característica do GSM fase 2 que dá suporte à *Operator Specific Services* (OSS). O CAMEL é uma característica para criar serviços, ou seja, não é um serviço específico, trabalhando no UMTS *Virtual Home Environment* (VHE).

O CAMEL na primeira versão (*release 96*) oferece serviços de supervisão e triagem de chamadas originadas e recebidas, translação de números, melhoramento no encaminhamento de chamadas e *Fraud Information Gathering Services* (FIGS). O CAMEL, nesta fase, é limitado a serviços e pontos de *trigger* para respostas e desconexões de chamadas. Na fase 2 (*release 97*), o CAMEL inclui o *Support Private Numbering Plan* (SPNP), *Prepaid Card Service with Advice of Charge* (PCSAC), *Free Phone and Universal*

Number (FPUN) e *CAMEL Service Environment* (CSE). O CSE possibilita ao assinante receber mensagens em sua língua nativa até em *roaming*.

Na fase 3 (*release 98*), adicionais características foram alocadas para o acesso total à IN por usuários em *roaming*. A HPLMN e VPLMN são conectadas a várias plataformas IN utilizadas entre redes nacionais, provendo características como serviços de *roaming* pré-pago, números especiais e grupos fechados de numeração pessoal (números de equipes de trabalho, por exemplo), além de serviços dependentes de localização mais complexos.

Na fase 4 (*release 00*), desenvolve-se a especificação do *CAMEL Application Part* (CAP). O CAMEL torna-se atraente, pois é um método relativamente barato de instalação para adição de novos serviços à infra-estrutura de rede existente das operadoras.

2.7.10. WAP

O *Wireless Application Protocol* (WAP) refere-se a um grupo de tecnologias e protocolos amplamente utilizados como padrões *de fato*, provendo acesso à Internet aos dispositivos móveis (ou *Mobile Equipment* (ME)) ou a outros dispositivos.

Um típico uso do WAP é visto na transmissão de um *Website* com várias versões internas de páginas *Web* otimizadas para o uso em dispositivos celulares. Quando é usado juntamente com o *Wireless Markup Language* (WML), *hyperlinks* podem ser acessados através do uso das teclas do aparelho celular em conjunto com *hotkeys*.

O WAP foi proposto e desenvolvido por um grupo denominado *WAP Forum*, sendo reconhecido posteriormente pelo IEEE. Ele se baseia nos padrões de Internet já existentes, como o *HyperText Markup Language* (HTML), *Extensible Markup Language* (XML), *Extended HTML* (XHTML) e TCP/IP. O WAP será combinado com o GPS e outras tecnologias de localização no modelo da arquitetura 3G, disponibilizando com o mínimo esforço entre as partes, serviços baseados em localização e tempo.

Figura 40. Arquitetura e modelo de referência WAP1.
(Fonte: <http://www.tml.tkk.fi/>, consulta em 25/01/2008)

A suíte WAP é baseada nas camadas do modelo OSI. No nível mais baixo, o *Wireless Datagram Protocol* (WDP) transfere informação da origem ao destino e é modelado com o *User Datagram Protocol* (UDP) no método de entrega de melhor esforço do IP. Acima do WDP existe o *Wireless Transport Layer Security* (WTLS) que faz a segurança no tráfego de dados, como autenticação, confidencialidade e integridade, e o *Wireless Transaction Protocol* (WTP) que faz a certificação de que os fragmentos de dados enviados sejam realmente recebidos, usando, para isso, a comunicação de reconhecimento dos pacotes (*Acknowledgement* (ACK) e *Non Acknowledgement* (NACK)). Por último estão as camadas *Wireless Session Protocol* (WSP) que executa a seção entre os sistemas de comunicação e *Wireless Application Environment* (WAE) que provém um ambiente onde rodam aplicações WAP e Web.

Figura 41. Comparação entre as arquiteturas WAP1 e WAP2.

(Fonte: <http://www.cs.wustl.edu/>, consulta em 25/01/2008)

No WAP1 (*release 98*), assume-se que os dispositivos móveis têm baixa potência, dentre outros recursos e possibilita simplicidade no compartilhamento de segurança com os *gateways* (GW). Foi gerado o WAP2 através do *release 02*, o qual assume que os dispositivos móveis são poderosos e podem se conectar diretamente aos servidores de informação. A figura anterior mostra as pilhas de protocolo do WAP1 e WAP2.

A suíte WTLS provê o protocolo de estabelecimento de chave, volume do algoritmo de encriptação e algoritmo MAC. O conjunto SSL/TLS pode ser utilizado independentemente no WTLS.

Os protocolos utilizados na estrutura de segurança do WAP são:

- *Key Exchange Suite* (KES): é o responsável por estabelecer uma chave secreta entre cliente e servidor. Um exemplo é o *Rivest Shamir & Adleman* (RSA) que consiste em situações onde o *gateway* WAP envia um certificado que englobam a chave pública RSA do GW e a assinatura pela chave privada da *Certification Authority* (CA). Os clientes checam a validade da assinatura da CA e, se for válida, o cliente gera um valor secreto e o

encripta com a chave pública do GW. A partir deste ponto, ambos os lados podem calcular as chaves comuns entre eles utilizando o valor secreto. No caso de não validade da assinatura da CA, a comunicação é abortada;

- *Bulk Encryption and MAC Suite* (BEMS): a *Bulk encryption* (ou encriptação de volume) é usada para a confidencialidade dos dados e o *Message Authentication Code* (MAC) é usado para a integridade. Neste caso, a chave comum que foi calculada na KES pode ser utilizada para ambos os propósitos. Na encriptação de volume, algoritmos como *Data Encryption Standard* (DES), *Triple Data Encryption Standard* (3DES), *International Data Encryption Algorithm* (IDEA) e *Rivest Cipher 5* (RC5) são utilizados. Para a integridade, o WTLS usa o algoritmo *Hash Message Authentication Code* (HMAC) que, por sua vez, utiliza o *Secure Hash Algorithm 1* (SHA-1) ou *Message Digest 5* (MD5);
- *WAP-Profiled TLS* (WPT): o WAP2 utiliza o WPT que consiste em um conjunto de cifragem, autenticação, capacidade de tunelamento, resumo e identificação de sessão. O conjunto de cifragem consiste no estabelecimento de chaves, encriptação e integridade. Um identificador de sessão é usado para identificar uma sessão específica e a autenticação cliente/servidor é feita utilizando-se mecanismos de certificados parecidos ao WTLS. Por fim, o tunelamento é a forma de configuração entre cliente e servidor, possibilitando a comunicação mesmo se as camadas de rede subjacentes forem diferentes;
- *WAP Identity Module* (WIM): é o método de identificação na estrutura do WAP, habilitando dispositivos a terem identificações separadas, o que acarreta, no caso de *update* do dispositivo, não haver alteração do número de telefone ou informação de bilhetagem. O WIM proporciona operações como geração de chaves, números randômicos, assinaturas, encriptação/decriptação, troca de chaves, armazenamento de certificados e outras funcionalidades de segurança.

2.7.11. HSPA – HSDPA e HSUPA

O *High Speed Packet Access* (HSPA) é formado pelo *High Speed Downlink Packet Access* (HSDPA) e *High Speed Uplink Packet Access* (HSUPA). O HSDPA é um serviço de dados da parte relacionada à PS no *downlink* do WCDMA, com taxa de transmissão de dados acima de 8 a 10Mbps, trabalhando sobre uma BW de 5MHz. As implementações incluem o *Adaptive Modulation and Coding* (AMC), *Multiple-Input and Multiple-Output* (MIMO), *Hybrid Automatic Repeat reQuest* (HARQ), procura rápida de células e projeto avançado no receptor. Foi desenvolvido para ter compatibilidade com o exposto no *release 99* do 3GPP.

Nas especificações do 3GPP, o *release 4* provê eficiente suporte ao IP, habilitando o fornecimento de serviços através de um CN *All-IP* e o *release 5* foca no HSDPA, além do IMS, para que as taxas de dados cheguem a aproximadamente 10Mbps, munindo a rede para operar serviços multimídia baseados em pacotes.

O HSUPA tem a mesma função que o HSDPA, porém, para o enlace de subida (*uplink*) fornecendo velocidade de até 5,7Mbps na transmissão de dados de *upload*.

As especificações do *release 6* trabalham sobre o MIMO, que segundo o 3GPP, deve alcançar taxas acima de 20Mbps. A tabela abaixo mostra a evolução do GSM em direção à rede de pacotes.

Figura 42. Evolução até o HSDPA e tendências.
 (Fonte: <http://tech.digitimes.com.tw/>, consulta em 25/01/2008)

2.7.12. Migração no Brasil

A implantação do UMTS por uma operadora envolve uma série de aspectos que vão desde a disponibilidade de terminais à existência de serviços desenvolvidos para o usuário.

Figura 43. Alocação de banda sugerida pela WRC2000.
 (Fonte: <http://www.umtsworld.com/>, consulta em 25/01/2008)

O UMTS assumiu como hipótese que o novo sistema seria implantado utilizando novas faixas de frequências a serem adquiridas pelas operadoras, sendo necessária a disponibilidade de espectro de RF para a adoção do WCDMA com canais de 5MHz.

O IMT-2000, na WRC2000 [WRC00], alocou frequências para os sistemas móveis celulares, possibilitando não só a implantação de novos sistemas, como também, um alinhamento global das frequências a serem utilizadas no 3G, em grande parte do mundo. A Anatel alocou as frequências na faixa de 1,8GHz para as bandas D e E, tendo como objetivo preservar a faixa de 1,9GHz para os sistemas 3G. Seguindo esta estratégia, as operadoras de GSM dispõem de tempo e podem fazer esquemas de migração graduais para o UMTS, através da implantação do EDGE. A abrangência inicial (área de cobertura) do UMTS será menor que a dos outros sistemas devido à transição gradual.

2.7.13. Considerações do UMTS

Este padrão foi desenvolvido pelo 3GPP devendo incorporar em seus futuros *releases* o IP *Multimedia Subsystem* (IMS) em sua *Core Network* (CN), o que permitirá a um usuário estabelecer uma sessão multimídia com outro usuário, ou seja, a estrutura *All-IP*. Com a implantação do *High Speed Downlink Packet Access* (HSDPA) e do *High Speed Uplink Packet Access* (HSUPA) a taxa de dados será ampliada nos enlaces de descida e subida, respectivamente. As primeiras redes UMTS entraram em operação na Europa em 2003 e a previsão de início para operação no Brasil é no 2º semestre de 2008.

Enquanto o modo FDD é destinado especialmente a grandes coberturas, aplicações de banda larga e de rádio simétricas como vídeo e telefonia móvel, utilizando uma grande gama de frequências, o modo TDD proporciona altas taxas de dados para aplicações assimétricas e de reduzida mobilidade, incluindo serviços baseados na Internet, aproveitando melhor o uso do espectro de radiofrequência.

A Tabela 19 dá uma visão panorâmica sobre os principais padrões mais disseminados no mundo. Outra comparação que demonstra a força e respectivas opções dos padrões 3G é representada através da Tabela 20, na qual pode-se observar que o UMTS WCDMA e CDMA2000 1xEV-DO, utilizam o CDMA como método de acesso múltiplo, porém, apresentam diferenças como uso de portadoras, largura de banda dos canais de RF, estrutura de frame e sincronismo na Estação Rádio-Base (ERB).

Como a evolução da rede de pacotes trouxe novos horizontes, na Tabela 21 é feita a comparação do HSDPA (da estrutura UMTS) com o 1xEV-DV (da estrutura CDMA2000).

Tabela 19 – Comparação entre os padrões utilizados em tecnologia celular.

Geração	Padrão	Padronização	Taxa de Dados	Número de Canais	Número de Usuários por Canal	Tecnologia de Acesso Múltiplo	Largura do canal	Tipo de Modulação
1G	AMPS	NAMPS IS-41 EIA/TIA-553	10kbps (somente canal de controle)	832	1	FDMA/FDM FDD	30kHz	FM (voz) FSK (dados)
2G	TDMA	IS-54 e IS-136	48,6kbps	832 (2496 para 3 slots)	3 para <i>Full-rate</i> 6 para <i>Half-rate</i>	TDMA/FDM FDD	30kHz	$\pi/4$ Shifted DQPSK
2G	GSM	GSM 02.01	9,6kbps <i>Half-rate</i> 13kbps <i>Full-rate</i>	124 no P-GSM900 374 no DCS1800 (2992 para 8 slots no DCS1800)	8 para <i>Full-rate</i> (voz)	TDMA/FDM FDD	200kHz	0,3GMSK
2G	CDMAone	IS-95A e IS-95B	14,4kbps	20	798 (depende da relação S/N)	CDMA/FDM FDD	1,25MHz	QPSK e OQPSK
2,5G	GPRS	GSM 03.60	115kbps	124 no P-GSM900 374 no DCS1800	8 para <i>Full-rate</i>	TDMA/FDM FDD	200kHz	GMSK
2,75G	EDGE	GSM 03.64	473,6kbps (69,2kbps por time slot)	124 no P-GSM900 374 no DCS1800	8 para <i>Full-rate</i>	TDMA/FDM FDD	200kHz	8-PSK
3G	CDMA2000 1xRTT	ANSI-41 EIA/TIA TR 45.5 ITU-R M.1457	9,6kbps (<i>outdoor</i>) 2Mbps (<i>indoor</i>)	48 (N=1) 24 (N=2) 16 (N=3)	1,2288Mcps (x N portadoras)	CDMA FDD	1xRTT 1,25MHz 3xRTT 3,75MHz	BPSK, QPSK, 8-PSK e 16QAM
3G	CDMA2000 1xEV-DO	3GPP2 A.S00007	153kbps (<i>outdoor</i>) 2,46Mbps (<i>indoor</i>)	48 (N=1) 24 (N=2) 16 (N=3)	1,2288Mcps (x N portadoras)	CDMA/OFDM FDD	1,25MHz	QPSK, 8-PSK e 16QAM
3G	CDMA2000 1xEV-DV	3GPP2 C.S0033-0	614,4kbps (<i>outdoor</i>) 3,09Mbps (<i>indoor</i>)	48 (N=1) 24 (N=2) 16 (N=3)	1,2288Mcps (x N portadoras)	CDMA FDD	1,25MHz	QPSK, 8-PSK e 16QAM
3G	UMTS (WCDMA)	3GPP TS 25.213 ITU-R M.1457	144kbps (<i>outdoor</i>) 384kbps (<i>urban</i>) 2Mbps (<i>indoor</i>)	23 UMTS ITU 12 UMTS Anatel	3,84Mcps	WCDMA, FDD e TDD	5MHz	QPSK
3G	HSDPA	3GPP TS 25.101 3GPP TS 25.890	0,9Mbps (<i>outdoor</i>) 14,4Mbps (<i>indoor</i>)	23 UMTS ITU	3,84Mcps	WCDMA (adaptado), FDD e TDD	5MHz	AMC, QPSK e 16QAM

Tabela 20 – Comparação entre UMTS WCDMA e CDMA2000 1xRTT.

Característica	WCDMA	CDMA2000 1xRTT
Modos de Operação	FDD e TDD	FDD
Origem do padrão	Europa	E.U.A
Alocação de Banda	No FDD: 1920 – 1980MHz (UL) 2110 – 2170MHz (DL) No TDD: 1900 – 1920MHz (UL) 2010 – 2025MHz (DL)	No FDD: 1850 – 1910MHz (UL) 1930 – 1990 (DL)
Banda por Portadora	5MHz	1,25 x N MHz Inicialmente com N = 1, 2 ou 3 e posteriormente N = 6, 9 ou 12
Estrutura de <i>Frame</i>	10ms	20ms
Chip Rate	3,84Mcps	1,2288Mcps x N portadoras

Continua

Característica	WCDMA	CDMA2000 1xRTT
Tipo de Modulação	QPSK	QPSK
Codificação de Voz	AMR	AMR
Capacidade de Transferência de Dados do Usuário	Modo CS acima de: 144kbps, 384kbps e 2048kbps Modo PS até: 144kbps, 384kbps e 2048kbps	144kbps, 384kbps e 2048kbps
Interface de Rede 3G	GSM MAP	ANSI-41
Frequência do Controle de Potência	1,5kHz	0,8kHz
Sincronismo na ERB	Não necessita	Necessita

Fonte: [KARI 02], pg. 23.

Tabela 21 – Comparação entre UMTS HSDPA e CDMA2000 1xEV-DV.

Característica	HSDPA	1xEV-DV
Tamanho de <i>Frame</i> (DL)	2ms TTI (3 <i>slots</i>)	1,25, 2,5, 5 ou 10ms (tamanho de <i>frames</i> variável) com 1,25 de tamanho de <i>slot</i>
<i>Channel Feedback</i>	Qualidade de canal reportada à taxa de 2ms ou 500Hz	C/I feedback a 800Hz (todo 1,25ms)
Multiplexação de dados	TDM/CDM	TDM/CDM (<i>frame</i> variável)
Modulação Adaptativa e Codificação	QPSK e 16QAM (16QAM mandatório)	QPSK, 8-PSK e 16QAM
HARQ	<i>Chase</i> ou <i>Incremental Redundancy</i> (IR)	<i>Asynchronous Incremental Redundancy</i> (AIR)
<i>Spreading Factor</i> (SF)	SF=16 usando códigos de canalização UTRA OVFS	Código <i>Walsh</i> de comprimento 32
Aproximação do Canal de Controle	Dedicated Channel apontando para Shared Channel	Common Control Channel

Fonte: (<http://www.umtsworld.com/>, consulta em 29/01/2008).

Considerando-se os padrões com suas respectivas aplicações, características de área de cobertura para uma célula ou AP e frequência de operação, abaixo são apresentadas algumas tecnologias. Enfim, os padrões seguem em busca de taxas de transmissão cada vez mais altas e acesso a serviços IP, o que acarreta nos estudos da 4ª Geração de telefonia celular (4G), que vislumbra a possibilidade de acesso entre 100Mbps (em movimento) e 1Gbps (em repouso).

Tabela 22 – Comparação entre variadas tecnologias de transmissão sem fio.

Tecnologia	Padrão	Aplicação	Range de Cobertura (m)	Frequência (GHz)
UWB	802.15.3 ^a	WPAN	10	705
Wi-Fi	802.11 a	WLAN	100	5
Wi-Fi	802.11b	WLAN	100	2,4
Wi-Fi	802.11g,n	WLAN	100	4,4
Wi-Max	802.16d	WMAN	6400 a 9600	11
Wi-Max	802.16e	Mobile/WMAN	1600 a 4800	2 a 6
WCDMA	3G	WWAN	1600 a 8000	1,8, 1,9 ou 2,1
CDMA2000	3G	WWAN	1600 a 8000	0,4, 0,8 ou 0,9
1xEV-DO	3G	WWAN	1600 a 8000	1,7, 1,8, 1,9 ou 2,1
MBWA	802.20	WWAN	4000 a 12000	3,5

Fonte: (<http://www.citel.oas.org/>, consulta em 29/01/2008).

3. Conceitos e Características de Segurança

A segurança da informação é composta por quatro conceitos fundamentais: confidencialidade, integridade, disponibilidade e legitimidade [MACH 00].

A confidencialidade é a garantia de que a informação não seja revelada a pessoas não autorizadas. A integridade é a garantia de consistência da informação, prevenindo-se a alteração, criação ou destruição de informação por terceiros não autorizados. A disponibilidade é a garantia de que os usuários legítimos não sejam impedidos indevidamente de acessarem informações e recursos do sistema. A legitimidade, por sua vez, é a garantia de que os recursos não sejam utilizados por pessoas não autorizadas ou usados de forma não autorizada. Envolve-se também neste contexto, a política de segurança, que delimita o conjunto de regras e procedimentos aplicáveis a todas as atividades relacionadas com a segurança de um sistema de informação dentro de um determinado domínio.

3.1. Mecanismos de Segurança

Neste capítulo serão abordadas as técnicas de segurança relacionadas aos sistemas celulares do ETSI e 3GPP que foram explicados no capítulo anterior. Nas seções a seguir serão descritas as técnicas e algoritmos utilizados na autenticação de usuários e criptografia de mensagens.

3.1.1. Segurança no GSM

O GSM é baseado no sistema criptográfico de chave simétrica, utilizando como processo de autenticação um mecanismo de desafio-resposta. A característica de autenticação é entendida, na estrutura do GSM, como um operador para identificar a identidade de um usuário, tornando praticamente impossível para alguém fazer chamadas fraudulentas, ou seja, se mascarar como um usuário legítimo da rede.

A confidencialidade protege o tráfego de voz e dados, além de dados sensíveis de sinalização (como números de telefones discados), contra ataques de escuta nos pacotes enviados pelos canais de RF. A anonimidade é uma característica que foi desenvolvida para proteger o usuário, de alguém que conhece o *International Mobile Subscriber Identity* (IMSI), contra o uso desta informação para traçar a localização do usuário ou identificar chamadas feitas pelo mesmo. Além do IMSI, é usado também o *Temporary Mobile Subscriber Identity* (TMSI) que é uma identidade temporária com formato de 32bits. A TMSI é mudada toda vez que é enviada sob um canal encriptado, sendo, portanto, uma variável do sistema.

No processo de autenticação existe uma chave K_i que se encontra na MS e no conjunto HLR/AuC. Para inicializar o processo, a rede confere se a MS é autêntica, através do fornecimento de um desafio que é calculado pela UE usando sua chave K_i . A partir daí uma cadeia de números randômicos (*Random number* (RAND)) é enviada ao móvel, que, por sua vez, transfere o parâmetro ao SIM *card* com o objetivo de executar uma *One-Way Function* (OWF) A3 (algoritmo usado na autenticação do usuário) com as entradas K_i e RAND. A saída é um valor resposta de 32bits, denominado *Signed Response* (SRES), que é enviado à CN para verificação do SRES.

Da mesma forma, uma chave temporária de sessão é estabelecida (K_c) como saída de outra OWF baseada em outro algoritmo (A8), utilizando os mesmos parâmetros K_i e RAND na entrada. Esta chave é utilizada para encriptar as chamadas na interface aérea. Tripletos (RAND, *Expected Response* (XRES) e K_c) de autenticação são enviados para o elemento *Serving Network* (SN) formado pelo conjunto MSC/VLR ou SGSN/VLR (no caso do GPRS), como mostra a figura abaixo. Se $XRES = SRES$, então o sistema prossegue com o processo de segurança, no qual a BTS envia o TMSI e a chave de sessão sobre o canal encriptado.

Figura 44. Identificação e autenticação do usuário no GSM.
(Fonte: [NIEM 03], pg. 10)

A cifragem dos dados é feita para a travessia dos dados entre a MS e BTS, utilizando a chave K_c descrita anteriormente. O algoritmo utilizado para a encriptação é chamado de A5 (sendo uma OWF), a especificação interna do algoritmo é confidencial, possibilitando apenas a visão geral ilustrada na Figura 45.

Figura 45. Uso do A5 como gerador de chaves.
(Fonte: [NIEM 03], pg. 10)

A Figura 46 mostra a sequência e interações entre os algoritmos A3, A5 e A8.

Figura 46. Algoritmos usados na autenticação e encriptação do GSM.
(Fonte: [HUJI 08])

3.1.2. Segurança no GPRS

No GPRS, o algoritmo A5 de cifragem do GSM é substituído por outra cadeia de cifras, denominada *GPRS Encryption Algorithm* (GEA). O que muda é o ponto de troca de informações, que agora passa a ser entre a MS e SGSN. A cifragem passa a ser de alto nível, como mostra a figura a seguir. No *Circuit Switched* GSM (CS-GSM) a encriptação dos dados é feita na camada PHY, enquanto que no GPRS é na camada LLC.

Figura 47. Identificação do IMSI.
(Fonte: [T102 00])

No GPRS é utilizada uma identidade temporária denominada *Packet TMSI* (P-TMSI) proveniente do SGSN.

3.1.3. Segurança no UMTS

As características de segurança de acesso estão especificadas no TS 33.102, que está incluído na primeira maior versão das especificações do 3GPP, conhecida como *release 99*.

A segurança do UMTS foi construída sobre o sucesso do GSM, ou seja, mantendo as características de segurança que provaram ser necessárias e robustas ao sistema. Assim como no GSM, um *smart card* é usado para armazenar todos os dados de identificação e segurança que o assinante necessita para efetuar e receber chamadas, denominado *Universal Subscriber Identity Module* (USIM).

O UMTS provém autenticação mútua entre o assinante UMTS (representado pelo USIM) e a rede (SN). Uma das mais importantes características do UMTS é a inserção do

mecanismo de integridade nos dados de sinalização, pois permite proteção contra ataques de falsas *Base Stations* (BS) ou *Node-B*. Este mecanismo protege o UE, devido à autenticação da sinalização de mensagens de requisição da rede (utilizada na configuração de uma comunicação com a própria UE), ou seja, autenticação mútua.

A confidencialidade é alcançada através do uso de algoritmos de cifragem de dados de tráfego (além de confidencialidade para a identidade do usuário), com o uso de um mecanismo de identidade temporária (TMSI), fazendo com que o IMSI não possa ser espionado.

3.1.3.1. Troca de Mensagens no UMTS

Figura 48. Troca de informações de segurança no UMTS (camadas internas).
(Fonte: [NIEM 03], pg. 58)

As mensagens de dados e sinalização são trocadas entre o UE e o conjunto SGSN/VLR através de enlaces de radiofrequência (UE ↔ *Node-B* e UE ↔ RNC) e enlaces cabeados (BS ↔ RNC e RNC ↔ SGSN/VLR), conforme a Figura 48. As mensagens de sinalização são trocadas entre todas as quatro camadas de sinalização RRC, RLC, MAC e PHY. Através da figura, observa-se que o mecanismo de integridade troca mensagens de sinalização no nível do RRC e o de cifragem da sinalização (entre UE e RNC), nas camadas RLC e MAC. Também, pode-se visualizar o transporte da *Cipher Key* (CK) e *Integrity Key* (IK), através do uso de controle de sinalização pelo *Signalling Connection Control Part* (SCCP) e tecnologia de transmissão de dados *Asynchronous Transfer Mode/Internet Protocol* (ATM/IP).

Através da Figura 49, visualiza-se melhor dos tipos de informações que são trocadas na rede UMTS, destinadas à proteção dos dados (criptação e integridade no sentido UE ↔ RNC) e autenticação mútua (USIM ↔ SGSN/VLR e HLR/AuC ↔ USIM).

Figura 49. Troca de informações de segurança no UMTS (visão geral).
(Fonte: [PÜTZ 01], pg. 2)

O HLR é o dispositivo da rede que armazena os dados do ambiente onde o UE está registrado (política de segurança) e o AuC é parte da rede onde são gerados os números de sequência nas mensagens de autenticação, além dos números randômicos para serem correlacionados com a chave secreta K, que é compartilhada entre o UE e a *Home Network* (HN), formada pelo conjunto HLR/AuC.

3.1.3.2. Autenticação – AKA

Figura 50. Compartilhamento da chave secreta K (de 128bits) entre HN e HE.

O esquema apresentado na Figura 50 fornece o conceito e a dinâmica de funcionamento do UMTS *Authentication and Key Agreement* (AKA). São realizadas cinco funções (f_1 , f_2 , f_3 , f_4 e f_5) no HN. O *Sequence number* (SQN), com comprimento de 48bits, é um número aleatório que, assim como o RAND, é gerado pelo AuC.

No início da troca de informações entre o *Home Environment* (HE), que é formado pelo UE/USIM, e o AuC, é gerado um SQN recente e um não previsível desafio RAND (com comprimento de 128bits). As funções f_1 e f_2 correspondem às funções de autenticação de mensagens e as funções f_3 , f_4 e f_5 são funções de geração de chaves (conforme Tabela 23). A chave secreta K que é compartilhada entre o HE e o AuC é composta por 128bits.

Tabela 23 – Simbologia utilizada na segurança do UMTS.

Símbolos	Significado
$\parallel$	Concatenação.
$\oplus$	Ou-Exclusivo (EX-OR).
f_1	Função de autenticação de mensagem usada para gerar o MAC.
f_1^*	Função de autenticação de mensagem usada para gerar o MAC-S.
f_2	Função de autenticação de mensagem usada para gerar o RES and XRES.
f_3	Função de geração de chave usada para gerar o CK.
f_4	Função de geração de chave usada para gerar o IK.
f_5	Função de geração de chave usada para gerar o AK nos procedimentos normais.
f_5^*	Função de geração de chave usada para gerar o AK nos procedimentos de re-sincronização.
K	Longo termo de chave secreta compartilhada entre o USIM e o AuC.

Para cada usuário, o HE/AuC gera um SQN_{HE} . Subseqüentemente, os valores são computados pelo HE/AuC usando a chave específica de cada usuário K e um operador específico denominado *Authentication Management Field* (AMF), conforme as formulações abaixo:

- Um *Message Authentication Code* (MAC): $MAC = f_1(K)(SQN \parallel RAND \parallel AMF)$, onde f_1 é uma função da mensagem de autenticação de comprimento 64bits;
- Um *Expected Response* (XRES): $XRES = f_2(K)(RAND)$, onde f_2 é uma função da mensagem de autenticação de comprimento variável entre 4 e 16 octetos (possibilidade truncada);
- Uma *Cipher Key* (CK): $CK = f_3(K)(RAND)$, onde f_3 é uma função de geração de chaves de comprimento 128bits;
- Uma *Integrity Key* (IK): $IK = f_4(K)(RAND)$, onde f_4 é uma função de geração de chaves de comprimento 128bits;
- Uma *Anonymity Key* (AK): $AK = f_5(K)(RAND)$, onde f_5 é uma função de geração de chaves de comprimento 48bits;

- Construção do *Authentication Token* (AUTN): $AUTN = SQN \oplus AK \parallel AMF \parallel MAC$.

O AMF serve para definir as opções de operador específico nos processos de autenticação, como, por exemplo, o uso de múltiplos algoritmos de autenticação ou uma limitação do tempo de vida da chave.

Figura 51. Visão geral do AKA no UMTS.
(Fonte: [BOMA 02], pg. 194)

A Figura 51 apresenta de forma mais simples a troca de mensagens AKA entre os dispositivos da rede UMTS. No processo, depois da requisição de uma autenticação de dados, o HN gera uma matriz ordenada de n *Authentication Vector* (AV). Cada AV consiste de cinco componentes (que podem ser chamados de “quintetos” UMTS, em analogia aos “tripletos” do GSM): RAND, XRES, CK, IK e AUTN.

Esta matriz de n AV é enviada do HN para o SN. Na autenticação o SN seleciona primeiro o próximo vetor de autenticação (i -ésimo) da matriz e envia os parâmetros $RAND_i$ e $AUTN_i$ para o usuário. O USIM checa se o $AUTN_i$ pode ser aceito e, no caso de aceitação, produz uma resposta RES_i , que é enviada de volta ao SN. O $AUTN_i$ somente pode ser aceito se o SQN contido neste token é recente. O USIM também armazena o CK_i e o IK_i . O SN compara o RES_i recebido com o $XRES_i$, e se forem iguais, o SN considera a troca de autenticação completada com sucesso. As chaves estabelecidas CK_i e IK_i são então transferidas para o UE pelo VLR (ou SGSN) para o RNC. As chaves são então utilizadas para as funções de encriptação e integridade.

O UE envia uma mensagem de requisição ao SN. O SN se comunica com o AuC. O

AuC fornece o SQN e o RAND, que são enviados ao UE. O UE, com os dados recebidos, verifica o MAC, e se $MAC = XMAC$, verifica o SQN no USIM. Neste ponto o desafio da rede foi autenticado e o UE envia o RES ao SN, que por sua vez verifica se $RES = XRES$. Caso sejam iguais, a autenticação se completa. Se MAC ou RES não estiverem de acordo com o esperado, o processo é reiniciado. Se SQN não for recente, é efetuada re-sincronização com o AuC (processo chamado de *Authentication Token in re-Synchronization (AUTS)*). Se o SQN no AuC estiver correto, o processo é reiniciado, caso contrário o MAC é verificado pelo SN. Estando o MAC irregular, o processo é reiniciado, porém, estando correto, o SQN é reinicializado no AuC, e então, o processo é recommçado.

Figura 52. Segurança de acesso no UMTS.
(Fonte: [NIEM 03], pg. 64)

Na Figura 52 visualizam-se as interconexões entre os dispositivos de rede e seus mecanismos de encriptação e integridade. No ambiente AuC são gerados a chave secreta K e o SQN_{AuC} , que são encapsulados nos algoritmos AKA através das funções descritas anteriormente através da Tabela 23, gerando os AV que são encaminhados aos componentes da rede (VLR para rede comutada a circuito e SGSN para rede comutada a pacotes), os quais repassam os dados ao RNC através de uma comunicação segura. O RNC seleciona o RAND e

o AUTN para o ME usando algoritmos f8 (criptação) e f9 (integridade). O UE, também utilizando tais algoritmos, fornece confidencialidade e integridade na comunicação. O USIM, através de uma interface interna do UE, utiliza o algoritmo AKA para gerar o RES e enviar ao VLR/SGSN, além de gerar o SQN_{USIM}.

3.1.3.3. Função de Encriptação – f8

A Figura 53 ilustra o uso do algoritmo de encriptação f8 para codificar o texto não criptografado aplicando uma operação ou-exclusivo, ou seja, uma adição binária bit-a-bit do texto não criptografado com a cadeia de chaves, gerando um texto criptografado. O texto não criptografado pode ser novamente obtido através do uso da mesma operação no receptor. Os parâmetros de entrada do f8 são descritos na Tabela 24.

Figura 53. Encriptação dos dados no UMTS.
(Fonte: [BOMA 02], pg. 197)

Tabela 24 – Parâmetros de f8.

Parâmetro	Quantidade de Bits	Descrição
COUNT-C	32	Quadro dependente de entrada (COUNT 0 a COUNT 31).
BEARER	5	Identidade do portador (BEARER 0 a BEARER 4).
DIRECTION	1	Direção de transmissão (DIRECTION 0).
LENGTH	x18	N.º de bits a serem encriptados/decriptados (de 1 a 20000).
CK	128	Chave de confidencialidade (CK 0 a CK 127).

Baseando-se nos parâmetros de entrada, o algoritmo gera uma cadeia de chaves de bloco *keystream* (KS) usada para codificar o texto não criptografado. O texto, já criptografado, pode ser enviado ao receptor através do enlace de comunicação. O parâmetro de entrada LENGTH afeta somente o comprimento do bloco KS e não os bits internos do bloco.

3.1.3.4. Função de Integridade – f9

A Figura 54 ilustra o uso do algoritmo de integridade f9 para efetuar a integridade de

dados de uma mensagem RRC. Os parâmetros de entrada do f_9 são descritos na Tabela 25.

Tabela 25 – Parâmetros de f_9 .

Parâmetro	Quantidade de Bits	Descrição
COUNT-I	32	Quadro dependente de entrada (COUNT 0 a COUNT 31).
MESSAGE	LENHT	Entrada de cadeia de bits (x19).
DIRECTION	1	Direção de transmissão (DIRECTION 0).
FRESH	32	N.º aleatório (FRESH 0 a FRESH 31).
IK	128	Chave de integridade (IK 0 a IK 127).

Figura 54. Integridade dos dados no UMTS.
(Fonte: [BOMA 02], pg. 196)

Baseando-se nos parâmetros de entrada, o transmissor computa os 32 bits MAC para integridade de dados (MAC-I) usando o algoritmo f_9 . O MAC-I é então adicionado à mensagem RRC, que é enviada sobre um enlace de acesso via RF. O receptor calcula o *Expected* MAC-I (XMAC-I) na mensagem recebida, da mesma forma que o transmissor, verificando a integridade dos dados da mensagem através da comparação $\text{MAC-I} = \text{XMAC-I}$.

A característica de integridade também fornece a autenticação de dados da origem, permitindo que o sistema não execute o AKA toda vez que uma conexão é estabelecida.

3.1.3.5. Kernel Algoritmo KASUMI

O algoritmo KASUMI [T202 05] baseia-se em um bloco de cifragem que produz uma saída de 64bits para dados de entrada de 64bits, sob o controle de uma chave de 128bits. Nele é feita a decomposição do número em funções (FL, FO e FI) que são usadas em conjunto com sub-chaves associadas em uma estrutura de Feistel, compreendendo um número de *rounds* = 8 (e *rounds* com *rounds* para algumas sub-funções). Específicas instâncias das funções e/ou chaves são representadas por $\text{XX}_{i,j}$, onde i é o número do *round* de saída e j é o número do *round* de entrada.

A Figura 55 é apresenta o algoritmo KASUMI e suas funções: (a) KASUMI; (b) função FO_i ; (c) função $\text{FI}_{i,j}$; e (d) função FL_i . A estrutura do KASUMI é dividida em partes, onde as inversões de função (para o ou-exclusivo) são chamadas de funções f_i e são

diferenciadas dependendo do *round*, ou seja, para *rounds* ímpares (1, 3, 5 e 7) ou pares (2, 4, 6 e 8).

Figura 55. Algoritmo KASUMI.
(Fonte: [NIEM 03], pg. 180)

As funções FL fazem uso das simples operações de rotação circular (ROL) de um bloco de dados, ou $(\cap)$ e $(\cup)$ entre dois blocos de dados. A sub-chave KL_i de 32bits é dividida em duas sub-chaves para efetuar operações com as duas metades dos dados de entrada (de 16bits cada). Os 32bits de saída da função FL são definidos como L' || R', onde: $R' = R \oplus \text{ROL}(L \cap \text{KL}_{i,1})$ e $L' = L \oplus \text{ROL}(R' \cup \text{KL}_{i,2})$.

As funções FO_i trabalham com dois conjuntos de sub-chave, KO_i e KI_i (ambas com 48bits). As sub-chaves KO_i e KI_i são subdivididas em três sub-chaves de 16bits, para operar nos três *rounds* relacionados com as funções FI. A saída da função FO_i é um bloco de dados de 32bits L₃ || R₃.

Cada função FI_{i,j} usa duas S-boxes: S7 que mapeia 7bits de entrada para 7bits de saída e S9 que mapeia 9bits de entrada para 9bits de saída. As funções FI utilizam, também, as

funções adicionais *Zero-Extend* (ZE) que pega 7bits e converte para 9bits, com o acréscimo de 2bits com valor zero no lado mais significativo da *string* e o *Truncate* (TR) que faz o inverso (converte 9bits em 7bits, descartando os 2bits mais significativos da *string*). A saída da função $FI_{i,j}$ é um bloco de dados de 16bits $L4 \parallel R4$.

3.1.3.6. *f8 com KASUMI*

A principal tarefa do algoritmo f8 foi a elaboração de uma cadeia de cifras fora da cifra de KASUMI. Uma combinação de *Output Feedback* (OFB) e um modo contador foram usados para a proteção do KASUMI contra ataques a textos não codificados, além de proteção contra ataques de colisão. Para prevenção aos referidos ataques, o *Initialization Vector* (IV) é encriptado com uma chave diferente $CK' = CK \oplus KM$, onde KM significa *Key Modifier*.

O algoritmo f8 faz uso da chave KM que é uma constante igual ao octeto 0x55 = 01010101 repetido por 16 vezes. Uma única operação do KASUMI é aplicada ao registrador A, usando uma versão modificada de CK, o CK' que é armazenado no registrador.

A Figura 56 ilustra a passagem dos blocos de encriptação com uma função de contagem de blocos (BLKCNT) de 64bits que vai de 0 a n-1 blocos.

Figura 56. f8 com uso do *kernel* KASUMI.
(Fonte: [NIEM 03], pg. 150)

3.1.3.7. *f9 com KASUMI*

Figura 57. f9 com uso do *kernel* KASUMI.
(Fonte: [NIEM 03], pg. 164)

O algoritmo f9 é uma *Cipher Block Chain – Message Authentication Code* (CBC-MAC) que utiliza o KASUMI como bloco de encriptação subjacente [T201 05]. No término da codificação é gerada uma chave diferente $IK' = IK \oplus KM$ para ser operada juntamente com o KASUMI, conforme a Figura 57.

3.1.3.8. Criptografia AES

O *National Institute of Standards and Technology* (NIST) que substituiu a *National Security Agency* (NSA), promoveu uma competição com o intuito de produzir um algoritmo para substituir o *Data Encryption Standard* (DES), sendo denominado *Advanced Encryption Standard* (AES) [DAEM 02].

O algoritmo deveria atender aos requisitos de: definição pública, cifra simétrica de bloco, projetado para que o tamanho da chave possa ser expandida, implementável tanto em HW quanto em SW e disponibilizado livremente ou de acordo com os termos do *American National Standards Institute* (ANSI). O algoritmo selecionado pelo NIST foi o Rijndael [DAEM 02].

O Rijndael foi desenvolvido por Joan Daemen and Vincent Rijmen. O algoritmo tem um número variável de *rounds* em função da chave (sem contar um último *round* que é executado no término da cifragem e fica omitido), conforme segue abaixo:

- 9 *rounds* se o tamanho do bloco ou da chave for de 128bits;
- 11 *rounds* se o tamanho do bloco ou da chave for de 192bits;
- 13 *rounds* se o tamanho bloco ou da chave for de 256bits.

Características do Rijndael:

- Os bytes das chaves e dos blocos são organizados em forma de matrizes;
- Tem três tamanhos de chaves (16, 24 e 32bytes) e três tamanhos de blocos (16, 24 e 32bytes);
- Tem uma função de passo F que é aplicada 10, 12 ou 14 vezes;
- Possui cifras iterativas;
- Trabalha sobre aritmética de corpo finito $GF(2^8)$.

Executam-se quatro operações no Rijndael, conforme a Figura 58, para as seguintes finalidades:

- *ByteSub*: não linearidade;
- *ShiftRow*: difusão entre as colunas de dados;

- *MixColumn*: difusão dentro de cada coluna;
- *AddRoundKey*: aplicação da chave.

A dinâmica de geração da criptografia dos dados pode ser vista através de um bloco de 128bits que fica particionado em 16 octetos (representados por S), conforme Figura 58. Primeiro uma substituição é aplicada a cada byte (octeto). Em seguida uma permutação é aplicada aos 16 octetos. Uma sub-chave de 128bits, gerada por uma rotina de expansão, é adicionada bit-a-bit ao resultado da permutação. A chave K_i do ciclo n_i é obtida da chave da rotina de expansão utilizando a sub-chave K_{i-1} do ciclo n_{i-1} sendo K_0 a chave secreta. Os 16bytes da chave K_{i-1} são processados por partes, ou seja, de 4 em 4.

Figura 58. Estrutura do algoritmo Rijndael (AES).
(Fonte: [ROSA 02])

3.1.3.9. Algoritmo MILENAGE

O AES – Rijndael foi um bom exemplo de *kernel* que atendeu aos requerimentos do MILENAGE [T205 05], que são: comprimento dos blocos de entrada/saída e comprimento de chave, todos com 128bits.

O conjunto de algoritmos MILENAGE faz uso de funções de encriptação de blocos, pegando 128bits de entrada e 128bits de chave, retornando uma saída de 128bits.

Se uma operadora escolher o MILENAGE como seu algoritmo AKA, ela pode customizá-lo por um operador variante de configuração de características do algoritmo (*Operator* (OP) de 128bits). Para proteger o OP contra revelação, o mesmo deve ser encriptado *offline* com a chave específica K do usuário e somente o texto cifrado OP_C deve ser armazenado no USIM.

A Figura 58 mostra o algoritmo MILENAGE e suas iterações internas para a encriptação, onde E_K representa o algoritmo Rijndael usando a chave K. Além do OP, o MILENAGE usa as constantes r_1, r_2, r_3, r_4 e r_5 (que são números inteiros que determinam a quantidade de variáveis a serem roteadas ciclicamente) e c_1, c_2, c_3, c_4 e c_5 (que são constantes de 128bits originadas pela álgebra booleana EX-OR ($\oplus$) em variáveis intermediárias), que podem ser modificadas por um operador e são escolhidas em pares diferentes (c_i, r_i).

Assume-se paridade par ou ímpar para a sequência de estágios. No caso de assumirmos o c_1 com paridade par e c_2 a c_5 com paridade ímpar, o OP_C na entrada do segundo estágio tem paridade par. Sendo que:

$$OP_C = OP \oplus E_K(OP) \quad (9)$$

Então, a entrada para a encriptação do segundo nível tem a mesma paridade:

$$TEMP = E_K(RAND \oplus OP_C) \quad (10)$$

desde que OP_C, c_1 e:

$$IN_1 = SQN \parallel AMF \parallel SQN \parallel AMF \quad (11)$$

tenham paridade par (SQN com 48bits e AMF com 16bits).

De outra forma, se for assumido o OP_C com paridade ímpar, a entrada para o segundo estágio terá paridade oposta e os dados de encriptação de todos os outros estágios terão as mesmas paridades $TEMP = E_K(RAND \oplus OP_C)$.

As funções f_1 e f_1^* são construídas como um padrão CBC-MAC com os dois blocos de entrada $RAND \oplus OP_C$ e $rot(IN_1 \oplus OP_C, r_1)$. Todas as outras funções derivam valores diferentes de RAND sob o controle da chave específica K do usuário e do operador variante

de configuração de características do algoritmo OP, gerando as saídas mostradas a seguir:

$$\begin{aligned}
 \text{OUT}_1 &= E_K[\text{TEMP} \oplus \text{rot}(\text{IN}_1 \oplus \text{OP}_C, r_1) \oplus c_1] \oplus \text{OP}_C \\
 \text{OUT}_2 &= E_K[\text{rot}(\text{TEMP} \oplus \text{OP}_C, r_2) \oplus c_2] \oplus \text{OP}_C \\
 \text{OUT}_3 &= E_K[\text{rot}(\text{TEMP} \oplus \text{OP}_C, r_3) \oplus c_3] \oplus \text{OP}_C \\
 \text{OUT}_4 &= E_K[\text{rot}(\text{TEMP} \oplus \text{OP}_C, r_4) \oplus c_4] \oplus \text{OP}_C \\
 \text{OUT}_5 &= E_K[\text{rot}(\text{TEMP} \oplus \text{OP}_C, r_5) \oplus c_5] \oplus \text{OP}_C
 \end{aligned} \tag{12}$$

Neste caso, com os valores de saída mostrados acima, temos uma estrutura de autenticação como visualizada através da figura abaixo.

Figura 59. Algoritmo MILENAGE com o uso do *kernel* AES Rijndael.
(Fonte: [NIEM 03], pg. 219)

3.1.4. Considerações de Segurança

As funções e algoritmos apresentados formam uma base sólida para a utilização dos serviços a que se dispõe implementar o UMTS, pois a inserção de mecanismos de segurança voltados para a integridade, autenticidade e confiabilidade dos dados de sinalização e usuário, através de encriptação de chaves simétricas, são importantes principalmente devido ao fato de serem enviados entre o equipamento do usuário e a rede via canais de RF.

O mecanismo de troca de chaves foi analisado em [SANT 02] através de um método de análise formal de protocolos de segurança, onde constatou-se que o UMTS fornece os serviços de segurança desejados: autenticação mútua, distribuição de chave de sessão, sigilo da identidade e sigilo dos dados do assinante. Os mecanismos de segurança trabalham no esquema CBC, provendo uma encriptação de blocos em cadeia sequencial e utilizando itens randômicos ou outros dispositivos, gerando certa dificuldade para a fraude das informações. As funções f8 (encriptação) e f9 (integridade) utilizam o *kernel* KASUMI, fornecendo uma chave favorável contra métodos de ataque poderosos que tentam derivar informação sobre a

pesada estrutura de sub-chaves internas.

Através de análises da Força Tarefa do ETSI, concluiu-se que o algoritmo MILENAGE contempla os requerimentos: nível de segurança e baixos saltos de complexidade que podem ser alocados por possíveis ataques, sem causar qualquer tipo de ameaça ao algoritmo. No MILENAGE, com o uso do parâmetro OP_C sendo gravado no USIM, através de uma OWF em que o caminho ao OP não pode ser refeito, utilizando-se para isto, números existentes nos cartões USIM válidos, protegendo-se o sistema contra a produção não autorizada de USIM.

A principal força criptográfica do MILENAGE está no *kernel* de encriptação de blocos, ou seja, o AES, que é um padrão de encriptação atual e aberto, portanto, com muitas cripto-análises realizadas, como, por exemplo, em [FERG 01] e [DOBB 05]. Apesar do algoritmo KASUMI ser robusto e prover a segurança com alto grau de confiabilidade na encriptação e integridade dos dados, o algoritmo Rijndael fornece a mesma robustez, porém, com padronização de 128bits de blocos e chave, rotação dos dados de entrada, diferenciação no número de *rounds* executados (9 *rounds* para 128bits), cifras iterativas e aritmética sobre corpo finito $GF(2^8)$.

4. Modelagem dos Mecanismos de Segurança

Para a realização de um estudo coerente sobre o desempenho relacionado à segurança em redes UMTS, foi necessário implementar cenários de simulação. Para tal, foi selecionado o software OPNET Modeler¹, pois, conforme análise realizada em [LUCI 03], o OPNET fornece as ferramentas necessárias para a implementação de cenários e oferece base para simulações de eventos discretos.

Pode-se inserir um cenário UMTS no OPNET, devendo-se atentar às características do sistema para que sejam representadas e simuladas situações próximas ao ambiente real. Neste caso o software dá suporte aos serviços e características de implementação da rede, através de módulos e processos já desenvolvidos pelo fabricante e, a partir dos quais (e com o uso dos mesmos) existe a possibilidade de conexão aos objetos e processos criados neste trabalho.

Na simulação, foi utilizado o software OPNET [OPNT 07], o qual possibilitou as interações entre os dispositivos da rede UMTS e a inclusão de parâmetros de segurança conforme apontados nos tópicos de modelagem dos mecanismos de segurança, facilitando a análise dos dados obtidos em simulações através de interfaces gráficas e caminhos para visualização de desempenho das técnicas de segurança utilizadas.

Foi adotada metodologia de pesquisa que visa a padronizar e definir critérios de coleta e análise de dados acerca de redes UMTS, conforme descrito a seguir:

- Pesquisas em entidades de padronização (protocolos, normas, regulamentos, recomendações, etc.);
- Estudo dos mecanismos de segurança do GSM, da estrutura de segurança do UMTS e das melhorias do UMTS em relação ao GSM;
- Estudo de situações de ataque e ameaça à rede UMTS;
- Estudo de situações de segurança através do uso de software de simulação;
- Simulação de carga na rede UMTS através de variações do número de dispositivos conectados à rede nos cenários de simulação;
- Diagnóstico de possíveis efeitos dos mecanismos de segurança no desempenho dos sistemas.

Com o intuito de analisar o desempenho de redes UMTS relacionado aos padrões de segurança apresentados, foi utilizado o software para as seguintes situações:

- Transição de pacotes pela rede, conforme o tipo de tráfego gerado;

¹ O software OPNET *Modeler* foi providenciado sob programas universitários. Apresenta uma diversidade de ferramentas de modelagem de eventos discretos. Para mais informações sobre a utilização, disponibilidade e configuração, recomenda-se o acesso ao site: <http://www.opnet.com/>.

- Verificação de atrasos nos nós e na rede em geral;
- Verificação da carga gerada pelos dispositivos de uma mesma PLMN;
- Análise dimensional do ponto de vista da variação do tamanho de chaves de criptografia;
- Análise de níveis de segurança relacionados ao desempenho (QoS) do ponto de vista do usuário.

No software foram feitas as seguintes configurações, que serão descritas com mais detalhes no próximo capítulo:

- Configuração das interfaces entre os dispositivos que compõem a rede UMTS, descritos na seção 2.7;
- Configuração dos módulos referentes às trocas de mensagens de sinalização e dados entre os dispositivos da rede;
- Criação de máquina de estados (*Finite State Machine* (FSM)) nas interfaces internas do dispositivo *Network SubSystem* (NSS), que englobam as tarefas relacionadas à pesquisa de parâmetros de segurança (que foram descritos na seção 3.1) através de interações entre os elementos internos *Mobile Switching Center* (MSC), *Home Location Register* (HLR), *Equipment Identity Register* (EIR) e *Authentication Center* (AuC). Este dispositivo faz a interface e encaminhamento de sinalização;
- Configuração de segurança (*handshake*) entre os nós e, também, no sistema;
- Configuração da distribuição de pacotes entre os nós.

Com relação à medição de energia dispendida pelos dispositivos móveis, foram gerados gráficos para os cenários simulados que representam os níveis de energia de acordo com a variação dos parâmetros de segurança.

A capacidade máxima de UE para a célula está relacionada com a potência que o *Node-B* pode tratar, segundo a capacidade de canais, que é dada por:

$$C \leq \frac{1}{2} \log_2 \left(1 + \frac{2P}{2} \right) = \frac{1}{2} \log_2 (1 + P) \quad (13)$$

onde C representa a capacidade de canais (em bits) e P a potência (em Watts).

Sendo assim, a máxima capacidade do sistema é limitada pela quantidade de canais, pelas interfaces físicas e pelo número de UE presentes na mesma célula, utilizando ao mesmo tempo os canais disponíveis na área de cobertura.

A Figura 60 apresenta uma visão geral do cenário a ser simulado, no qual, as linhas vermelhas em destaque representam as interações dos elementos que compõem a rede. A linha contínua representa a conexão lógica de voz entre dois UE e a linha tracejada refere-se à

troca de sinalização entre os elementos do NSS e da UTRAN.

Figura 60. Visão geral da comunicação e troca de sinalização entre UTRAN e NSS.

Para o tempo de resposta às requisições de acesso *Web* foram configurados os acessos ao servidor *Web* nos diversos cenários que serão descritos no próximo capítulo, sendo definidos para tal, dois tipos de acessos:

- Acessos a páginas: que tem tamanho entre 1,5kbytes e 3kbytes, sendo formada por um objeto de 1kbyte e uma imagem que pode variar entre 500 e 2000bytes; e
- Acessos a objetos: objetos com tamanho fixo de 1kbyte.

Os experimentos foram realizados em ambientes de simulação, com configurações de uso real nas interfaces físicas e aéreas. Os dispositivos móveis encontram-se parados nos cenários, ou seja, não há deslocamento dos dispositivos móveis dentro da área de cobertura do *Node-B* (ou da célula).

Os dispositivos móveis ou *User Equipments* (UE) foram distribuídos de forma aleatória na célula. Foram definidos dois tipos de UE no *profile_definition*:

- UE vermelhos: que têm as funções de conversação com perfil *Voice User* e de acesso a páginas *Web* contidas no *web_server* com perfil *Web User*, ambos definidos na caixa de configuração *application_definition*; e

- UE pretos: que têm a função de conversação com perfil *Voice User*.

No *application_definition* foram configurados dois tipos de perfis utilizados pelos UE:

- *Voice*: trata-se de voz com característica *Pulse Code Modulation* (PCM) e uso de silêncio suprimido; e
- *Web Browsing (Heavy)*: acesso ao servidor de dados utilizando HTTP v1.1 e serviço de melhor esforço.

Baseando-se no disposto, o próximo capítulo descreve os procedimentos (incluindo configurações das caixas *profile_definition*, *application_definition* e *task_definition*) e cenários criados no ambiente de simulação, fornecendo base para as análises sobre os dispositivos e a rede como um todo, agregando valor à conclusão deste trabalho.

5. Procedimentos e Simulação

Conforme descrito na modelagem dos mecanismos de segurança, foram simulados diversos cenários utilizando a estrutura de rede UMTS, de acordo com as seguintes etapas:

- Configuração de um cenário inicial com perfil estável, constituído de elementos de rede básicos para o funcionamento de uma rede UMTS (tendo, a princípio, apenas dois equipamentos de usuário ou *User Equipment* (UE), conforme Figura 61), efetuando-se as análises descritas na modelagem dos mecanismos de segurança;
- Com base nos testes do passo anterior, efetuou-se a ampliação do número de dispositivos móveis da rede e, passo a passo, prosseguindo com a análise dos dados para cada cenário implementado;
- Foram adicionados e aplicados à rede elementos básicos de segurança e troca de mensagens nos cenários, conforme abaixo;
- Foram simulados quatro tipos de configurações de segurança em cenários: a) sem inserção de segurança; b) apenas com autenticação; c) com confidencialidade e integridade e; d) com autenticação, confidencialidade e integridade;
- Foram executadas as análises descritas no capítulo anterior sobre os elementos da rede UMTS, buscando comparações com os resultados dos cenários de rede simulados.

Figura 61. Cenário inicial da configuração da rede UMTS com dois UE no software OPNET.

A Figura 61 apresenta o cenário global, ou seja, envolvendo toda a estrutura do *Core Network* (CN) e respectivas interligações entre os meios via *links* ATM OC-3 (velocidade de transmissão de até 155,52Mbps) e PPP DS3 (velocidade de transmissão de até 44,736Mbps).

A rede é composta pelos elementos *Gateway GPRS Support Node* (GGSN), *Serving GPRS Support Node* (SGSN) e *UMTS Terrestrial Radio Access Network* (UTRAN) (que inclui o *User Equipment* (UE), *Node-B* e RNC) e *Packet Data Network* (PDN) (que inclui o Servidor HTTP). Além destes módulos, já presentes para configuração no OPNET, foi desenvolvido o dispositivo de conexão denominado *Network Subsystem* (NSS), que engloba as funcionalidades de segurança através dos dispositivos internos *Mobile Switching Center* (MSC), *Home Location Register* (HLR), *Equipment Identity Register* (EIR) e *Authentication Center* (AuC).

Neste trabalho não se levou em consideração o *Visitor Location Register* (VLR), pois o objetivo principal não é a verificação dos aspectos de *roaming* e *handoff* (sendo estas as principais funções do VLR em conexão ao MSC) e sim, o estudo dos mecanismos de segurança relacionados ao desempenho do sistema em uma mesma *Public Land Mobile Network* (PLMN).

Na Figura 62 é mostrada a parte do cenário correspondente à UTRAN. As configurações foram feitas ao nível de aplicação (dados a serem trafegados), perfil de usuário (tipo de serviços permitidos ao UE relacionado à camada de aplicação), tráfego na rede (trâmite de dados no CN e nos UE) e configurações IP (QoS e dispositivos do cenário com numeração IP).

Figura 62. Cenário mostrando a UTRAN (apresentando quatro UE, um *Node-B* e um RNC).

Acima, é apresentada a parte do cenário configurado para quatro UE. Neste caso o usuário pode comunicar-se através da rede a um servidor de informação (neste caso, um servidor contendo página de Internet) ou a outro dispositivo UE. Partindo deste cenário inicial, a seguir serão fornecidas as estruturas internas dos dispositivos apresentados e descritos nas seções anteriores.

ambientes com interface aérea (que utiliza o WCDMA FDD, descrito na seção 2.7.3) e interface cabeada até o RNC (com conexão ATM OC-3).

Figura 65. Estrutura interna do RNC.

Na Figura 65, visualiza-se a estrutura interna do dispositivo *Radio Network Controller* (RNC), na qual aparecem as interfaces ATM para conexão à *Core Network* (CN) e ao *Node-B*. Como explicado anteriormente, este é o ponto da rede que faz o controle dos canais de comunicação para tráfego de dados *Circuit Switched* (CS), *Packet Switched* (PS) e de sinalização (SS7).

Figura 66. Estrutura interna do SGSN.

Através da Figura 66, visualiza-se a estrutura interna do dispositivo *Serving GPRS Support Node* (SGSN), também com as interfaces ATM para trafegar dados provenientes e direcionados à rede de pacotes (PDN). É neste nó que existe a interface do sistema à parte da rede comutada por pacotes (PS), possibilitando a inserção de mecanismos de segurança na rede comutada a pacotes.

Figura 67. Estrutura interna do GGSN.

Na Figura 67 visualiza-se a estrutura interna do dispositivo *Gateway GPRS Support Node* (GGSN), onde se tem a interface entre a rede de pacotes (com os respectivos protocolos usados na PDN) e a rede UMTS através dos *links* ATM do CN. Lembrando que é este o dispositivo que faz a interface com a PDN e/ou outras PLMN.

Na Figura 68 é mostrada a estrutura de módulos do dispositivo desenvolvido neste trabalho, o *Network Subsystem* (NSS), assim como as interações de segurança e troca de informações de autenticação, confidencialidade e integridade. O NSS, juntamente com o SGSN, tem o objetivo de efetuar a interação dos mecanismos da CN do UMTS através das interfaces ATM, em busca da análise de desempenho descrita nos objetivos.

Neste nó são efetuadas algumas tarefas a serem executadas pelos módulos internos do NSS. Estas tarefas incluem consultas a tabelas nos módulos *Equipment Identity Register* (EIR) e *Home Location Register* (HLR) e, ainda, troca de mensagens com o *Authentication Center* (AuC). O *Mobile Switching Center* (MSC) é o controlador que faz a distribuição das

conexões entre os nós externos e os módulos internos do NSS, através de sinalização SS7.

O NSS tem interfaces físicas para comunicação direta com o SGSN e o RNC, através de *links* ATM OC-3, como pode ser visto na Figura 68. Estas interfaces estão ligadas diretamente ao MSC.

Figura 68. Estrutura interna do NSS (conjunto MSC, HLR, AuC e EIR, localizados no bloco UTRAN).

A parte referente à conexão com a rede, ou seja, *links* ATM foi obtida do próprio software de simulação, cabendo apenas o desenvolvimento da plataforma que encontra-se dentro da região denominada UTRAN da Figura 68.

No módulo MSC foi implementada a máquina de estados referente a consultas nos outros três dispositivos (EIR, HLR e AuC) e ao retorno de dados com informações sobre os UE pertencentes à *Public Land Mobile Network* (PLMN), conforme Figura 69.

Figura 69. *Finite State Machine* (FSM) do módulo MSC (estrutura interna do NSS).

Internamente, mais precisamente no *State* central (ou estado transitório, denominado *WAIT*) da figura anterior, foi designado o comportamento (ou fluxo de comandos) do nó NSS na rede, através de implementação em linguagem C.

Abaixo segue a parte relacionada à chegada de pacotes e tratamento pelo NSS.

```
if (debug_mode && (op_prg_odb_ltrace_active("umts") ||
    op_prg_odb_ltrace_active("umts_cn") ||
    op_prg_odb_ltrace_active("umts_nss")))
    ltrace_active = OPC_TRUE;
else
    ltrace_active = OPC_FALSE;
    current_time = op_sim_time();
    type = op_intrpt_type();
    ...
```

Neste passo, as informações chegam ao MSC, mais precisamente ao estado WAIT, que por sua vez, verifica se as informações estão dentro do padrão. Após, é então iniciado o processo de encaminhamento dos pacotes de sinalização e verificação de temporização do GPRS *Mobility Management* (GMM).

```

...
if (type == OPC_INTRPT_STRM)
{
    strm    = op_intrpt_strm ();
    pkptr    = op_pk_get (strm);
    pdu_iciptr = op_pk_ici_get (pkptr);
    if (pdu_iciptr == OPC_NIL)
    {
        mt = DATA;
        op_pk_format (pkptr, packet_name);
        if (strcmp (packet_name, "umts_gmm") == 0)
        {
            op_pk_nfd_access (pkptr, "cabecalho", &gtp_header_fields_ptr);
            gtp_msg = gtp_header_fields_ptr->msg_type;
            if (gtp_msg == IpC_Gtp_Create_Pdp_Context_Response)
                mt = GTP_RESPONSE;
            else if (gtp_msg == IpC_Gtp_Pdu_Notification_Request)
                mt = GTP_REQUEST;
        }
    }
    else
    {
        if (op_ici_attr_exists (pdu_iciptr, "tipo_de_mensagem"))
            op_ici_attr_get (pdu_iciptr, "tipo_de_mensagem", &mt);
        else
            op_pk_nfd_get (pkptr, "id_da_mensagem", &mt);
    }
}
...

```

Na continuação dos comandos é que se faz a verificação dos perfis e demais características dos UE. Quando ocorre a interrupção, por um evento, que no caso é a chegada de um pacote de sinalização, verifica-se o perfil que foi definido no *profile_definition*.

```

...
if (type == OPC_INTRPT_SELF)
{
    code = op_intrpt_code ();
    if ((code & TIMER_MASK) == Umts_NSS_Hold_Timer)
    {
        attached_ue_id = code & UE_ID_MASK;
        qos_type = (code & QOS_MASK) >> MASK_ID_BITS;
        subq_index = attached_ue_id * UMTSC_NUM_QOS_CLASSES + qos_type;
        if (!trace_active)
        {
            ue_profile [attached_ue_id]->imsi, qos_type);
            op_prg_oddb_print_minor (str1, OPC_NIL);
        }
        pkptr = op_subq_pk_remove (subq_index, OPC_QPOS_HEAD);
        op_ici_destroy (op_pk_ici_get (pkptr));
        op_pk_destroy (pkptr);
        if (op_subq_empty (subq_index) == OPC_FALSE)
        {
            pkptr = op_subq_pk_access (subq_index, OPC_QPOS_HEAD);
            transfer_delay = ue_profile[attached_ue_id]->pdp_profile[qos_type].qos.transfer_delay / 1000.0;
            ue_profile[attached_ue_id]->pdp_profile[qos_type].hold_time_evh =
                op_intrpt_schedule_self (op_q_insert_time (pkptr) + transfer_delay, code);
        }
    }
}
...

```

A segurança foi implementada através de inserção de chaves e configuração dos algoritmos de segurança do UMTS na caixa de configuração *task_definition*. Nesta caixa de configuração foram configurados os mecanismos de segurança utilizados pelos elementos da rede conforme discriminado na Figura 70.

Figura 70. *task_definition* com as configurações internas.

Esta caixa de configuração está presente em todos os cenários, exceto nos cenários nos quais não existe segurança (caso a).

Figura 71. *task_definition* com as configurações internas (função f8 de confidencialidade).

No *task_definition* foram configurados: a autenticação com o uso do algoritmo MILENAGE juntamente com o *kernel* AES/Rjindael (Figura 73), função de encriptação f8 (Figura 71) e de integridade f9 com *kernel* KASUMI (Figura 72).

Figura 72. *task_definition* com as configurações internas (função f9 de integridade).

Figura 73. *task_definition* com as configurações internas (função de autenticação MILENAGE com AES).

As interações e trocas de informações entre os elementos de rede foram descritos no capítulo 3 e aplicados no início do contato do UE com a rede para a autenticação e durante a conversação e transmissão de dados, para integridade e confidencialidade.

Com base nas configurações feitas nos dispositivos, foram realizados os testes nos cenários abaixo, nos quais houve variação dos níveis de segurança conforme os quatro tipos de ambientes de segurança (a, b, c e d) descritos no começo deste capítulo, para cada um dos cenários:

Figura 74. Cenário UMTS com dois UE.

Figura 75. Cenário UMTS com quatro UE.

Figura 76. Cenário UMTS com dez UE.

Figura 77. Cenário UMTS com vinte UE.

Figura 78. Cenário UMTS com quarenta UE.

Figura 79. Cenário UMTS com sessenta UE.

O servidor de informações (*web_server*, Figura 60) tem a capacidade de enviar respostas para todas as requisições que lhe chegarem, não tendo, portanto, perda de pacotes e descarte de dados.

A parte do trabalho que faz a análise sobre a rede de pacotes trata do circuito formado pelo *Packet Switched* (PS) no UMTS interligado à *Packet Data Network* (PDN) (rede da qual o servidor faz parte).

Com base nos cenários apresentados, o próximo capítulo trata sobre as análises e os resultados obtidos das exaustivas simulações realizadas, servindo como alicerce para as conclusões deste trabalho.

6. Resultados Obtidos

Diante dos cenários apresentados no capítulo anterior, foram gerados gráficos em cada um dos cenários simulados.

Foram simulados quatro tipos de configurações de segurança:

- Configuração a: cenários sem inserção de segurança;
- Configuração b: cenários com inserção de autenticação de usuário, através do algoritmo MILENAGE com o uso do *kernel* AES (Rjindael), para a variação de chaves de 128kbits, 192kbits e 256kbits;
- Configuração c: cenários com inserção de confidencialidade e integridade de dados, através das funções f8 e f9 com o uso do *kernel* KASUMI;
- Configuração d: cenários com inserção de autenticação de usuário, através do algoritmo MILENAGE com o uso do *kernel* AES (Rjindael), confidencialidade e integridade de dados, através das funções f8 e f9 com o uso do *kernel* KASUMI, para a variação de chaves de 128kbits, 192kbits e 256kbits.

Figura 80. Comparativo dos cenários de segurança com relação à potência e ao número de UE.

O gráfico da Figura 80 apresenta o nível de potência irradiada dos dispositivos UE para o *Node-B*, de acordo com o tipo e grau de segurança inserido no sistema para cada cenário. Este gráfico foi obtido da média de potência dispendida de todos os UE participantes de conversações e/ou acessos ao servidor.

O que se nota através do gráfico, é que no cenário b (autenticação), mesmo com a variação de chaves, o nível de potência irradiada continuou homogêneo até o cenário com 20 UE. Para o cenário b, ou seja, o cenário com 60 UE, o nível passou a ser praticamente o dobro para o uso de chaves de 256kbts. Com apenas 2 UE, o nível de potência atingiu o maior patamar para os cenários a (sem segurança) e c (com confidencialidade e integridade).

Os níveis de potência irradiada mais baixos foram os obtidos no cenário d (autenticação, confidencialidade e integridade) contendo 60 UE, com exceção do cenário com uso de chaves de 128kbts, o qual se aproximou do nível referente ao cenário b com chave de 256kbts. Abaixo, segue a tabela com os dados demonstrando os valores correspondentes ao gráfico da Figura 80.

Tabela 26 – Potência de transmissão média no *uplink* para UE (RLC/MAC) por canal de radiofrequência (dBm).

SEGURANÇA	CONFIGURAÇÃO	NÚMERO DE CELULARES						Média
		2	4	10	20	40	60	
Não	Sem segurança	14,51	11,39	7,65	7,45	7,35	3,87	8,70
Autenticação	MILENAGE com AES (chave 128K)	12,31	9,88	7,45	7,40	4,91	2,58	7,42
	MILENAGE com AES (chave 192K)	12,31	11,07	7,28	7,21	4,86	2,38	7,52
	MILENAGE com AES (chave 256K)	12,11	11,27	7,58	7,08	6,99	4,17	8,20
Confidencialidade e Integridade	Funções F8 e F9 com KASUMI	14,71	9,93	6,45	6,06	5,86	2,48	7,58
Confidencialidade, Integridade e Autenticação	Funções F8 e F9 com KASUMI e MILENAGE (chave 128K)	13,67	11,62	7,45	6,42	6,29	4,07	8,25
	Funções F8 e F9 com KASUMI e MILENAGE (chave 192K)	12,31	10,97	6,53	6,43	6,37	1,98	7,43
	Funções F8 e F9 com KASUMI e MILENAGE (chave 256K)	12,66	10,72	6,16	5,85	4,71	1,59	6,95
Média		13,07	10,86	7,07	6,74	5,92	2,89	7,76

Com relação aos acessos feitos ao *web_server* (HTTP), nas simulações para acesso a páginas de Internet (WWW) e requisições de objetos que compõem as páginas, foram obtidos os dois próximos gráficos (Figuras 81 e 82), nos quais, trabalhou-se com ambiente comutado por pacotes (PS), no acesso dos UE às páginas disponíveis no *web_server*.

Partindo-se dos resultados (Figura 81), constatou-se que as configurações do cenário c (com uso do *kernel* KASUMI), a (sem segurança) e b (autenticação) com chave de 128kbts fugiram drasticamente à curva média de 1,142s para 20 UE, 60 UE e 40 UE, respectivamente.

Os dados podem ser verificados através da Tabela 27, que representa o tempo de resposta para as requisições de páginas feitas ao *web_server*.

Tabela 27 – Tempo de resposta médio para acesso a páginas HTTP (s).

SEGURANÇA	CONFIGURAÇÃO	NÚMERO DE CELULARES						Média
		2	4	10	20	40	60	
Não	Sem segurança	1,172	1,107	1,102	1,132	1,088	1,087	1,115
	MILENAGE com AES (chave 128K)	1,172	1,142	1,147	1,142	1,058	1,137	1,133
	MILENAGE com AES (chave 192K)	1,182	1,187	1,142	1,117	1,122	1,137	1,148
Autenticação	MILENAGE com AES (chave 256K)	1,172	1,122	1,097	1,132	1,112	1,132	1,128
	Funções F8 e F9 com KASUMI	1,231	1,122	1,132	1,192	1,137	1,142	1,159
	Funções F8 e F9 com KASUMI e MILENAGE (chave 128K)	1,231	1,177	1,157	1,122	1,132	1,132	1,159
Confidencialidade e Integridade	Funções F8 e F9 com KASUMI e MILENAGE (chave 192K)	1,192	1,167	1,127	1,142	1,117	1,137	1,147
	Funções F8 e F9 com KASUMI e MILENAGE (chave 256K)	1,206	1,177	1,103	1,137	1,112	1,167	1,150
	Média	1,195	1,150	1,126	1,140	1,110	1,134	1,142

Figura 81. Comparativo dos cenários de segurança com relação aos acessos a páginas HTTP.

Quanto às requisições de objeto feitas ao servidor, foram atendidas em média de 289ms, conforme a curva média do gráfico presente na Figura 82. O melhor desempenho está na configuração de segurança com a inserção das funções f8 e f9 (*kernel* KASUMI), tendo em média 280ms. A segunda melhor situação encontrada é a do cenário sem segurança, com média de 281ms. As piores situações estão nos cenários configurados com autenticação, confidencialidade e integridade para os tamanhos de chaves de 128kbits e 256kbits, com 295ms.

Tabela 28 – Tempo de resposta médio para acesso a objetos HTTP (s).

SEGURANÇA	CONFIGURAÇÃO	NÚMERO DE CELULARES						Média
		2	4	10	20	40	60	
Não	Sem segurança	0,279	0,278	0,283	0,283	0,279	0,283	0,281
Autenticação	MILENAGE com AES (chave 128K)	0,278	0,302	0,298	0,298	0,293	0,293	0,294
	MILENAGE com AES (chave 192K)	0,283	0,303	0,293	0,288	0,283	0,298	0,291
	MILENAGE com AES (chave 256K)	0,278	0,288	0,283	0,298	0,283	0,288	0,286
Confidencialidade e Integridade	Funções F8 e F9 com KASUMI	0,283	0,273	0,283	0,283	0,273	0,283	0,280
Confidencialidade, Integridade e Autenticação	Funções F8 e F9 com KASUMI e MILENAGE (chave 128K)	0,298	0,302	0,293	0,293	0,288	0,293	0,295
	Funções F8 e F9 com KASUMI e MILENAGE (chave 192K)	0,288	0,302	0,278	0,293	0,293	0,288	0,290
	Funções F8 e F9 com KASUMI e MILENAGE (chave 256K)	0,288	0,312	0,288	0,298	0,288	0,298	0,295
	Média	0,284	0,295	0,287	0,292	0,285	0,291	0,289

Figura 82. Comparativo dos cenários de segurança com relação às requisições de objetos HTTP.

Para o cenário representando o uso de autenticação, confidencialidade e integridade, cenário d, com tamanho de chave 128kbits, houve uma tendência de aproximação à curva da função representada pelo cenário a (sem segurança), porém, com o acréscimo da quantidade de informações, devido aos algoritmos MILENAGE com AES/Rjindael e *kernel* KASUMI nas funções f8 e f9, ocorre conseqüentemente um atraso três vezes maior.

Para o gráfico contendo o desempenho do sistema relacionado ao atraso de voz, foram obtidos os dados e, desta forma, construiu-se a Tabela 29. É na Figura 83 que se tem o atraso

fim-a-fim para os diversos cenários. O cenário que apresenta menor atraso para maior quantidade de celulares em uma mesma célula é o cenário com segurança utilizando o MILENAGE com AES e chave de 256kbits.

Figura 83. Comparativo dos cenários de segurança com relação ao atraso de voz fim-a-fim.

Tabela 29 – Atraso médio na transmissão de voz fim-a-fim (ms).

SEGURANÇA	CONFIGURAÇÃO	NÚMERO DE CELULARES						Média
		2	4	10	20	40	60	
Autenticação	Não Sem segurança	16,50	55,40	43,20	120,60	125,60	124,60	80,98
	MILENAGE com AES (chave 128K)	16,60	47,90	120,60	108,40	123,60	130,70	91,30
	MILENAGE com AES (chave 192K)	16,60	51,20	114,50	126,60	133,70	131,70	95,72
	MILENAGE com AES (chave 256K)	16,70	53,30	115,50	122,60	126,60	121,60	92,72
Confidencialidade e Integridade	Funções F8 e F9 com KASUMI	16,60	59,40	125,60	124,60	126,60	133,70	97,75
Confidencialidade, Integridade e Autenticação	Funções F8 e F9 com KASUMI e MILENAGE (chave 128K)	16,40	129,70	119,50	122,60	135,80	133,70	109,62
	Funções F8 e F9 com KASUMI e MILENAGE (chave 192K)	16,60	45,90	117,50	124,60	126,60	130,70	93,65
	Funções F8 e F9 com KASUMI e MILENAGE (chave 256K)	16,60	54,00	115,50	123,60	125,60	132,70	94,67
	Média	16,58	62,10	108,99	121,70	128,01	129,93	94,55

Comparando-se os cenários (com chaves de 128kbits, 192kbits e 256kbits), contemplando somente o algoritmo MILENAGE com AES/Rjindael na autenticação, constatou-se que o desempenho cresceu proporcionalmente com o aumento do tamanho de

chave, otimizando a carga de dados relativos à segurança, conforme o maior número de UE (Figura 84).

Figura 84. Comparativo dos cenários de autenticação (atraso de voz fim-a-fim).

Figura 85. Comparativo dos cenários de autenticação, confidencialidade e integridade (atraso de voz fim-a-fim).

De acordo com a Figura 85, observou-se que o cenário contendo tamanho de chave de 128kbts tem pior desempenho, pois corresponde à maior média de atraso (109,62ms), observando-se também a ascendência abrupta da curva de atraso para apenas 4 UE.

Analisando-se as curvas da Figura 86, constatou-se que a melhor situação englobando segurança ocorre para a função representada pelo uso do algoritmo MILENAGE de *kernel* AES/Rjindael com chave de 256kbts, pois tende a aproximar-se da função representada pela ausência de segurança, com pequena diferença (moderado crescimento) para cenários com mais do que 40 UE.

Figura 86. Comparativo dos cenários de segurança com relação à variação de atraso.

Figura 87. Comparativo dos cenários de segurança com relação à variação de atraso do MILENAGE.

Na comparação contida na Figura 87, apenas as funções referentes ao uso somente de

autenticação, afirma-se novamente que a função representada pelo uso do algoritmo MILENAGE de *kernel* AES/Rjindael com chave de 256kbits tem melhor desempenho com relação às demais curvas.

O valor de atraso tem seus piores índices maximizando e minimizando o número de UE ao extremo (no gráfico da Figura 88, $\min\{2 \text{ UE}\}$, $\max\{60 \text{ UE}\}$).

A Tabela 30 corresponde aos gráficos das Figuras 86, 87 e 88.

Figura 88. Comparativo dos cenários de segurança com relação à variação de atraso do MILENAGE/KASUMI.

Tabela 30 – Variação de atraso médio na transmissão de voz fim-a-fim (ms).

SEGURANÇA	CONFIGURAÇÃO	NÚMERO DE CELULARES						Média
		2	4	10	20	40	60	
Autenticação	Sem segurança	0,0000695	0,0479729	0,0790540	0,0902027	0,0800675	0,0702702	0,0612728
	MILENAGE com AES (chave 128K)	0,0000702	0,0205405	0,1043918	0,0722972	0,1054054	0,1297297	0,0720725
	MILENAGE com AES (chave 192K)	0,0000723	0,0030405	0,0841216	0,0942567	0,0780405	0,1378378	0,0662282
	MILENAGE com AES (chave 256K)	0,0000716	0,0210810	0,0831081	0,0902027	0,0861486	0,0993243	0,0633227
Confidencialidade e Integridade	Funções F8 e F9 com KASUMI	0,0000702	0,0425675	0,1013513	0,0912162	0,0697297	0,1310810	0,0726693
Confidencialidade, Integridade e Autenticação	Funções F8 e F9 com KASUMI e MILENAGE (chave 128K)	0,0000697	0,1297297	0,0881756	0,0912162	0,0810810	0,1337837	0,0873427
	Funções F8 e F9 com KASUMI e MILENAGE (chave 192K)	0,0000723	0,0254054	0,0891891	0,0922297	0,0820945	0,1338378	0,0704715
	Funções F8 e F9 com KASUMI e MILENAGE (chave 256K)	0,0000719	0,0291891	0,0861486	0,0932432	0,0675675	0,1378378	0,0690097
	Média	0,0000710	0,0399408	0,0894425	0,0893581	0,0812668	0,1217128	0,0702987

7. Conclusão e Trabalhos Futuros

A universalização dos serviços é a base para um futuro sólido de troca de informações, o que torna ainda mais atraente a idéia de termos mobilidade e acesso internacional, promovendo não somente a disseminação de informações, mas também, a aproximação de culturas, realçando ainda mais a força da globalização.

Este trabalho foi apresentado no Congresso Internacional IBERSENSOR2008 (6th *Iberoamerican Congress on Sensors*), realizado em São Paulo, Brasil, no período de 24 a 27 de novembro de 2008, na sessão *Instrumentation, Signal Processing and Communications*, através do artigo denominado **Influência da Autenticação de Dados Sobre o Desempenho de Redes UMTS**, publicado nos anais do evento (*Proceedings of the IBERSENSOR 2008*, pg. 648).

Os cenários e respectivas simulações caracterizam a influência dos algoritmos de autenticação (MILENAGE com uso do *kernel* AES/Rjindael), confidencialidade (função f8 com *kernel* KASUMI) e integridade (função f9 com *kernel* KASUMI) e tamanho de chaves utilizado sobre a capacidade de tráfego e o atraso das mensagens na UMTS *Terrestrial Radio Access Network* (UTRAN), contendo apenas um *Node-B* interfaceando com o *Core Network* (CN) e *General Packet Radio Service* (GPRS).

Os links que interconectam os elementos do CN, GPRS e outras redes, também influem fortemente sobre a capacidade da rede de acesso.

Com base nos gráficos gerados através das simulações, pôde-se observar que cenários sem inserção de segurança possuem menor atraso, porém, o preço a ser pago é a vulnerabilidade da rede *Universal Mobile Telecommunication System* (UMTS).

As chaves proporcionam maior atraso, porém, os cenários indicam que existem situações em que há otimização sobre o tempo de resposta mesmo com a variabilidade do número de chaves e *User Equipments* (UE), o que acarreta na possibilidade de uso de chaves com maior tamanho e pouca perda de desempenho coerente do sistema.

Como possibilidade de implementação e pesquisa futura e, dando continuidade ao desenvolvimento deste trabalho, têm-se alguns assuntos importantes a serem abordados e que não fazem parte do escopo deste, sendo estes:

- Medição e análise da influência da criptografia sobre a sinalização entre os elementos do *Core Network* (CN), inclusive entre redes distintas, tais como, *Public Land Mobile Network* (PLMN) e *Public Switched Telephone Network* (PSTN);

- Verificação da segurança entre redes de diferentes tipos conectadas à rede UMTS (ou seja, com uso de tecnologias de acesso diferentes), contendo análise de segurança relacionada ao desempenho do ponto de vista da rede para os mesmos aspectos de cenário estudados neste trabalho;
- Implementação de segurança na comunicação entre diferentes PLMN da rede UMTS e estudo sobre universalização dos serviços prestados entre as redes celulares, outras redes sem fio, de telefonia fixa e *Packet Data Network* (PDN);
- Estudo e impacto de outros tamanhos de chaves e outras formas de inserção de segurança, tanto como algoritmos com o uso de diferentes kernels e variações de blocos;
- Análise sobre o impacto de algoritmos de segurança, em diversos níveis, sobre interconexões de redes 3G com redes 2G e 4G;
- Estudo da variabilidade da autenticação, autorização e registro num ambiente *Next Generation Network* (NGN) (*IP Multimedia Subsystem* (IMS) + *PSTN Emulating Subsystem* (PES)).

8. Referências

8.1. Livros

- [CAST 01] CASTRO, J. P. **The UMTS Network and Radio Access Technology**. Chichester: John Wiley & Sons, 2001.
- [CHAN 05] CHANDRA, P. **Bulletproof Wireless Security: GSM, UMTS, 802.11 and Ad Hoc Security**. Burlington: Elsevier, 2005.
- [COME 01] COMER, D. E. **Redes de Computadores e Internet**. 2. ed. São Paulo: Bookman, 2001.
- [DANT 02] DANTAS, M. **Tecnologias de Redes de Comunicação e Computadores**. Rio de Janeiro: Axcel Books, 2002.
- [DAVI 06] DAVIDSON, J. et al. **Voice over IP Fundamentals**. 2nd ed. New York: Cisco Press, 2006.
- [ESMA 03] ESMAILZADEH, R.; NAKAGAWA, M. **TDD-CDMA for Wireless Communications**. Norwood: Artech House, 2003.
- [FREI 02] FREIRE, V. A.; SOARES, L. C. **Redes Convergentes**. Rio de Janeiro: Alta Books, 2002.
- [GALL 03] GALLO, M. A.; HANCOCK, W. M. **Comunicação entre Computadores e Tecnologias de Redes**. São Paulo: Thomson, 2003.
- [HERS 02] HERSENT, O.; GUIDE, D.; PETIT, J. P. **Telefonia IP: Comunicação Multimídia Baseada em Pacotes**. São Paulo: Makron Books, 2002.
- [HILL 02] HILLEBRAND, F. **GSM and UMTS: The Creation of Global Mobile Communication**. Chichester: John Wiley & Sons, 2002.
- [HOLM 00] HOLMA, H.; TOSKALA, A. **WCDMA for UMTS: Radio Access for Third Generation Mobile Communications**. Chichester: John Wiley & Sons, 2000.
- [HOLM 04] HOLMA, H.; TOSKALA, A. **WCDMA for UMTS: Radio Access For Third Generation Mobile Communications**. 3rd ed. Chichester: John Wiley & Sons, 2004.
- [HOLM 06] HOLMA, H.; TOSKALA, A. **HSDPA/HSUPA for UMTS: High Speed Radio Access for Mobile Communications**. Chichester: John Wiley & Sons, 2006.
- [KAAR 05] KAARANEN, H. et al. **UMTS Networks: Architecture, Mobility and Services**. 2nd ed. Chichester: John Wiley & Sons, 2005.
- [KARI 02] KARIM, M. R.; SARRAF, M. **W-CDMA and CDMA2000 for 3G Mobile Networks**. New York: McGraw-Hill, 2002.
- [KURO 03] KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet: Uma Nova Abordagem**. São Paulo: Addison Wesley, 2003.
- [LIMA 01] LIMA JÚNIOR, A. W. **Telecomunicações Multimídia: Internet, LANs e WANs**. Rio de Janeiro: Book Express, 2001.
- [NIEM 03] NIEMI, V.; NYBERG, K. **UMTS Security**. Chichester: John Wiley & Sons, 2003.
- [PFLE 02] PFLEEGER, C. P.; PFLEEGER, S. L. **Security in Computing**. 3rd ed. New Jersey: Prentice Hall PTR, 2002.
- [PFLE 06] PFLEEGER, C. P.; PFLEEGER, S. L. **Security in Computing**. 4th ed. New Jersey: Prentice Hall PTR, 2006.
- [RAPP 02] RAPPAPORT, T. **Wireless Communications: Principles and Practice**. 2nd ed. New Jersey: Prentice Hall PTR, 2002.
- [RAPP 96] RAPPAPORT, T. **Wireless Communications: Principles and Practice**. New Jersey: Prentice Hall PTR, 1996.
- [REDL 98] REDL, S. M.; WEBER, M. K.; OLIPHANT, M. W. **GSM and Personnal Communications Handbook**. Norwood: Artech House, 1998.
- [SEUR 03] SEURRE, E.; SAVELLI, P.; PIETRI, P-J. **EDGE for Mobile Internet**. Norwood: Artech House, 2003.

- [SOAR 95] SOARES, L. F. G.; SOUZA, F. G. L.; COLCHER, S. **Redes de Computadores**: Das LANs, MANs e WANs às Redes ATM. 2. ed. Rio de Janeiro: Campus, 1995.
- [SOUS 99] SOUSA, L. B. **Redes de Computadores**: Dados, Voz e Imagem. São Paulo: Érica, 1999.
- [STAL 99] STALLINGS, W. **Cryptograph and Network Security**: Principles and Practice. 2nd ed. New Jersey: Prentice Hall, 1999.
- [SVER 05] SVERZUT, J. U. **Redes GSM, GPRS, EDGE e UMTS**: Evolução a Caminho da Terceira Geração (3G). São Paulo: Érica, 2005.
- [TANE 97] TANENBAUM, A. S. **Redes de Computadores**. 3. ed. Rio de Janeiro: Campus, 1997.
- [TERA 00] TERADA, R. **Segurança de Dados**: Criptografia em Redes de Computador. São Paulo: Edgard Blücher, 2000.
- [TOLE 01] TOLEDO, A. P. **Redes de Acesso em Telecomunicações**. São Paulo: Makron Books, 2001.
- [TORR 01] TORRES, G. **Redes de Computadores**: Curso Completo. Rio de Janeiro: Axcel Books, 2001.
- [WAGN 06] WAGNER, F. et al. **Modeling Software with Finite State Machines**: A Practical Approach. New York: CRC Press, 2006.
- [WALK 03] WALKER, B.; SEIDENBERG, P.; ALTHOFF, M. P. **UMTS**: The Fundamentals. Chichester: John Wiley & Sons, 2003.
- [WILC 05] WILCOX, J. R.; GIBSON, D. K. **Video Communications**: The Whole Picture. San Francisco: CMP Books, 2005.
- [WISE 02] WISELY, D.; EARDLEY, P.; BURNES, L. **IP for 3G**: Networking Technologies for Mobile Communications. Chichester: John Wiley & Sons, 2002.

8.2. Artigos

- [ADAC 98] ADACHI, F.; SAWAHASHI, M.; SUDA, H. Wideband DS-CDMA for Next Generation Mobile Communications System. **IEEE Communication Magazine**, v. 36, n. 9, pp. 56-69, sep. 1998.
- [BALD 04] BALDERAS-CONTRERAS, T. et al. Security Architecture in UMTS Third Generation Cellular Networks. **Coordinación de Ciencias Computacionales INAOE**, n. CCC-04-002 27, feb. 2004.
- [BOMA 02] BOMAN, K. et al. UMTS Security. **IEEE – Eletronic & Communication Engineering Journal**, oct. 2002.
- [BOSW 01] BOSWORTH, K. P.; TEDESCHI, N. Public key-infrastructures – the next generation. **BT Technology Journal**, v. 19, n. 3, pg 44-59, jul. 2001.
- [BRIT 03] BRITO, R. C.; MARTENDAL, D. M.; OLIVEIRA, H. E. M. Máquinas de estados finitos de Mealy e Moore. **Departamento de Informática e Estatística – INE da Universidade Federal de Santa Catarina (UFSC)**, Brasil, 2003.
- [CARN 04] CARNEIRO, G. Cross-Layer Design In 4G Wireless Terminals. **IEEE Wireless Communications**, 2004.
- [CARP 00] CARPENTER, B.; FINK, B.; MOORE, K. Connecting IPv6 Routing Domains Over the IPv4 Internet. **The Internet Protocol Journal**, v. 3, n. 1, mar. 2000.
- [DAEM 02] DAEMEN, J.; RIJMEN, V. The Design of Rijndael, AES - The Advanced Encryption Standard. **Springer-Verlag**, 2002.
- [DAHL 98] DAHLMAN, E. et al. UMTS/IMT-2000 Based on Wideband CDMA. **IEEE Communication Magazine**, p. 70-80, sep. 1998.
- [DOBB 05] DOBBERTIN, H.; KNUDSEN, L.; ROBSHAW, M. The Cryptanalysis of the AES – A Brief Survey. **Springer-Verlag**, Berlin, Heidelberg, p. 1-10, 2005.
- [DONZ 04] DONZÉ, F. IPv6 Address Autoconfiguration. **The Internet Protocol Journal**, v. 7, n. 2, jun. 2004.
- [FERG 01] FERGUSON, N. et al. Improved Cryptanalysis of Rijndael. **Springer-Verlag**, Berlin, Heidelberg, p. 213-230, 2001.
- [FERN 04] FERNANDEZ, E. et al. An overview of the security of wireless networks. **Handbook of Wireless LANs**, CRC Press, 2004.

- [FERN 05] FERNANDEZ, E. et al. Some security issues of wireless systems. **Advanced Distributed Systems: 5th International School and Symposium - ISSADS 2005**, Guadalajara, p. 24-28, jan. 2005. Revised Selected Papers.
- [GEHR 04] GEHRMANN, C. Manual authentication for wireless devices. **RSA Cryptobytes**, 2004.
- [GERL 02] GERLA, M. et al. UMTS-TDD: A Solution for Internetworking Bluetooth Piconets in Indoor Environments. **Computers and Communications**, 2002. **Proceedings of ISCC 2002 Seventh International Symposium**, p. 825-830, 1-4 jul. 2002.
- [GREC 03] GRECAS, C. F. et al. Introduction of the Asymmetric Cryptography in GSM, GPRS, UMTS, and Its Public Key Infrastructure Integration. **Kluwer Academic Publishers – Mobile Networks and Applications**, Netherland, 2003.
- [HAAR 00] HARRDT, M. et al. The TD-CDMA Based UTRA TDD Mode. **IEEE Journal on Selected Areas in Communications**, v. 18, n. 8, p. 1375-1385, aug. 2000.
- [HARN 03] HARN, L.; HSIN, W-J. On the Security of Wireless Network Access with Enhancements. **ACM WiSe'03**, San Diego, California, p. 88-95, sep. 2003.
- [KARR 01] KARREBERG, D. et al. Development of the Regional Internet Registry System. **The Internet Protocol Journal**, v. 4, n. 4, dec. 2001.
- [KOIE 05] KOIEN, G. M. Privacy Enhanced Cellular Access Security. **ACM – International Conference on Mobile Computing and Networking**, Germany, 2005.
- [LAUT 04] LAUTER, K. The Advantages Of Elliptic Curve Cryptography For Wireless Security. **IEEE Wireless Communications**, v. 11, n. 1, p. 62-67, feb. 2004.
- [LUCI 03] LUCIO, G. F. et al. OPNET Modeler and NS-2: Comparing the Accuracy of Network Simulators for Packet-Level Analysis using a Network Testbed. **WSEAS Transactions on Computers**, UK, 2003.
- [MACH 00] MACHADO, P. P.; BEZERRA, E.; LIMA, J. O. Segurança da Informação: Fundamentos do Modelo de Segurança da Informação. **Ministério do Planejamento**, Brasília/DF, 2000.
- [MEAL 55] MEALY, G. H. A Method for Synthesizing Sequential Circuits. **Bell System Technology Journal**, v. 34, p. 1045-1079, sep. 1955.
- [MOOR 56] MOORE, E. F. Gedanken-experiments on Sequential Machines. **Annals of Mathematical Studies**, Automata Studies of Princeton University Press. Princeton, n. 34, p. 129-153, 1956.
- [OJAN 98] OJANPERA, T.; PRASAD, R. An Overview of Air Interface Multiple Access for IMT-2000/UMTS. **IEEE Communication Magazine**, v. 36, n. 9, p. 82-95, sep. 1998.
- [PATI 99] PATIYOOT, D.; SHEPHERD, S. J. Cryptographic Security Techniques for Wireless Networks. **ACM – SIGOPS Operating Systems Review**, v. 33, n. 2, apr. 1999.
- [PAUT 91] PAUTET, M.; MOULY, M. GSM Protocol Architecture: Radio Sub-System Signalling. **41st IEEE Vehicular Technology Conference - 1991 Gateway to the Future Technology in Motion**, St. Louis, p. 326-332, 1991.
- [PRAS 04] PRASAD, A. R.; KEMPF, J. Security for Next Generation Communications. **Kluwer Academic Publishers – Wireless Personal Communications**, n. 29, p. 157-160, 2004.
- [PÜTZ 01] PÜTZ, S. et al. Security Mechanisms in UMTS. **DuD – Datenschutz und Datensicherheit**, 2001.
- [RAHM 02] RAHMAN, M. G.; IMAI, H. Security in Wireless Communications. **Kluwer Academic Publishers – Wireless Personal Communications**, n. 22, p. 213-228, 2002.
- [RENA 04] RENAUDIN, M. et al. High Security Smartcards. **IEEE - Proceedings of the Design, Automation and Test in Europe Conference and Exhibition**, 2004.
- [RICC 06] RICCIATO, F. Unwanted Traffic in 3G Networks. **ACM – SIGCOMM Computer Communication Review**, v. 36, n. 2, apr. 2006.
- [ROSA 02] ROSA, R. A. S.; FALEIROS, A. C. Análise do algoritmo vencedor do AES: o Rijndael. Instituto Tecnológico da Aeronáutica – ITA, 2002.
- [SANT 02] SANTOS, M. C. M.; XEXEO, J. A. M.; REZENDE, J. F. Análise Formal de Protocolos de Segurança para Redes Celulares. **IV Workshop de Comunicação Sem Fio e Computação Móvel – IME-USP**, São Paulo, v. 1, p. 78-89, 2002.

- [WONG 03] WONG, K. D. et al. UMTS Signaling over 802.11 Wireless LAN. IEEE 58th, Vehicular Technology Conference, 2003 - VTC 2003, v. 3, p. 1798-1802, oct. 2003.
- [XU 04] XU, W. et al. Channel Surfing and Spatial Retreats: Defenses against Wireless Denial Of Service. **Proceedings of the 2004 ACM Workshop on Wireless Security**, 2004.
- [YANG 06] YANG, H. et al. Securing A Wireless World. **Proceedings of the IEEE**, v. 94, n. 2, feb. 2006.
- [ZHU 04] ZHU, J. A new authentication scheme with anonymity for wireless environments. **Consumer Electronics**, IEEE Transactions, v. 50, n. 1, p. 231- 235, feb. 2004.

8.3. Normas e Padrões

- [ETSI 00] Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification (GSM 09.02 version 5.15.1 Release 1996). Valbonne, France, 2000.
- [G702 88] Recommendation G.702: Digital Aspects of Digital Transmission Systems – Terminal Equipments – Digital hierarchy bit rates – Plesiochronous Digital Hierarchy (PDH). 1988.
- [G703 01] Recommendation G.703: Physical/electrical characteristics of hierarchical digital interfaces. 2001.
- [G707 88] Recommendation G.707/Y.1322: Network Node Interface for the Synchronous Digital Hierarchy (SDH). 1988.
- [I120 93] Integrated Services Digital Network (ISDN). 1993.
- [I136 94] EIA Interim Standard IS-136.2, “800 MHz TDMA—Radio Interface—Mobile Station—Base Station Compatibility— Traffic Channels and FSK Control Channels”. 1994.
- [I312 92] Integrated Services Digital Network (ISDN) I.312 (10/92); Overall Network Aspects and Functions, ISDN User-Network Interfaces Q.1201 (10/92); Principles of Intelligent Network Architecture. 1992.
- [IMTe 07] Detailed specifications of the radio interfaces of International Mobile Telecommunications-2000 (IMT-2000). Geneva, 2007.
- [IS41 82] Cellular Radiotelecommunications Intersystem Operations: Intersystem Handoff TIA/EIA/IS-41.2-C. January, 1982.
- [IS41 88] Cellular Radiotelecommunications Intersystem Operations: Functional Overview ANSI/TIA/EIA/IS-41-A. February, 1988.
- [IS41 96] Cellular Radiotelecommunications Intersystem Operations: Intersystem Handoff TIA/EIA-41.2-D. January, 1996.
- [IS54 92] EIA Standard IS-54-B, “Cellular System Dual-Mode Mobile Station—Base Station Compatibility Standard,” 1992.
- [LSMP 02] BRASIL. Agência Nacional de Telecomunicações. Licitação para a aquisição de licença de uso do SMP nas bandas D e E. Licitação nº 002/2002/SPV-ANATEL de 22/08/2002. Brasília/DF, 2002.
- [M687 97] Recommendations ITU-R M.687-2, International Mobile Telecommunications-2000 (IMT-2000), 1997.
- [PGOu 04] BRASIL. Agência Nacional de Telecomunicações. Resolução Anatel Nº 376 de 02/09/2004, que aprova o Plano Geral de Outorgas (PGO). Brasília/DF, 2004.
- [R272 01] BRASIL. Agência Nacional de Telecomunicações. Resolução nº 272, de 9 de agosto de 2001, que aprova o Regulamento do Serviço de Comunicação Multimídia. Brasília/DF, 2001.
- [R328 07] BRASIL. Agência Nacional de Telecomunicações. Resolução nº 328, de 29 de janeiro de 2003, que aprova os modelos de Termo de Autorização para Exploração dos Serviços de Comunicação Multimídia, de interesse coletivo. Brasília/DF, 2007.
- [RSMP 07] BRASIL. Agência Nacional de Telecomunicações. Resolução nº 477, de 7 de agosto de 2007, que aprova o Regulamento do Serviço Móvel Pessoal. Brasília/DF, 2007.
- [T102 00] 3GPP TS 33.102. 3G security; security architecture, 2000.
- [T201 05] 3GPP TS 35.201. Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications (Release 6), 2005.

- [T202 05] 3GPP TS 35.202. Specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI algorithm specification (Release 6), 2005.
- [T203 05] 3GPP TS 35.203. Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors test data (Release 7), 2007.
- [T204 05] 3GPP TS 35.204. Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data (Release 7), 2007.
- [T205 05] 3GPP TS 35.205. 3Gsecurity; specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: general (Release 6), 2005.
- [TR21 08] ETSI TR 121.905. Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (3GPP TR 21.905 version 8.6.0 Release 8), 2008.
- [U105 99] 3GPP TS 22.105. Release 1999, Service Aspects; Services and Service Capabilities, 1999.
- [U401 00] 3GPP TS 25.401. UTRAN Overall Description, 2000.
- [X210 93] Data Networks and Open System Communications; Open System Interconnection – General; Information Technology – Open Systems Interconnection – Basic Reference Model: Conventions for the Definition of OSI Services. 1993.
- [X680 02] OSI networking and system aspects – Abstract Syntax Notation One (ASN.1); Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2002.

8.4. Acesso a Website

- [HUJI 08] The Hebrew University of Jerusalem. Computer Science and Engeneering. Disponível em: <<http://www.cs.huji.ac.il/site/index.php>>. Acesso em: 15 dez. 2008.
- [OPNT 07] OPNET Modeler v. 10.0. Disponível em: <<http://www.opnet.com/>>. Acesso em: 10 fev. 2006.
- [OSSL 07] OpenSSL v.3. Disponível em: <<http://www.openssl.org/>>. Acesso em: 25 mar. 2007.
- [TUDE 04] Tutorial UMTS. Disponível em: <<http://www.teleco.com.br/tutoriais/>>. Acesso em: 15 dez. 2007.
- [WARC 92] World Administrative Radio Conference 1992. Genebra, 1992. Disponível em: <<http://www.umtsworld.com/technology/frequencies.htm>>. Acesso em: 12 jan. 2008.
- [WIKI 08] Wikipedia: A Enciclopédia Livre. Disponível em: <<http://www.wikipedia.org/>>. Último acesso em: 10 dez. 2008.
- [WRCo 00] World Radiocommunication Conference 2000. Istambul, 2000. Disponível em: <<http://www.umtsworld.com/technology/frequencies.htm>>. Acesso em: 15 jan. 2008.

APÊNDICE I

FSM

Finite State Machine (FSM), também chamado de Autômato Finito (AF), é uma poderosa ferramenta de representação (abstração) de qualquer evento que se deseja modelar. Segundo [WAGN 06], “... um dos mais poderosos modelos é a *Finite State Machine* (FSM), que é usada para descrever comportamento: o que fazer em todas as situações imagináveis.”.

O controle do sistema define as saídas conforme as entradas, ou seja, se existirem valores de entrada suficientes para determinar as saídas, então, o sistema é combinacional e não é necessário o conceito de estados. Contudo, se o sistema precisar de informação adicional sobre a seqüência de dados alterados na entrada, para depois determinar as saídas, o sistema é seqüencial. A parte lógica do sistema responsável pelo comportamento do sistema é denominada máquina de estado. Qualquer lógica que determina o comportamento do sistema é uma máquina de estados, portanto, uma máquina de estados pode ser representada pela figura abaixo.

Figura 89. Elementos da definição da máquina de estados.
(Fonte: [WAGN 06], pg. 65)

O histórico de mudança das entradas é armazenado em uma variável interna, denominada estado (ou *State*). As condições de transição de estado e saída são funções da entrada mais um estado. Para que o modelo FSM não fique complexo demais, os números de entradas, saídas e estados têm limites. Estes limites não são constantes fixas, porém, resultam de um senso comum de aplicabilidade, itens de projeto e outros fatores a serem abstraídos.

O modelo de Moore é usado para situações em que as máquinas de estados só geram ações *Entry*. No caso de as máquinas de estados que geram ações *Input*, dá-se o nome de

modelo de Mealy. A escolha do modelo influencia o projeto, mas não existem indicações sobre qual o melhor modelo, pois este depende da aplicação.

As transições entre estados podem ser visualizadas através do diagrama de transições da figura a seguir. Na figura, demonstra-se que os estados e condições de transição, para que a tabela de transição de estados do estado *State*, deva corresponder às seqüências de ações. A existência de quaisquer ações é indicada pelas letras E (*Entry*), X (*Exit*) e I (*Input*).

No exemplo, existe um *State* em que uma *Condition2* para uma ação *Input* é igual a uma transição *Condition2*, existindo duas transições possíveis. Se somente a *Condition2* for verdadeira, a *Action* será carregada e a máquina de estados mudará para o *State2*. Se a *Condition1* e *Condition2* forem ambas verdadeiras, a *Action* será executada no curso, mas a transição para o *State1* será feita. Nós podemos ver a *Action* como uma transição do *State* para o *State1*.

Figura 90. Diagrama e tabela de transição de estados.
(Fonte: [WAGN 06], pg. 65)

A teoria das máquinas de estado surgiu em 1950 através dos trabalhos de George H. Mealy [MEAL 55] e Edward F. Moore [MOOR 56]. As máquinas seqüenciais combinam lógica combinacional *booleana* com memória, para gerar mecanismos seqüenciais de controle.

Como exemplos, serão mostrados Autômatos Finitos que são divididos em dois tipos:

Autômato Finito Determinístico (AFD) e Autômato Finito Não Determinístico (AFND). As máquinas de Mealy e Moore são modificações sobre o AFD e serão explicadas a seguir.

Modelo de Moore

Figura 91. Modelo de Moore.

Neste modelo, as ações de controle estão associadas aos estados, ou seja, as saídas são associadas às lógicas de entrada, como ilustra a figura anterior.

A FSM do modelo de Moore (MMo) possui uma função que gera uma saída (que pode ser vazia) para cada estado da máquina. Esta saída só depende do estado atual da máquina. A MMo é um AFD com suas saídas associadas aos estados, sendo representada formalmente por $MMo = (\Sigma, Q, \delta, q_0, F, \Delta, \delta S)$, onde:

- Σ – é a representação de símbolos de entrada;
- Q – é um conjunto de estados possíveis do autômato, sendo finito;
- δ – é a função programa ou de transição $\delta: Q \times \Sigma \rightarrow Q$;
- q_0 – é o estado inicial do autômato, tal que q_0 é elemento de Q ;
- F – é um conjunto de estados finais tal que F está contido em Q ;
- Δ – é a representação de símbolos de saída;
- δS – é a função de saída $\delta S: Q \rightarrow \Delta$, sendo uma função total.

Este esquema pode ser utilizado em compiladores e tradutores de linguagens, como em [BRIT 03].

Modelo de Mealy

No modelo de Mealy, as ações de controle estão associadas com as transições, ou seja, as saídas estão associadas aos estados (*States*) e entradas, assim como mostra a figura abaixo.

Figura 92. Modelo de Mealy.

A FSM do modelo de Mealy é um AF modificado de forma a gerar uma saída para cada transição entre estados. Neste tipo de FSM as saídas dependem do estado atual e do valor das entradas.

Uma Máquina de Mealy (MMe) é AFD com saídas associadas às transições, podendo ser representada formalmente por $MMe = (\Sigma, Q, \delta, q_0, F, \Delta)$, onde:

- Σ – é a representação de símbolos de entrada;
- Q – é um conjunto de estados possíveis do AF, o qual é finito;
- δ – é a função programa ou de transição $\delta: Q \times \Sigma \rightarrow Q \times \Delta$;
- q_0 – é o estado inicial do autômato, tal que q_0 é elemento de Q ;
- F – é um conjunto de estados finais tal que F está contido em Q ;
- Δ – é a representação de símbolos de saída.

O processamento de uma MMe para uma dada entrada Σ consiste na aplicação sucessiva da função programa para cada símbolo, até ocorrer uma condição de parada. Caso a saída da função programa seja vazia, nada é realizado. Porém, se todas as transições de uma determinada MMe gerarem saídas vazias, então esta se comporta como um AF.

Considerações dos Modelos de Moore e Mealy

O processamento de uma FSM com o modelo de Moore ocorre da mesma forma que na FSM do modelo de Mealy, assim como o tratamento para as saídas vazias. No modelo de Mealy, se todos os estados gerarem saída vazia, ele também se comporta como um AF.

A equivalência dos dois modelos de AF para saídas com entrada vazia não é válida. Neste caso, enquanto o modelo de Moore gera a palavra correspondente ao estado inicial, o modelo de Mealy não gera qualquer saída, devido à não execução de qualquer transição. Entretanto, para os demais casos, os modelos são equivalentes. Deste modo, toda Máquina de Moore pode ser simulada por uma Máquina de Mealy e vice-versa, para entradas não vazias [BRIT 03].

Baseando-se nestes mecanismos de abstração, o simulador OPNET adotou a estrutura de FSM em sua diagramação interna, ou seja, para as partes intrínsecas dos modelos de nós usados nas simulações.

APÊNDICE II

ATM

O ATM é dividido em três camadas, sendo estas, a Camada Física, Camada ATM e *ATM Adaptation Layer* (AAL).

A Camada Física está dividida em duas subcamadas: subcamada *Physical Medium* (PM) e *Transmission Convergence* (TC).

A subcamada PM contém apenas as funções dependentes do meio físico. Ela Fornece capacidade de transmissão, incluindo alinhamento de bit. Realiza codificação linear e também conversão eletro-óptico se necessário. A fibra-óptica será o meio físico e, em alguns casos, pares de cabos coaxiais e trançados são utilizados. Inclui funções de tempo de bit, tais como a geração e recepção de ondas no meio e, também, inserção e extração de informação de tempo de bit.

A subcamada TC faz, principalmente, cinco funções. A mais baixa é a geração e recuperação da transmissão de frames. A próxima função, ou seja, adaptação da transmissão de frame cuida de todas as ações para adaptar o fluxo de células de acordo com a estrutura de carga utilizada no sistema de transmissão. Ela extrai o fluxo de células ATM a partir da recepção do frame. O frame pode ser um *Synchronous Digital Hierarchy* (SDH) ou de acordo com a recomendação ITU-T G.703.

A função de delineação de célula permite que o receptor possa recuperar os limites das células. A ordenação e desordenação são feitas no corpo da informação de uma célula, antes que esta seja transmitida e recebida, para proteger o mecanismo de delineação de células. A sequência de geração *Header Error Control* (HEC) é feita na transmissão e seu valor é recalculado e comparado com o valor recebido para, assim, ser usado na correção de erros de cabeçalho. Se o cabeçalho contiver erros que não possam ser corrigidos, as células serão descartadas.

A dissociação de taxa de célula permite inserir células ociosas na transmissão, a fim de adaptar a taxa de células ATM para a capacidade de carga do sistema e suprime todas as células ociosas no recebimento. Somente células atribuídas e não atribuídas são passadas à camada ATM.

A Camada ATM é a camada acima da Camada Física, que faz as quatro funções, que são discriminadas a seguir.

- Geração e extração de cabeçalho de célula: esta função acrescenta o cabeçalho apropriado

à célula ATM (exceto para o valor do HEC) para células recebidas do AAL a serem transmitidas. Os valores do *Virtual Path Identifier* (VPI) e *Virtual Channel Identifier* (VCI) são obtidos através da translação dos identificadores *Service Access Point* (SAP). Do outro lado, na recepção, o cabeçalho é retirado. Apenas os campos de informação da célula são passados para o AAL.

- MUX/DEMUX de células: esta função multiplexa células de individuais VP e VC resultando em uma cadeia de células para transmitir. Ela divide a chegada da cadeia de células em fluxos de células individuais escritas nos VC ou VP.
- Translação VPI e VCI: esta função é desempenhada na comutação ATM e/ou na interconexão de nós. Ao mudar de VP, o valor do campo VPI de cada célula de entrada se traduz em um novo valor VPI da célula de saída. Os valores de VPI e VCI são traduzidos em novos valores em uma comutação VC.
- *Generic Flow Control* (GFC): esta função dá suporte ao controle do fluxo de tráfego ATM na rede e é definida no B-ISDN *User-to-Network Interface* (UNI).

AAL é dividida em duas subcamadas, *Segmentation and Reassembly* (SAR) e *Convergence Sublayer* (CS).

- Subcamada SAR: Esta camada realiza segmentação da informação da camada superior em um tamanho adequado para a carga útil das células ATM de uma conexão virtual e, no lado da recepção, o conteúdo das células é refeito de uma conexão virtual em unidades de dados a serem entregues às camadas superiores.
- Subcamada CS: Esta camada desempenha funções como identificação da mensagem e recuperação de tempo (*clock*). É ainda subdividida em *Common Part Convergence Sublayer* (CPCS) e *Service Specific Convergence Sublayer* (SSCS), para suportar o transporte de dados sobre ATM.

Figura 93. Estrutura de camadas ATM.
(Fonte: <http://penta2.ufrgs.br/>, consulta em 15/02/2008)

Unidades de dados de serviço AAL são transportados de um AAL-SAP para outros através da rede ATM. Os usuários podem selecionar um determinado AAL-SAP associado ao QoS requerido para o transporte. Cinco AAL foram definidos, um para cada classe de serviço.

Para entrar em contato com o autor, enviar um e-mail para marcel-wagner@hotmail.com