UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSTA DE MODELO DE AUTENTICAÇÃO PARA INTERCONEXÃO DE REDES SEM FIO HETEROGÊNEAS.

SEBASTIÃO BOANERGES RIBEIRO JÚNIOR

ORIENTADOR: PAULO ROBERTO DE LIRA GONDIM

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
PUBLICAÇÃO:
BRASÍLIA/DF: SETEMBRO – 2011

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSTA DE MODELO DE AUTENTICAÇÃO PARA INTERCONEXÃO DE REDES SEM FIO HETEROGÊNEAS.

SEBASTIÃO BOANERGES RIBEIRO JÚNIOR

DISSERTAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISÍTOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM ENGENHARIA ELÉTRICA.

APROVADA POR:

_____

Prof. Paulo R. L. Gondim, Doutor
(Orientador)

_____

Prof. Joel José Puga Coelho Rodrigues, Doutor
(UBI - Portugal)

_____

Prof. Lisandro Zambenedetti Granville, Doutor
(UFRGS)

BRASÍLIA/DF, 27 DE SETEMBRO DE 2011

FICHA CATALOGRÁFICA

RIBEIRO JR, SEBASTIÃO BOANERGES

Proposta de Modelo de Autenticação para Interconexão de Redes Sem Fio Heterogêneas. [Distrito Federal] 2011.
xvii, nnp., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2007).

Dissertação de Mestrado – Universidade de Brasília. Faculdade de Tecnologia.

Departamento de Engenharia Elétrica.

1.Convergência de redes sem fio heterogêneas 2.Gerência de Mobilidade

3.Arquitetura de Autenticação 4.Redes WLAN

I. ENE/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

RIBEIRO JR., S. B. (2011). Proposta de Modelo de Autenticação para Interconexão de Redes Sem Fio Heterogêneas. Dissertação de Mestrado em Engenharia Elétrica, Publicação 080/2011, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 2011.

CESSÃO DE DIREITOS

AUTOR: Sebastião Boanerges Ribeiro Júnior.

TÍTULO: Proposta de Modelo de Autenticação para Interconexão de Redes Sem Fio Heterogêneas.

GRAU: Mestre ANO: 2011

_____

Sebastião Boanerges Ribeiro Júnior
Rua Cesar Lattes, 700 Bloco 2 Apto 606
22.793-082 Rio de Janeiro – RJ – Brasil.

AGRADECIMENTOS

Agradeço ao meu pai, Sebastião Boanerges (*in memoriam*) pelo exemplo de vida e de perseverança que guiou minha trajetória até aqui.

Agradeço a compreensão, carinho e apoio da minha família, principalmente da minha esposa Silvana. Sem o qual este trabalho não teria sido completado.

Agradeço minha mãe, Julieta, e meus irmãos pelo modelo de vida que são.

Agradeço também aos colegas de mestrado que muito auxiliaram e serviram de exemplo.

Agradeço a Brasil Telecom e ao Mauro Fukuda pela oportunidade de realizar este mestrado.

Agradeço especialmente ao meu orientador Paulo Gondim pela inspiração e suporte na condução deste trabalho e em seus desdobramentos.

RESUMO

PROPOSTA DE MODELO DE AUTENTICAÇÃO PARA INTERCONEXÃO DE REDES SEM FIO HETEROGÊNEAS

A necessidade de evolução das redes de telecomunicações para atender a demanda por serviços convergentes entre redes com diferentes tecnologias de acesso envolve o desenvolvimento de mecanismos de gerência de mobilidade e *handover*. Estes mecanismos devem prever o incremento da utilização de serviços de comunicação multimídia em tempo real utilizando protocolos emergentes para controle de sessão como, por exemplo, o SIP (*Session Initiation Protocol*). Entre os procedimentos de gerência de mobilidade para atender este cenário, a possibilidade de autenticação única e transparente nas diferentes redes é um dos mais críticos.

Este trabalho avalia o impacto que a introdução de mecanismos de autenticação padronizados pode gerar no atraso da execução do *handover* vertical entre redes heterogêneas. As redes heterogêneas consideradas são WWAN (*Wireless Wide Area Network*) celular baseada nos padrões 3GPP (*3G Partnership Project*) e WLAN (*Wireless Local Area Network*) baseada nos padrões do *Institute of Electrical and Electronics Engineers* (IEEE). O atraso é avaliado através de modelagem analítica e complementado com medidas realizadas em elementos em operação comercial.

A modelagem e as medidas realizadas serviram de base para apresentação de propostas alternativas de melhorias, incluindo a definição de uma nova arquitetura baseada em distribuição prévia de chaves de autenticação. As melhorias propostas são modeladas e evidenciam a possibilidade de redução do tempo de atraso na execução do *handover* vertical em até trinta vezes. Com esta redução se espera que a utilização futura de serviços de comunicação multimídia de tempo real não sofra interrupções perceptíveis pelo usuário final durante o procedimento de *handover* vertical.

ABSTRACT

The mobility management and handover mechanisms development and the network evolution have been driven by the convergent services demand between heterogeneous accesses networks technologies. Those mechanisms are foreseen the increase usage of real time multimedia communication together emerging protocols such as SIP (Session Initiation Protocol). The availability of single seamless authentication between different networks is one of the most critical mobility management procedures.

This work evaluates the impact in the vertical handover execution delay after the introduction of standardized authentication mechanisms between heterogeneous wireless access networks. The target wireless networks are defined as a cellular WWAN (Wireless Wide Area Network) based on 3GPP (3G Partnership Project) standards and a WLAN (Wireless Local Area Network) based on IEEE (Institute of Electrical and Electronics Engineers) standards. The overall handover delay was evaluated through analytical modeling and supplemented with measurements in commercial live network elements.

Based on the results reached, improvements are proposed, including the definition of a new architecture for authentication keys distribution. The improvements proposed as result of this work can potentially reduce the handover delay by a rate of thirty. The new architecture with diminished handover delay allows the offer to the end users of real time communication services without disruption during vertical handover procedures.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURAS E ABREVIAÇÕES

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AP	Access Point
APN	Access Point Name (3GPP)
ASF	Alerting Standards Forum
AuC	Authentication Centre (3GPP)
B2BUA	Back-to-Back User Agent (elemento da arquitetura SIP IETF)
BSC	Base Station Controller
BSS	Base Station Subsystem
BSSMAP	Base Station System Management Part (3GPP)
BTS	Base Transceiver Station
CAMEL	Customized Applications for Mobile network Enhanced Logic (3GPP)
CAP	Camel Application Part (protocolo sinalização SS7 definido pelo 3GPP)
CBC-MAC	Cipher-Block Chaining with Message Authentication Code (IEEE)
CCMP	CTR with CBC-MAC Protocol (IEEE)
CN	Core Network (3GPP)
CS	Circuit Switched (3GPP)
CSCF	Call Session Control Function (3GPP IMS)
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol (IETF)
DNS	Domain Name System (IETF)
DTAP	Direct Transfer Application Part (3GPP)
EAP	Extensible Authentication Protocol (IETF)
ENUM	E.164 Number
EIR	Equipment Identity Register (3GPP)
ERL	Erlang
GERAN	GSM EDGE Radio Access Network (3GPP)
GGSN	Gateway GPRS Support Node (3GPP)
GMSC	Gateway MSC (3GPP)

GPRS	General Packet Radio Service (3GPP)
GSM	Global System for Mobile communication
GSN	GPRS Support Node (SGSN ou GGSN)
GTK	Group Temporal Key (IEEE 802.11i)
GTP	GPRS Tunneling Protocol (3GPP)
HLR	Home Location Register
HPLMN	Home PLMN
HSS	Home Subscriber Server (3GPP IMS)
HTTP	Hyper Text Transfer Protocol (IETF)
ISC	IMS Service Control (3GPP IMS)
IE	Information Element (IEEE)
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem (3GPP)
IMSI	International Mobile Subscriber Identifier (3GPP)
IP	Internet Protocol (IETF)
IPv4	Internet Protocol version 4 (IETF)
IPv6	Internet Protocol version 6 (IETF)
IPsec	IP security (IETF)
IP-CAN	IP-Connectivity Access Network (3GPP)
ISIM	IP Multimedia Identity Services Module (3GPP IMS)
ISP	Internet Service Provider
ISUP	ISDN User Part (protocolo da rede SS7)
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
I-CSCF	Interrogating-CSCF (3GPP IMS)
I-WLAN	Interworking WLAN (3GPP)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol (IETF)
LTE	Long Term Evolution (3GPP)
MAC	Message Authentication Code
MAP	Mobile Application Part (3GPP)
MD-5	Digest 5

ME	Mobile Equipment
MGCF	Media Gateway Control Function (3GPP IMS)
MGF	Media Gateway Function (3GPP IMS)
MGW	Media Gateway (3GPP)
MO	Mobile Originated
MPDU	MAC Protocol Data Unit (IEEE 802.11)
MRF	Media Resource Function (3GPP IMS)
MS	Mobile Station
MSC	Mobile Services Switching Centre (3GPP)
MSISDN	Mobile Station ISDN number (3GPP)
MT	Mobile Terminated
MMS	Multimedia Messaging Service
MPCC	Multi-Party Call Control
NAI	Network Access Identifier (IETF)
NAT	Network Address Translator (IETF)
O&M	Operação e Manutenção
P-CSCF	Proxy-CSCF (3GPP IMS)
PDF	Policy Decision Function (3GPP IMS)
PDN	Packet Data Network
PDP	Packet Data Protocol (3GPP)
PMK	Pairwise Master Key (IEEE 802.11i)
PS	Packet Switched (3GPP)
PTK	Pairwise Transient Key (IEEE 802.11i)
P-TMSI	Packet - Temporary Mobile Subscriber Identity
PTS	Ponto de Transferência de Sinalização (elemento da rede SS7)
QoS	Quality of Service
RFC	Request for Comments (IETF)
RLC	Radio Link Control
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RRC	Radio Resource Control
RSN	Robust Security Network (IEEE 802.11i)
SCCP	Signaling Connection Control Part (protocolo da rede SS7)
SDC	Servidor de Distribuição de Chaves

SDP	Session Description Protocol (IETF)
SGSN	Serving GPRS Support Node (3GPP)
SIM	Subscriber Identity Module (3GPP)
SIP	Session Initiation Protocol (IETF)
SNMP	Simple Network Management Protocol (IETF)
SS7	Signaling System number 7 (ITU-T)
SSID	Service Set Identifier (IEEE 802.11)
S-CSCF	Serving-CSCF (3GPP IMS)
STFC	Serviço de Telefonia Fixa Comutada (ANATEL)
TCP	Transport Control Protocol (IETF)
TKIP	Temporal Key Integrity Protocol
TMSI	Temporary Mobile Subscriber Identity (3GPP)
TR	Technical Report (3GPP)
TS	Technical Specification (3GPP)
UA	User Agent (IETF)
UDP	User Datagram Protocol (IETF)
UE	User Equipment (3GPP)
UMTS	Universal Mobile Telecommunications System (3GPP)
URI	Uniform Resource Identifier (IETF)
URL	Universal Resource Locator (IETF)
USIM	Universal Subscriber Identity Module (3GPP)
UTRAN	UMTS Terrestrial Radio Access Network (3GPP)
VLAN	Virtual Local Area Network
VLR	Visitor Location Register
VMSC	Visited MSC
VPLMN	Visited PLMN
WAG	WLAN Access Gateway (3GPP)
WFA	Wi-Fi Alliance
WLAN	Wireless Local Area Network
WLAN AN	WLAN Access Network
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access (WFA)
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

W-APN	WLAN APN
XML	Extensible Markup Language

LISTA DE VARIÁVEIS

c	Valor constante
k	Número de quadros do enlace aéreo contidos no pacote
n	Número de tentativas/retransmissões/pares de mensagens de requisição e resposta
p	Probabilidade de um quadro estar com erro no enlace aéreo
q	Taxa de perda de pacotes
τ	Tempo inter-quadro
μ	Taxa de processamento de mensagens do terminal para rede WLAN
μ'	Taxa de processamento de mensagens do terminal para aplicação
μ_{AP}	Taxa de processamento de mensagens da rede WLAN para Internet
μ_{AP}'	Taxa de processamento de mensagens da rede WLAN para os terminais
μ_{AAA}	Taxa de processamento de mensagens dos servidores AAAs
μ_{SS7}	Taxa de processamento de mensagens do servidor AAA para mensagens SS7
λ_{MH}	Taxa de chegada de mensagens da aplicação para terminal
λ_{MH}'	Taxa de chegada de mensagens no terminal da rede WLAN
λ_{WLAN}	Taxa de chegada de mensagens na rede WLAN pelos terminais
λ_{WLAN}'	Taxa de chegada de mensagens na rede WLAN pela Internet
λ_{DHCP}	Taxa de chegada de mensagens no servidor DHCP
λ_{AAA_WLAN}	Taxa de chegada de mensagens no servidor AAA pela rede WLAN
$\lambda_{AAA'\_WLAN}$	Taxa de chegada de mensagens no AAA (WLAN) pela rede intermediária
λ_{AAA_INT}	Taxa de chegada de mensagens no servidor AAA da rede intermediária
λ_{AAA_WWAN}	Taxa de chegada de mensagens no AAA (WWAN) pela rede intermediária
$\lambda_{AAA'\_WWAN}$	Taxa de chegada de mensagens no servidor AAA pela rede SS7
λ_{HLR}	Taxa de chegada de mensagens no HSS/AuC pela rede SS7
λ_{HLR}'	Taxa de chegada de mensagens no HSS em direção à rede SS7
ρ_{DHCP}	Fator de utilização do servidor de DHCP
ρ_{HLR}	Fator de utilização do HLR
Δ_{SS7}	Atraso médio de mensagens na rede SS7
Δ_{HLR}	Atraso médio de processamento para consulta ao HLR/AuC
Δ	Atraso médio de mensagens pela Internet
ARP_{WAIT}	Atraso médio entre mensagens ARP
D	Atraso médio de propagação fim a fim do quadro sobre enlace WLAN
D'	Atraso médio para transmitir pacote com controle de retransmissão sobre interface WLAN
D_{AAA_WLAN}	Atraso médio de processamento devido ao servidor AAA da rede WLAN
D_{AAA_INT}	Atraso médio de processamento devido ao servidor AAA da rede intermediária
D_{AAA_WWAN}	Atraso médio de processamento devido ao servidor AAA da rede WWAN (HPLMN)
D_{AP}	Atraso médio de processamento devido aos elementos de acesso WLAN
D_{ARP}	Atraso médio de processamento das requisições de ARP
D_{AUT}	Atraso médio de autenticação
D_{CON}	Atraso médio de conexão
D_{DHCP}	Atraso médio de troca de mensagens DHCP entre terminal e AP
D_{DHCP_Server}	Atraso médio de processamento do servidor de DHCP
D_{EAP}	Atraso médio de troca de mensagens EAP entre terminal e AP
$D_{Handover}$	Atraso médio total do processo de *handover*
D_{HLR}	Atraso médio de processamento da rede SS7 e do HLR/AuC da rede WWAN (HPLMN)
D_{MH}	Atraso médio de processamento devido ao terminal
N_m	Número máximo de retransmissão
RTO_0	Valor inicial do temporizador de retransmissão do pacote
RTO_i	Valor do temporizador de retransmissão na i-nésima tentativa de transmissão do pacote
T	Atraso médio para transmitir um pacote
T'	Atraso de propagação fim a fim do pacote

1 – INTRODUÇÃO

A evolução verificada nos últimos anos no campo das telecomunicações tem tido um forte componente de mobilidade. Desde a última década do século passado podemos ver o expressivo crescimento na oferta e na adoção de serviços de telecomunicações móveis pelos usuários finais, sendo o exemplo mais evidente dado pela penetração de terminais móveis celulares, que em alguns países e regiões já passa de 100%.

Diferentes tecnologias de rede sem fio têm sido desenvolvidas para cobrir as diversas necessidades de comunicação, baseado principalmente no raio de abrangência propiciada pelas mesmas. Desta forma, as redes WWAN (*Wireless Wide Area Network*) para a cobertura de regiões extensas, WLAN (*Wireless Local Area Network*) para instalações locais e WPAN (*Wireless Personal Area Network*) com cobertura pessoal, têm evoluído de forma contínua e distinta.

Mais recentemente temos visto também o desenvolvimento de serviços de dados combinados com mobilidade, iniciando pelos serviços de rede celular, através das tecnologias de 2G, 3G e 3,5G/4G, e passando pelos serviços de rede local sem fio (WLAN). Estas tecnologias têm permitido a disseminação da oferta e a utilização de serviços de dados por usuários em trânsito e, também, a simplificação da instalação de novas redes no ambiente dos clientes.

A evolução continua com a adoção de novas tecnologias de acesso sem fio com taxas de transmissão mais elevadas, melhor eficiência espectral e melhor qualidade no enlace, tais como IEEE 802.16 (WiMAX), HSPA (*High Speed Packet Access* - definido pelo 3GPP – *3G Partnership Project – http://www.3gpp.org*), e LTE (*Long Term Evolution* - em definição pelo 3GPP). Estes últimos focados em redes WWAN. E também pela evolução das redes WLAN, com a adoção de novos padrões, tais como o IEEE 802.11n.

A oferta de redes móveis sem fio de dados também propiciou a evolução dos serviços passíveis de serem prestados. Serviços de dados multimídia em tempo real, tais como vídeo *streaming*, vídeo conferência, telefonia IP e outros podem ser ofertados sobre as redes sem fio mais recentes sem os problemas de qualidade enfrentados pelas primeiras tecnologias.

Tecnologias voltadas para a evolução de redes e oferta de serviços de telecomunicações sobre rede de dados estão sendo utilizadas também sobre os novos acessos sem fio. O exemplo mais evidente é a adoção do protocolo de controle de sessão SIP [14], padronizado pelo IETF (*Internet Engineering Task Force – http://www.ietf.org*), como base da arquitetura de serviços multimídia IMS [3], desenvolvido pelo 3GPP para as redes móveis de terceira geração.

A abrangência na oferta de novos serviços gerou também a demanda para manter o usuário sempre conectado, não importando a rede ou tecnologia de acesso sendo utilizada. Esta demanda propiciou o desenvolvimento de terminais móveis com múltiplas *interfaces* de rede sem fio. Inicialmente somente com diferentes tecnologias de acesso celular, como por exemplo: tecnologia analógica AMPS (*Advanced Mobile Phone System*) e digital TDMA, passando pela incorporação de diferentes bandas de frequência utilizadas pela mesma tecnologia, até chegar à utilização de tecnologias WWAN, WLAN e PAN no mesmo dispositivo móvel. Atualmente não é incomum encontrar terminais móveis com diferentes tecnologias WWAN (por exemplo: GSM e UMTS), WLAN (por exemplo: IEEE 802.11b/g) e WPAN (por exemplo: Bluetooth e IR – "Infrared") incorporados no mesmo elemento físico.

A adoção da arquitetura IMS e de outras arquiteturas que permitem a oferta centralizada de serviços de forma independente da tecnologia da rede de acesso estendeu a demanda de manter o usuário sempre conectado para incluir a manutenção transparente do acesso ao serviço. Desta forma, o modelo atual em desenvolvimento prevê a manutenção do usuário conectado ao serviço, independente da rede de acesso utilizada. Isso significa que a transferência de conexão entre as redes de acesso sem fio, ou *handover*, não deve afetar a conectividade e qualidade do serviço sendo utilizado.

O primeiro movimento no sentido de manter a conectividade do serviço sendo oferecido ao terminal foi iniciado com a definição do *Mobile IP* (MIP) [72] pelo IETF no final do século passado, anteriormente à própria definição da arquitetura IMS pelo 3GPP. Outras tentativas também foram realizadas, como a proposta de utilização de procedimentos baseados no protocolo SIP por Schulzrinne em [15]. Todas estas propostas focam no restabelecimento da conectividade da sessão de dados, ou ao servidor responsável

(*correspondent node*), após o terminal alterar o ponto de conexão na rede, seja através de um *handover* horizontal, mantendo a tecnologia de acesso, ou através de um *handover* vertical, em que há troca da tecnologia de acesso [59]. Estas soluções não focam nos procedimentos de gerência de mobilidade [58], incluindo o procedimento de *handover* e os procedimentos de conexão e autenticação na nova rede.

A crescente oferta de serviços de voz e multimídia sobre sessões de dados em redes sem fio determinou a necessidade de otimização dos procedimentos de gerência de mobilidade, com a finalidade de reduzir o tempo de indisponibilidade da conexão do terminal móvel à rede, e em última instância ao serviço. O objetivo final é a manutenção da percepção da qualidade do serviço pelo usuário final, de tal forma que a sua experiência com o serviço não seja alterada pelo fato do terminal móvel ter realizado um *handover* vertical.

A manutenção da conexão ao serviço de forma transparente ao usuário significa também que os procedimentos realizados durante o *handover* sejam os mais automáticos possíveis. Nas redes móveis celulares existem mecanismos estabelecidos para permitir a seleção de rede, o *handover* e a autenticação de forma automática e transparente, sem conhecimento pelo usuário. As redes WLAN inicialmente não possuíam este mecanismo, necessitando a seleção e configuração da rede pelo usuário, principalmente no caso de existir a necessidade de autenticação do terminal móvel. Este fato torna a associação a novas redes WLAN um processo demorado e manual, o que impede a realização de *handover* vertical de forma transparente ao usuário e também impede o desenvolvimento de modelos simples de terminais móveis capazes de *roaming* entre redes WLAN distintas.

Com a evolução das redes WLAN foram criados protocolos [10][28], procedimentos [7] e arquiteturas [4] para permitir a autenticação de terminais móveis nas redes WLAN através do uso das credenciais já existentes para as redes WWAN. Com estas soluções é possível o acesso dos terminais móveis aos serviços da rede WWAN caseira quando conectado em redes WLAN [4] e o desenvolvimento de modelos e arquiteturas de *roaming* automático de terminais entre redes WLAN de diferentes prestadores de serviço [65]. Estes modelos funcionam de forma similar ao que já ocorre hoje, por exemplo, entre as redes GSM comerciais ofertadas pelas operadoras de telefonia móvel.

Contudo, as soluções de autenticação desenvolvidas não consideraram as necessidades de qualidade de serviço (QoS) associadas ao *handover* vertical de terminais móveis utilizando aplicações multimídia em tempo real, tais como voz e vídeo. As arquiteturas propostas podem apresentar tempos de interrupção do serviço incompatíveis com as características dos serviços durante o procedimento de *handover* e, principalmente, devido ao procedimento de autenticação. Esta disrupção no serviço não se confunde com o QoS disponível em cada rede individual envolvida no processo de *handover* descrito.

Um dos objetivos deste trabalho de dissertação é demonstrar as afirmações acima e, com base nos resultados obtidos, desenvolver soluções para permitir a otimização do procedimento de autenticação e conexão em redes WLAN pelos terminais móveis. O objeto final alcançado é uma proposta de arquitetura capaz de realizar autenticação do terminal móvel sem gerar interrupção perceptível no serviço acessado pelo usuário final durante o processo de *handover* vertical.

Este trabalho está dividido em capítulos com a seguinte sequência. Inicialmente são descritos no capítulo 2 as diferentes arquiteturas de rede WWAN para a oferta de serviços de voz, dados e multimídia. Este capítulo trata principalmente as redes definidas pelo organismo de padronização 3GPP, por serem estas as redes comerciais de maior abrangência no mercado internacional. As redes WLAN são descritas no capítulo 3, com foco nas características principais das diversas tecnologias de acesso definida para as redes IEEE 802.11 [31]. As redes WPAN não serão referenciadas neste trabalho.

No capítulo 4 são definidos os conceitos de gerência de mobilidade [58] que são utilizados durante este trabalho. Neste capítulo são tratados os conceitos de gerência de localização, incluindo a autenticação e os conceitos de gerência de *handover*, incluindo a classificação dos diferentes tipos de *handover*.

O capítulo 5 descreve como os conceitos definidos no capítulo anterior são aplicados nas redes WWAN e WLAN. Neste capítulo são também introduzidos os conceitos de autenticação utilizados nas redes WWAN e também utilizados nas redes WLAN, através da definição dos protocolos EAP-SIM e EAP-AKA padronizados pelo IETF e utilizados nos padrões definidos pelo 3GPP e IEEE. A evolução nos padrões de conexão, segurança e autenticação nas redes WLAN advindos com as especificações IEEE 802.1x [7] e IEEE

802.11i [32] são também descritos. O capítulo termina com uma discussão dos modelos de arquitetura definidos atualmente para *roaming* e *interworking* de redes WLAN e WWAN e com a descrição dos padrões que estão em elaboração pelo IETF e IEEE para auxiliar o *handover* e autenticação em redes heterogêneas.

O estudo de caso realizado é apresentado no capítulo 6. Neste estudo foi selecionada uma das arquiteturas para autenticação de redes WLAN compatível com os modelos de *roaming* e *handover* vertical definidos pela indústria. A arquitetura selecionada foi modelada analiticamente com dados obtidos através de medidas em soluções equivalentes implantadas em rede comercial. Os resultados obtidos para diversas condições de rede foram analisados e comparados com os limites necessários para garantir a qualidade na oferta de serviços multimídia em tempo real.

No capítulo 7 são apresentadas soluções para as causas principais do atraso evidenciado pelo estudo realizado no capítulo anterior. Duas soluções são propostas, uma para otimizar o procedimento de conexão na rede WLAN e outra, uma nova arquitetura que altera o procedimento de autenticação, de forma a permitir que a mesma seja realizada sem afetar o tempo de indisponibilidade do serviço.

O trabalho é então concluído no capítulo 8 onde também são apresentadas sugestões de trabalhos futuros baseados nas propostas realizadas pelo presente trabalho.

A nova arquitetura proposta no capítulo 7, dado ao seu ineditismo, foi depositada junto ao INPI (Instituto Nacional de Propriedade Industrial) como o pedido de patente 'PI0902036-5A2' sob o nome de "Sistema e método de autenticação para interconexão de redes sem fio heterogêneas", conforme publicada na Revista da Propriedade Industrial nº 2092 em 08 de Fevereiro de 2011. As medidas e modelagens realizadas neste trabalho foram feitas entre os meses de Fevereiro e Outubro de 2007.

2 – REDES MÓVEIS WWAN

Uma rede *Wireless Wide Area Network* (WWAN) é definida como rede sem fio com abrangência geográfica extensa, geralmente cobrindo um estado ou país, e que utilizam tecnologia celular para permitir a mobilidade dos terminais.

As redes WWAN comerciais com maior abrangência mundial são baseadas nas tecnologias GSM e UMTS, conforme informação do GSMA (*http://www.gsmworld.com/technology/3g/statistics.shtml*). Ambas as tecnologias e soluções são definidas e mantidas pelo organismo de padronização internacional 3GPP. O 3GPP define os padrões para redes móveis de terceira geração baseados em UMTS (*Universal Mobile Telecommunication System*), e suas evoluções, e é também responsável por manter os padrões de segunda geração baseados em tecnologia GSM e GPRS.

Os padrões do 3GPP focam todos os aspectos relativos ao fornecimento de serviços pelas redes WWAN, incluindo a definição de arquiteturas para oferta de serviços avançados e as integrações com os servidores de aplicação responsáveis por hospedar as lógicas dos serviços. As definições principais da arquitetura e elementos especificados pelo 3GPP para redes WWAN e para a oferta de serviços de voz, dados e multimídia são descritas neste capítulo.

2.1 - SISTEMAS 3GPP – DOMÍNIOS CS E PS

Esta seção descreve a configuração, as entidades funcionais e *interfaces* de uma rede móvel terrestre PLMN (*Public Land Mobile Network*) baseada nos padrões definidos pelo organismo de padronização internacional 3GPP.

O 3GPP em [21] define os requisitos e arquiteturas para diferentes tecnologias das redes de acessos (GSM e 3G) e para os domínios de comutação de circuito, CS (*Circuit Switched*), de comutação de pacote, PS (*Packet Switched*), e de multimídia, IMS (*IP Multimedia Subsystem*).

As especificações definidas pelo 3GPP são divididas em séries e cada série descreve um assunto em particular, conforme descrito em *http://www.3gpp.org/specs/numbering.htm*.

As especificações são numeradas com 4 ou 5 dígitos numéricos, sendo que os dois primeiros definem a série. As versões principais dos documentos são divididas em *releases*, sendo que até 1999 estas tinham como referência o ano (por exemplo: R98, R99). A partir de 2000 os *releases* foram numerados, iniciando pelo dígito 4 (por exemplo: Rel-4, Rel-5, etc.), e a periodicidade de publicação não foi mais vinculada ao ano calendário. Após a publicação um *release* ele pode ainda sofrer modificações técnicas e editoriais que são referenciadas em um código de versão adicional de 3 dígitos. O *Release* 7 foi o último publicado pelo 3GPP e o *Release* 8 está atualmente em discussão.

Os sistemas e arquiteturas definidos pelo 3GPP possuem interoperabilidade de serviços entre os diversos *releases* e buscam compartilhar os mesmos elementos de arquitetura, conforme é descrito nos itens subsequentes.

2.1.1 – Rede Núcleo e Rede de Acesso

A infraestrutura das redes 3GPP é dividida em rede núcleo CN (*Core Network*) e em rede de acesso AN (*Access Network*). A CN é dividida em: domínio CS, domínio PS e subsistema IMS. A AN é chamada de BSS (*Base Station System*) para sistemas GSM e RNS (*Radio Network System*) para sistemas UMTS.

Até o *Release* 4 do 3GPP, a CN era constituída do domínio de comutação de circuito CS e do domínio de comutação de pacote PS. Estes dois domínios diferem pela maneira como suportam o tráfego de usuários. Eles também se sobrepõem e contêm algumas entidades comuns. Uma rede 3GPP pode implementar somente um domínio ou ambos, de acordo com a demanda de serviços e com o perfil de usuários.

2.1.2 - Domínios CS e PS

O domínio CS contempla o conjunto de todas as entidades da CN que oferecem conexão por comutação de circuito para tratamento de tráfego dos usuários, bem como, todas as entidades para suporte do sistema de sinalização correlato. Uma conexão por comutação de circuito é definida como uma conexão para a qual os recursos de rede são dedicados e alocados no estabelecimento da chamada e liberados somente ao término da conexão.

O domínio PS contempla o conjunto de todas as entidades da CN que oferecem conexão por comutação de pacote para tratamento de tráfego dos usuários, bem como, todas as entidades para suporte da sinalização correlata. Uma conexão por comutação de pacote transporta a informação de usuário pela concatenação de *bits* em pacotes de dados, de forma que cada pacote pode ser encaminhado de forma independente do precedente pela rede de transporte de dados, sem alocação de recursos dedicados durante a chamada, ou sessão de dados.

2.1.3 - *Interfaces* Padronizadas

Entre as entidades de rede definidas pelas especificações 3GPP [21] são definidas *interfaces* para troca de dados e sinalização. A cada *interface* definida são descritas as funções suportadas e os protocolos de comunicação necessários. A definição das *interfaces* pelo 3GPP permite que diferentes entidades, de diferentes fabricantes, possam ser interconectadas de forma transparente. A esta arquitetura que pode ser implementada de forma independente do fabricante é dada o nome de *multivendor*.

A figura 2.1 mostra a relação entre as entidades e as *interfaces* definidas para as redes 3GPP GSM e UMTS.

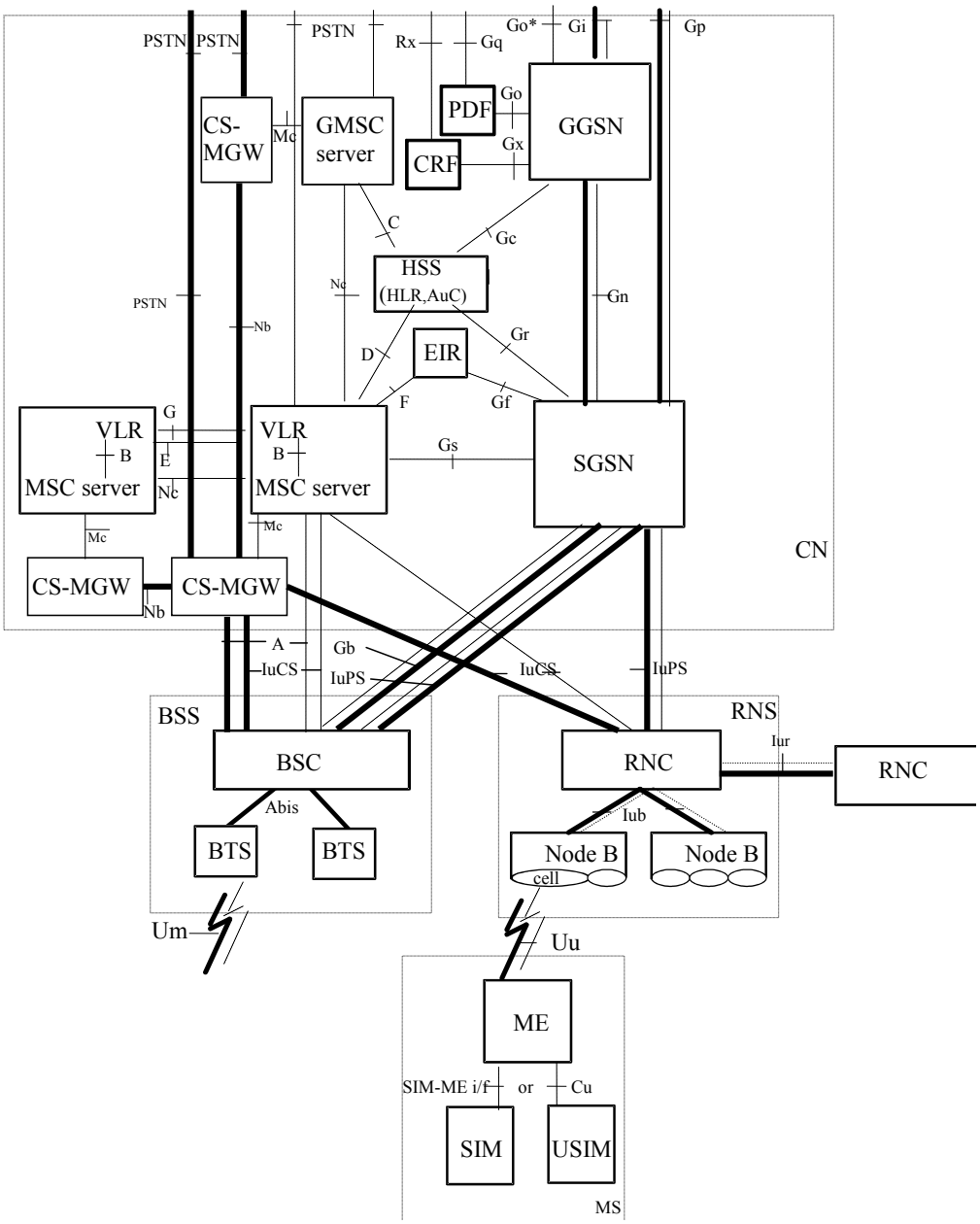


Figura 2.1 – Entidades e *Interfaces* em uma Rede GSM/UMTS (3GPP [21])

Não é objetivo de este trabalho detalhar cada *interface* e protocolo previsto para os sistemas 3GPP, mas somente os intrinsecamente necessários para o entendimento do objetivo proposto. Para descrição geral das *interfaces* deve ser consultada a especificação 3GPP TS 23.002 [21], para detalhes específicos das *interfaces* e protocolos devem ser consultadas as especificações das séries 24 e 28 do 3GPP (disponíveis em *http://www.3gpp.org/ftp/Specs/archive/*).

2.1.4 – Entidades da Rede Núcleo

A seguir, são descritas sumariamente as entidades funcionais da Rede Núcleo CN segundo 3GPP [21]. A implementação física destas entidades pode ser feita de forma distribuída ou integrada, sendo que, mesmo em caso de implementação integrada de duas entidades lógicas distintas deve ser também implementado e permitido o acesso à *interface* padrão entre elas para manter a aderência ao padrão.

a) HLR (*Home Location Register*)

O HLR é uma base de dados de registro de localização, na qual os assinantes são subscritos para propósito de gravação de informações, tais como:

- Informação de subscrição;
- Informação de localização: para permitir a tarifação e o encaminhamento de chamadas dentro dos domínios CS e PS, para as entidades de controle onde o UE (*User Equipment*) está registrado.

As seguintes funcionalidades são partes do escopo de operação do HLR:

- Prover suporte para entidades do domínio PS tais como SGSN e GGSN, através das *interfaces Gr* e *Gc*. A finalidade é prover informações às entidades de rede para acesso dos assinantes aos serviços do domínio PS.
- Prover suporte para entidades do domínio CS tais como MSC/MSC Server e GMSC/GMSC Server, através das *interfaces C* e *D*. A finalidade é prover informações às entidades de rede para acesso dos assinantes aos serviços do domínio CS.

O protocolo de comunicação utilizado pelas *interfaces* com o HLR é o *Mobile Application Part* (MAP), uma extensão específica para redes móveis da sinalização SS7, usada para comunicação entre elementos da rede CN e entre diferentes PLMN, conforme definido pelo 3GPP em [51]. O protocolo MAP é transportado sobre a pilha de protocolos *Transaction Capabilities Application Part* (TCAP), *Signaling Connection Control Part* (SCCP) e *Message Transfer Part* (MTP), todos definidos pelo ITU-T em [52], [53] e [54].

A após o *Release* 5 das especificações do 3GPP, o HLR é considerado como um subconjunto funcional da entidade HSS (*Home Subscriber Server*) que é definido como um dos elementos funcionais do domínio IMS.

b) AuC (*Authentication Centre*)

A partir do *Release* 5 das especificações do 3GPP, o *Authentication Centre* (AuC) pode ser considerado como um subconjunto do elemento HSS definido para o domínio IMS.

O AuC é geralmente fisicamente associado a um HLR/HSS e é responsável por armazenar uma chave de identidade para cada assinante vinculado àquele HLR/HSS. Esta chave é utilizada para gerar os dados de segurança únicos para cada assinante móvel, dentro do domínio CS e PS, com o objetivo de:

- Autenticar o *SIM Card* instalado no equipamento do usuário ou estação móvel;
- Verificar a integridade da comunicação sobre o link de rádio entre o equipamento de usuário e a rede;
- Cifrar a comunicação sobre o link de rádio entre o equipamento de usuário e a rede.

A comunicação entre HLR e AuC é feita por *interface* não padronizada e específica para cada diferente fabricante de equipamentos. As mensagens de requisição de autenticação e de resposta do AuC para os demais elementos da rede CN são realizadas via protocolo MAP [51] a partir do elemento HLR.

No capítulo 5 deste documento são descritos os métodos de autenticação existentes nas redes GSM e UMTS e implementados no AuC.

c) VLR (*Visitor Location Register*)

O VLR é uma base de dados local responsável por controlar os registros de localização das estações móveis em determinada área, chamada de área de localização. Uma estação móvel em *roaming* em uma dada área de localização é controlada por um VLR. Quando uma estação móvel entra em uma nova área de localização ele deve iniciar um novo

procedimento de registro. A central MSC responsável por aquela área transfere para o VLR a identidade da área de localização onde a estação móvel está situada. Caso a estação móvel não esteja registrada ainda no VLR há uma troca de informações entre o VLR e o HLR para permitir o tratamento apropriado das chamadas recebidas pela estação móvel.

Um dado VLR pode ser responsável por uma ou mais áreas de MSC, mas a configuração prática mais usual é a existência de elementos VLR co-locados ou integrados nas centrais MSC.

O VLR contém também na sua base de dados informações necessárias para tratar as chamadas originadas e recebidas pela estação móvel. Para alguns serviços suplementares o VLR pode ter que buscar informações adicionais no HLR chamada a chamada. Os seguintes elementos de dados podem estar incluídos na base do VLR:

- *International Mobile Subscriber Identity* (IMSI) da estação móvel;
- *Mobile Station International ISDN Number* (MSISDN) da estação móvel;
- *Mobile Station Roaming Number* (MSRN) da estação móvel, ver [1] para descrição dos princípios de alocação do número MSRN;
- *Temporary Mobile Station Identity* (TMSI) da estação móvel, caso aplicável;
- A área de localização onde a estação móvel está registrada;
- A identidade do SGSN onde a estação móvel está registrada. Somente aplicável em PLMN com suporte a GPRS e com implementação da *interface Gs* entre o MSC/VLR e o SGSN;
- A última localização conhecida e a localização inicial da estação móvel.

d) MSC (*Mobile-service Switching Centre*)

A MSC é uma central de comutação de serviços móveis e constitui a *interface* entre o sistema de rádio e a rede fixa de telefonia comutada. A MSC executa todas as funções necessárias para tratar os serviços de comutação de circuitos vindos de e direcionados para as estações móveis.

A MSC também executa todas as funções de sinalização e comutação para as estações móveis localizadas dentro de uma área geográfica designada. A principal diferença entre uma MSC e uma central de comutação convencional de uma rede de telefonia fixa comutada é que a MSC tem que levar em conta o impacto da alocação dos recursos de rádio e a natureza móvel dos assinantes. Adicionalmente, a MSC tem que realizar os seguintes procedimentos:

- Registro de localização conforme [22];
- *Handover* conforme [23].

Quando necessário, a MSC pode ser implementada em duas entidades diferentes: o MSC Server, responsável por tratar somente a sinalização e controle de chamadas, e o CS-MGW, tratando os dados de mídia e fluxos de dados do usuário. Uma MSC Server e um CS-MGW executam a totalidade de funcionalidades de uma MSC.

e) *MSC Server*

A *MSC Server* implementa somente as partes de controle de chamada e de mobilidade de uma MSC. A *MSC Server* é responsável pelo controle de chamadas originadas e terminadas dentro do domínio CS. Ela termina a sinalização de usuário-rede e a translada para a sinalização rede-rede relevante. Adicionalmente, a *MSC Server* pode também conter o elemento VLR.

As conexões de sinalização entre a *MSC Server* e os demais elementos do domínio CS pode ser realizada sobre rede de dados ATM ou IP, ao invés de enlaces comutados. A *MSC Server* utiliza o elemento CS-MGW para controlar a parte do estado da chamada referente ao controle de conexão para os canais de mídia.

f) CS-MGW (*Circuit Switched – Media Gateway Function*)

O CS-MGW é o ponto de terminação de transporte de mídia para demais redes fixas e móveis em uma rede PLMN definida e *interface* para rede de acesso móvel (AN) sobre o ponto de referência *Iu*, no caso de redes UMTS.

Um CS-MGW pode terminar canais de mídia vindos de uma rede de comutação de circuitos e fluxos de mídia vindos de uma rede de pacotes, tal como fluxo RTP sobre rede IP. Sobre a *interface Iu*, o CS-MGW pode suportar conversão de mídia, controle de *bearer* e processamento de *payload* (por exemplo: processamento de *codec*, cancelamento de eco e conferência). O CS-MGW suporta diferentes opções de protocolos de transporte na *interface Iu* para os serviços do domínio CS, tais como, AAL2/ATM bem como RTP/UDP/IP.

O CS-MGW é responsável também por:

- Interagir com elementos MGCF, *MSC Server* e GMSC Server para receber sinalização para controle de recursos;
- Possuir e tratar recursos tais como canceladores de eco, transcodificação, etc.

g) *Gateway MSC*

Quando uma rede de telefonia qualquer não pode interrogar o HLR diretamente ela encaminha a chamada para a PLMN caseira do usuário, esta chamada é então direcionada para uma MSC específica da PLMN. Esta MSC interroga o HLR apropriado e então encaminha a chamada para a MSC de destino onde a estação móvel está localizada. A MSC que executa as funções de interrogar o HLR no recebimento de chamadas e encaminhar a chamada para a posição real da estação móvel é chamada de *Gateway MSC* (GMSC).

Quando necessário, a GMSC pode ser implementada em duas entidades diferentes: o *GMSC Server*, responsável por tratar somente as funções de sinalização e controle, e o CS-MGW, tratando os dados de usuário e fluxos de mídia. Uma *GMSC Server* e um CS-MGW são equivalentes em funcionalidade a uma GMSC.

h) SGSN (*Serving GPRS Supporting Node*)

O SGSN é o elemento central no domínio PS. Ele controla o estabelecimento de sessões de dados pelas estações móveis e contém dois tipos de informações relacionadas às estações móveis sobre seu controle: de subscrição e de localização.

Informações de subscrição:

- IMSI da estação móvel;
- Identidades temporárias da estação móvel;
- Endereços PDP (*Packet Data Protocol*).

Informações de localização:

- A célula onde a estação móvel está registrada;
- Número do VLR;
- Endereço de GGSN para cada GGSN para o qual existe um contexto PDP ativo.

O SGSN conecta com a rede de acesso em um sistema UMTS através da *interface IuPS*. As demais conexões entre o SGSN com os elementos da rede UMTS estão mostradas na figura 2.1.

i) GGSN (*Gateway GPRS Support Node*)

O GGSN pertence ao domínio PS e corresponde funcionalmente ao GMSC. A diferença é que enquanto o GMSC somente encaminha o tráfego entrante, o GGSN tem de executar o roteamento do tráfego entrante e sainte. Ele deve manter informações de subscrição e de localização, que são recebidas através do HLR e dos elementos SGSN.

Informações de subscrição mantidas:

- IMSI da estação móvel;
- Endereços PDP.

Informações de localização mantidas:

- Endereço de SGSN dos SGSN onde as estações móveis estão registradas.

2.1.5 – Entidades da Rede de Acesso

Radio Network System (RNS) é a rede de acesso definida pelo 3GPP para sistemas UMTS, e a *Base Station System* (BSS) é a rede de acesso definida para sistemas GSM/GPRS. Os elementos da rede CN são capazes de interligar com redes de acessos distintas para atender diferentes *interfaces* aéreas. A seguir são descritas sumariamente as entidades da rede de acesso para o sistema UMTS. A figura 2.1 mostra a relação entre estas entidades e as *interfaces* definidas.

a) RNC (*Radio Network Controller*)

O RNC controla um ou mais *Node B* em uma rede de acesso UMTS. Ele pode ser conectado através da *interface Iu* com a MSC (*IuCS*) ou com o SGSN (*IuPS*). A *interface* entre diferentes RNC (*Iur*) é uma *interface* lógica e não necessariamente existe uma conexão física direta. A RNC é comparável ao elemento BSC (*Base Station Controller*), e a *interface A* é a *interface* entre a MSC e a BSS, em uma rede GSM/GPRS.

As funções executadas pela entidade RNC incluem:

- Gerência de recursos de transporte da *interface Iub*;
- Controle de recursos lógicos de O&M do *Node B*;
- Gerência de tráfego dos canais comuns;
- Diversidade macro pela combinação/separação de fluxos de dados transferidos entre diversos *Node B*;
- Procedimentos para *soft handover*;
- Alocação de códigos de canalização de DL;
- Controle de potência de *uplink*;
- Controle de potência de *downlink*;
- Controle de admissão;
- Gerência de tráfego de canais compartilhados.

c) MS (*Mobile Station*)

O MS consiste do equipamento físico que pode ser utilizado por um assinante da rede PLMN. A *interface* entre o MS e a rede WWAN é realizada através da *interface* rádio, adicionalmente, o MS também contém:

- *Mobile Equipment* (ME) – podendo ser dividido em vários componentes e grupos funcionais, conforme definido na especificação 3GPP TS 23.101 [55];
- *Subscriber Identity Module* (SIM) também chamado de UMTS *Subscriber Identity Module* (USIM) nos *releases* superiores ao R99 do 3GPP – o cartão SIM armazena todas as informações necessárias para transformar um ME em um MS, com os privilégios e credenciais do assinante. Cada SIM possui uma identificação única chamada de *International Mobile Subscriber Identity* (IMSI).

Nas especificações atuais do 3GPP o termo MS tem sido substituído pelo termo UE (*User Equipment*) utilizado de forma mais abrangente nas redes UMTS [55]. No presente documento serão utilizados de forma indistinta os termos estação móvel e terminal (ou terminal móvel) como referência ao MS.

2.2 – SISTEMAS 3GPP – DOMÍNIO IMS

Com o Release 5 do 3GPP foi introduzido um novo domínio de rede, chamado de *IP Multimedia Subsystem* (IMS) [3], [66]. Este domínio permite o suporte a serviços multimídia de tempo real sobre rede IP. Em conjunto com o domínio PS e a rede de acesso GPRS/EDGE/WCDMA, o domínio IMS permite que serviços fim a fim baseados em protocolo IP sejam ofertados com seus recursos próprios de segurança, autenticação e qualidade de serviço (QoS) [66].

Os requisitos funcionais para o desenvolvimento do IMS definem o modelo arquitetural criado para a entrega de serviços multimídia IP para usuários finais. O IMS deve atingir os seguintes requisitos [67]:

a) Suporte para o estabelecimento de sessões multimídia IP;

b) Suporte a mecanismo para negociar qualidade de serviço (QoS);

c) Suporte ao interfuncionamento com a Internet e redes comutadas de circuitos;
d) Suporte a *roaming*;
e) Suporte ao controle pela operadora dos serviços entregues aos usuários finais;
f) Suporte a rápida criação de serviços sem a necessidade de padronização dos mesmos;
g) Suporte diferentes redes de acesso, além das definidas pelo 3GPP.

Além dos requisitos funcionais acima, no desenvolvimento do IMS se procurou reutilizar os protocolos definidos por outros organismos de padronização, tais como IETF e ITU-T, com o objetivo de reduzir custos e acelerar o processo de desenvolvimento [67]. Os principais protocolos do IETF utilizados são: SIP, SDP, RTP e *Diameter*. Do ITU-T foram reutilizados principalmente os protocolos: BICC, ISUP e H.248.

O protocolo SIP [14] foi definido como o protocolo de controle de sessões para o IMS. O fato de o protocolo SIP ter sido desenvolvido baseado no HTTP torna fácil a sua utilização por programadores para o desenvolvimento de novos serviços [67].

Na definição da arquitetura do IMS foram padronizadas funções e *interfaces* entre as mesmas. As implementações práticas da arquitetura são livres para integrar as funções em um ou vários nós, ou elementos físicos. A figura 2.2 mostra uma visão geral da arquitetura, conforme padronizada pelo 3GPP. A lista completa das *interfaces* definidas pode ser encontrada em [21].

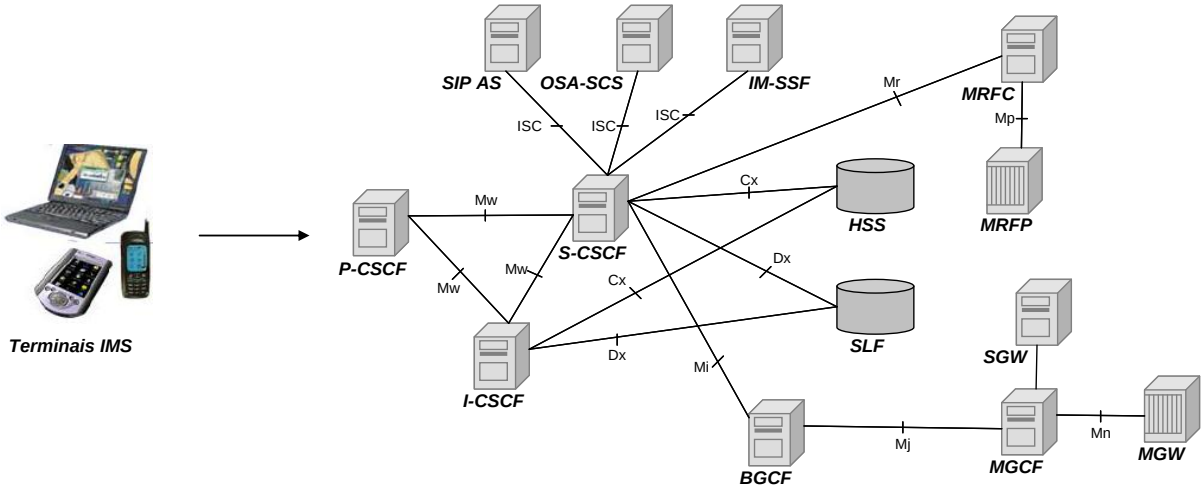


Figura 2.2 – Arquitetura geral do IMS (Camarillo, modificado [67])

Na figura 2.2 é mostrado o terminal IMS, ou *User Equipment* (UE), segundo a terminologia do 3GPP. Em redes 3GPP o terminal IMS se conecta através da rede GPRS (domínio PS) utilizando o enlace rádio da rede de acesso. O terminal IMS pode também utilizar redes não definidas pelo 3GPP para se conectar ao domínio IMS, tais com redes WLAN e redes de acesso fixo de banda larga.

Os elementos principais da rede núcleo do IMS são também mostradas na figura 2.2.

As bases de dados definidas para o IMS são o *Home Subscriber Server* (HSS) e o *Subscription Locator Function* (SLF). O HSS é o repositório central para informações relativas ao usuário, pode ser definido como uma evolução do HLR da rede GSM e engloba todas as funções definidas para este último e as específicas para o controle de autenticação, autorização, localização e serviços dos usuários IMS. O SLF é um banco de dados simples com o objetivo de mapear as identificações dos usuários ao HSS específico que hospeda as suas informações, este elemento é utilizado em redes que implementam mais de um HSS distinto.

O *Call/Session Control Function* (CSCF) é um servidor SIP e uma das funções essenciais de controle na arquitetura IMS. Dependendo da função que executa, o CSCF pode ser dividido em três tipos [67]:

a) *Proxy-CSCF* (P-CSCF): age como um servidor SIP *Proxy* [14] de entrada e saída e é o primeiro ponto de contato da sinalização do terminal na rede IMS. O P-CSCF executa funções de segurança, aplica políticas de acesso e de QoS e realiza compressão/descompressão das mensagens SIP;

b) *Interrogating-CSCF* (I-CSCF): é um servidor SIP *Proxy* na borda do domínio administrativo do IMS, seu endereço é listado nos registros do domínio no servidor DNS (*Domain Name System*). O I-CSCF possui também *interface* baseada em protocolo *Diameter* [41] com os elementos SLF e HSS para recuperar informação de localização e encaminhamento da sinalização do usuário. O I-CSCF pode cifrar de forma segura partes da mensagem SIP que tem informações sensíveis sobre a topologia do domínio IMS, antes de enviá-la para outras redes;

c) *Serving-CSCF* (S-CSCF): é um servidor SIP que também possui a função de SIP *registrar* [14]. O S-CSCF possui também *interface Diameter* com o HSS para recuperar os vetores de autenticação e o perfil de serviços do usuário. O S-CSCF dispara a sinalização

SIP para os serviços registrados pelo usuário, hospedados em servidores de aplicações, antes de encaminhá-las para o destino final.

O servidor de aplicação ou AS (*Application Server*) é uma entidade SIP que executa e hospeda os serviços da rede IMS. Três tipos de AS são definidos [67] para o IMS:
a) SIP AS: servidor de aplicação baseado em SIP e responsável por hospedar serviços desenvolvidos exclusivamente para o IMS;
b) *Open Service Access-Service Capability Server* (OSA-SCS): servidor de aplicação com *interface* para serviços em servidores de aplicações que implementam as *interfaces* de programação que seguem o padrão OSA, definido pelo 3GPP [68];
c) *IP Multimedia Service Switching Function* (IM-SSF): servidor de aplicação especializado que permite reutilização de serviços da rede GSM baseados no padrão CAMEL [67].

O *Media Resource Function* (MRF) foi definido para prover funções de mídia tais como: tocar anúncios, misturar fluxos de mídia, realizar transcodificação de *codecs*, etc. O MRF é dividido em *Media Resource Function Controller* (MRFC) para as funções de sinalização e no *Media Resource Function Processor* (MRFP) para executar as funções de mídia [67].

O *Breakout Gateway Control Functions* (BGCF) é um servidor SIP que realiza encaminhamento baseado em números telefônicos para sessões destinadas às redes de circuito comutado.

Para realizar *interface* com a rede de circuito comutada, tais como a rede de telefonia fixa legada e o domínio CS da rede GSM, o IMS define algumas funções específicas [67]:
a) *Signaling Gateway* (SGW): faz *interface* com o plano de sinalização do domínio CS e converte as camadas inferiores da sinalização SS7 [33] para o equivalente IP;
b) *Media Gateway Control Function* (MGCF): realiza o controle de chamadas destinadas e recebidas do domínio CS, a conversão da sinalização SIP para SS7 e o controle de recursos no elemento MGW através do protocolo H.248 [67];
c) *Media Gateway* (MGW): realiza a *interface* entre o plano de mídia da rede IMS, baseada em protocolo IP, com o plano de mídia de redes de circuito comutado [67].

3 – REDES SEM FIO WLAN

Uma rede *Wireless Local Area Network* (WLAN) pode ser definida como uma rede sem fio de abrangência local, geralmente cobrindo áreas que variam de pequena porção de um edifício até um campus. Algumas das tecnologias de WLANs podem possuir taxas de transmissão de dados maiores que as das redes WWAN baseadas nas tecnologias definidas pelo 3GPP.

A grande totalidade das redes WLANs disponíveis são baseadas no conjunto de padrões 802.11 [31] definidos pelo *Institute of Electrical and Electronics Engineers* (IEEE). A grande aceitação das redes 802.11 deve também ao fato destes padrões possuírem um programa de certificação promovido pela associação de fabricantes de equipamentos e softwares para redes 802.11, conhecido com *Wi-Fi Alliance* (WFA), e que tem como objetivo promover a adoção e evolução da tecnologia e garantir a compatibilidade entre equipamentos de diferentes fabricantes.

3.1 - SISTEMAS IEEE 802.11 / Wi-Fi

O padrão IEEE 802.11 [31] especifica a *interface* aérea entre o elemento de acesso chamado de *Access Point* (AP) e um terminal, ou entre dois terminais. O padrão originalmente publicado define a subcamada de controle de acesso ao meio *Media Access Control* (MAC) [56], incluindo os protocolos de gerenciamento e serviços da subcamada MAC e três camadas físicas: infravermelho, *Frequency Hopping Spread Spectrum* (FHSS) na faixa de 2,4 GHz e *Direct Sequence Spread Spectrum* (DSSS) também na faixa de 2,4 GHz [31].

A subcamada MAC do padrão 802.11 define o mecanismo de acesso ao meio chamado de Função de Coordenação Distribuída (DCF - *Distributed Coordination Function*) [31]. Este mecanismo fundamental implementa um esquema de acesso randômico, baseado no protocolo CSMA/CA (*Carrier Sense Multiple Access*/ *Collision Avoidance*) [56].

A faixa de 2,4 GHz é não licenciada, ou seja, tem uso livre, e é conhecida também como banda *Industrial Scientific and Medical* (ISM) [16]. Esta faixa é também utilizada por sistemas com tecnologia *Bluetooth* e algumas tecnologias de telefones sem fio.

Para a camada física do 802.11, foram desenvolvidas diferentes especificações englobando diferentes faixas de frequência e taxas de transmissão [31]:

a) 802.11

Padrão original publicado em 1997 e que suporta taxas de transmissão de 1 ou 2 Mbps, operando na faixa de 2,4 GHz (ISM).

b) 802.11b

Publicado em 1999 como um suplemento ao padrão 802.11 original [16], especificando o uso adicional das taxas de 5,5 e 11 Mbps, e também operando na faixa de frequência de 2,4 GHz (ISM). Este padrão utiliza a mesma subcamada MAC do padrão 802.11 original.

c) 802.11a

Outro suplemento ao padrão 802.11 também publicado em 1999. Este padrão suporta taxas de transmissão de 6, 9, 12, 18, 36 e 54 Mbps, utiliza a subcamada MAC original e define uma nova faixa de frequência de 5 GHz, com um sistema OFDM (*Orthogonal Frequency Division Multiplexing*). Esta faixa de frequência de 5 GHZ também é não licenciada e é conhecida como banda *Unlicensed National Information Infrastructure* (UNII) [16].

d) 802.11g

Publicado em 2003 como um suplemento ao padrão original, o 802.11g oferece taxas equivalentes ao padrão 802.11a, suporta 6, 9, 12, 18, 24, 36, 48 e 54 Mbps adicionalmente às taxas do padrão original, utiliza a subcamada MAC original e mantém a mesma faixa de frequência de 2,4 GHz do padrão 802.11b, mas com a utilização de OFDM. O padrão 802.11g possui modo de operação compatível com o 802.11b [16] [34].

e) 802.11n

Publicado em 2009 como um suplemento ao padrão original, o 802.11n aumentou de forma significativa a taxa de transmissão pela adição de MIMO (*Muliple-Input Multiple-Output*) e canais de 40 MHz na camada física (PHY) e pela agregação de quadro na camada MAC [79].

O IEEE continua o trabalho de definição de outros suplementos com objetivo de definir novas camadas físicas e melhorias em funcionalidades, tais como segurança e gerência (*http://grouper.ieee.org/groups/802/11/PARs*).

3.1.1 – Arquitetura 802.11

A base da arquitetura IEEE 802.11 é conhecido como *Basic Service Set* (BSS) [31]. O BSS é definido como um conjunto de terminais, ou estações (STA) em uma área em que podem ser comunicar entre si [16].

Múltiplas BSS podem ser interconectadas via um componente da arquitetura chamado de *Distribution System* (DS) [31]. O DS permite suporte à mobilidade através de serviços lógicos necessários para manusear o mapeamento de endereços e integração transparente entre as múltiplas BSS [31]. A estação que provê acesso ao DS e suporta os serviços da DS é um *Access Point* (AP). Uma rede 802.11 que contém pelo menos um AP é chamada também de rede WLAN do tipo infraestrutura [16].

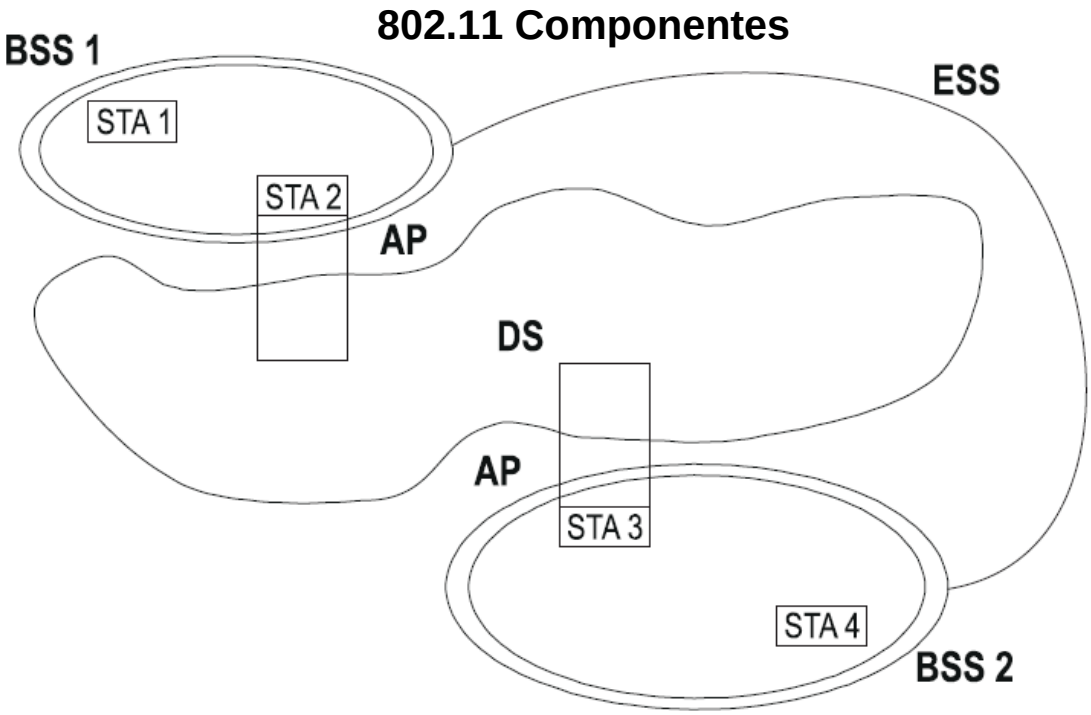


Figura 3.1 – Arquitetura 802.11 (IEEE, modificado [31])

O DS e as diversas BSS conectadas permitem a criação de redes 802.11 com praticamente qualquer tamanho e complexidade. A esta rede estendida é dado o nome de *Extended Service Set* (ESS) [31]. A figura 3.1 ilustra a arquitetura descrita.

As estações em uma rede 802.11 também podem comunicar entre elas sem a necessidade de um ponto centralizado de controle, tal como AP e DS. Neste caso a rede é chamada de *Independent Basic Set Service* (IBSS), ou rede *ad hoc* [16]. Neste cenário qualquer terminal pode estabelecer uma sessão de comunicação com outro terminal [56].

As redes ESS e IBSS são identificadas através do elemento de informação *Service Set Identifier* (SSID), composto de um campo que pode conter até 32 octetos de dados [31].

3.1.2 – Mecanismo de Acesso ao Meio

O DCF é o mecanismo fundamental de acesso ao meio do padrão IEEE 802.11, sendo um componente obrigatório na arquitetura. Nesta função os terminais devem competir entre si para obter acesso ao meio a cada transmissão de pacote, as retransmissões são gerenciadas

de acordo com uma regra exponencial de *backoff* [27][56], onde a cada retransmissão o tempo de *backoff* anterior é dobrado até um valor limite.

Existe um mecanismo opcional definido pelo padrão IEEE 802.11, chamado de *Point Coordination Function* (PCF). Neste mecanismo, indicado para dados com alta sensibilidade a atraso e *jitter*, o AP executa controle centralizado do canal e repassa esse controle aos terminais no momento apropriado [27]. O PCF não é adotado amplamente, devido a sua complexidade e ineficiência para os dados sem prioridade [56].

Duas técnicas são descritas pelo DCF para transmissão de pacotes. O mecanismo básico de acesso ao meio é baseado em uma técnica de *two-way handshaking* [56]. Este mecanismo é caracterizado pela transmissão imediata de uma confirmação positiva (ACK) pela estação de destino após o recebimento de um pacote transmitido pelo terminal de origem. A estação de origem somente tem certeza que o pacote alcançou o destino correto com o recebimento do pacote ACK.

O mecanismo básico de acesso não consegue evitar colisões causadas pelo fenômeno conhecido como terminal oculto [57], que ocorre quando dois terminais que não são capazes de se escutarem estão no alcance de um terceiro, os dois terminais são considerados ocultos entre si. Como estão ocultos, os dois primeiros terminais podem transmitir pacotes de forma simultânea, gerando colisão sobre o terceiro terminal.

O outro mecanismo definido para DCF é opcional e baseado em uma técnica de *four-way handshaking* conhecido como mecanismo *Request-To-Send/Clear-To-Send* (RTS/CTS). Uma estação operando em RTS/CTS envia sempre um quadro curto especial de RTS para reservar o canal, antes de transmitir um pacote. A estação de destino reconhece o recebimento do quadro RTS pelo envio de volta de um quadro CTS, após a recepção do CTS a transmissão normal do pacote e resposta via ACK ocorre. Neste caso a colisão pode ocorrer somente no envio do quadro RTS e é detectado pela falha em receber o quadro CTS [27]. O envio de RTS e CTS pelas estações de origem e destino também evita o problema de terminal oculto, pois pelo menos um dos quadros será percebido pelo terminal oculto, que pode ajustar seu tempo de transmissão para evitar colisão [56].

O DCF adota um esquema de *backoff* exponencial para transmissão de pacotes como parte do mecanismo para evitar colisões. A cada pacote a ser transmitido, o tempo de *backoff* é escolhido uniformemente no intervalo $(0, cw - 1)$, onde *cw* representa o tamanho da janela de contenção, que depende do número de transmissões falhas do pacote em questão. Na primeira tentativa de transmissão, é atribuído a *cw*, o valor CW_{min} (Janela de Contenção Mínima). Após cada tentativa de transmissão falha, *cw* é dobrado até o valor máximo CW_{max} (Janela de Contenção Máxima). Os valores de CW_{min} e CW_{max} estão publicados na versão final do padrão IEEE 802.11 e em seus suplementos, e são dependentes da camada física utilizada [27][31].

4 – CONCEITOS EM GERENCIAMENTO DE MOBILIDADE

Segundo Akyildiz [58], a gerência de mobilidade habilita as redes de telecomunicações a localizar terminais para entrega de chamadas e a manter a conexão quando o terminal mover para uma nova área de serviço. Gerência de mobilidade contém dois componentes: gerência de localização e gerência de *handover*.

O foco principal do trabalho atual é a avaliação de alternativas de autenticação em redes WLAN e o seu impacto durante cenários de *handover* vertical. Autenticação é uma das funções básicas dentro da gerência de mobilidade, sendo fundamental no processo de gerência de localização.

4.1 - GERÊNCIA DE LOCALIZAÇÃO

Gerência de localização é um processo de dois estágios que permite à rede descobrir o ponto atual de conexão da estação móvel para a finalidade de entrega de chamadas. O primeiro estágio é o de atualização de localização ou *location update*. Neste estágio, a estação móvel notifica a rede periodicamente do seu novo ponto de acesso, permitindo a rede autenticar e recuperar seu perfil de localização do usuário. O segundo estágio é o *call delivery*. Aqui a rede é consultada para receber o perfil de localização do usuário e para encontrar a posição atual da estação móvel [58]. A figura 4.1 ilustra as operações da gerência de localização.

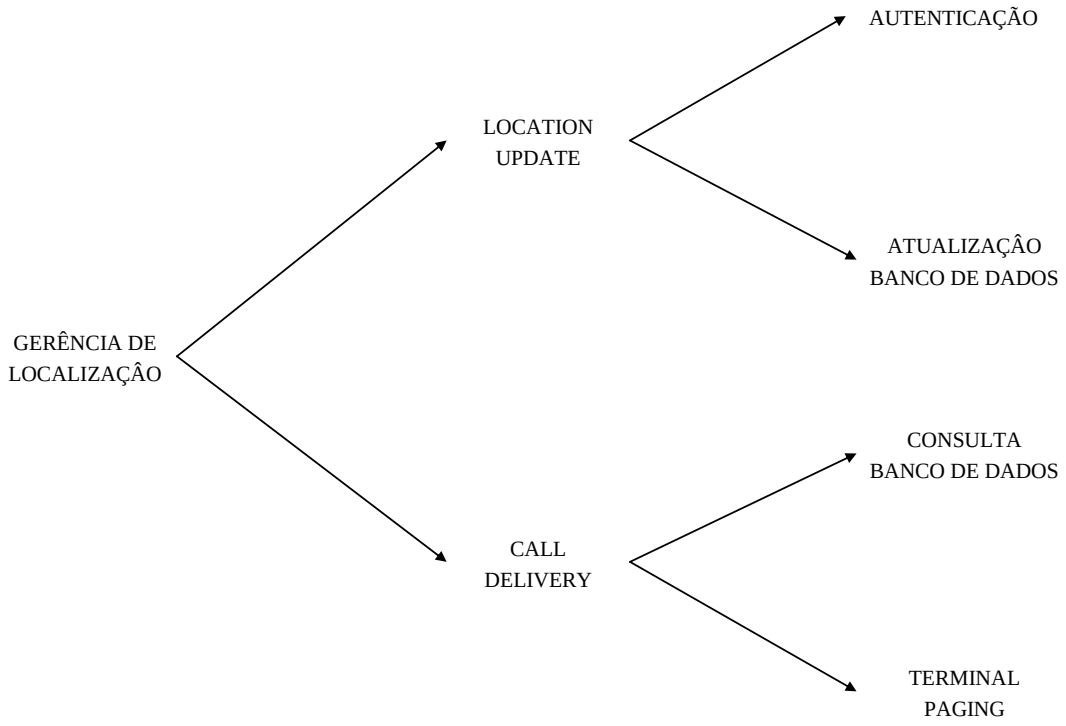


Figura 4.1 – Operações da Gerência de Localização (Akyildiz, modificado [58])

4.2 - GERÊNCIA DE HANDOVER

Segundo Akyildiz [58], a gerência de *handover* habilita a rede a manter a conexão do usuário enquanto a estação móvel está em movimento e muda o ponto de acesso ou a estação rádio base com a rede.

O *handover* envolve um processo de três estágios, sendo primeiro o de iniciação, onde o usuário ou um elemento de rede ou uma alteração na condição da rede identifica a necessidade de *handover* [58]. O segundo estágio é a geração de nova conexão, onde a rede deve encontrar novos recursos para a conexão de *handover* e executar operações adicionais de roteamento. Caso o *handover* seja controlado pela rede via *Network-Controlled Handover* (NCHO) ou *Mobile-Assisted Handover* (MAHO) a rede gera a nova conexão, encontrando os novos recursos para o *handover* e executando as operações adicionais de roteamento. Caso o *handover* seja controlado pelo terminal via *Mobile-Controlled Handover* (MCHO) o terminal encontra os novos recursos e a rede aprova a utilização dos mesmos.

O estágio final do *handover* é o controle de fluxo de dados, onde a entrega de dados da conexão antiga é mantida para a nova conexão de acordo com garantias de serviço previamente acordadas [58]. A figura 4.2 ilustra os estágios e as operações realizadas durante o *handover*.

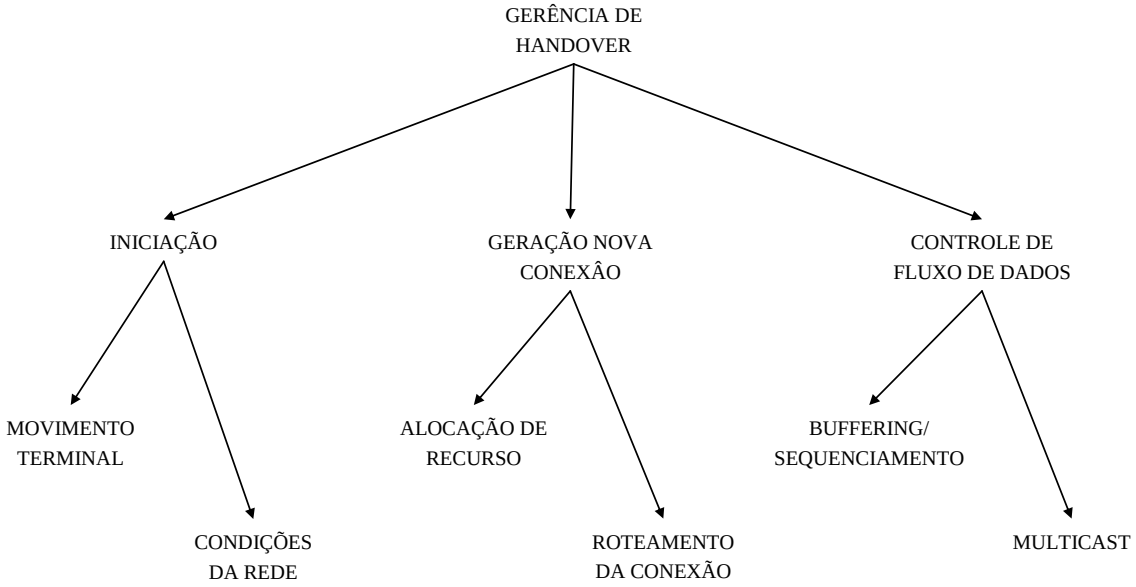


Figura 4.2 – Operações da Gerência de *Handover* (Akyildiz, modificado [58])

O *handover* pode ser classificado também com relação às diversas condições relacionadas com as redes envolvidas e as tecnologias implementadas, conforme é descrito na seção seguinte.

4.3 - CLASSIFICAÇÃO DOS HANDOVERS

Com a evolução e multiplicidade das tecnologias de comunicação sem fio, o *handover* não pode mais ser classificado somente por um único fator, como o tipo de rede. Muitos outros fatores constituem base para a classificação e categorização dos *handovers*. Nasser em [59], categoriza os processos de *handover* baseado nos: tipos de redes envolvidas, nas frequências engajadas, no número de conexões envolvidas, nos domínios administrativos envolvidos, na necessidade de *handover* e na permissão de controle do usuário. A figura 4.3 representa a árvore de classificação proposta.

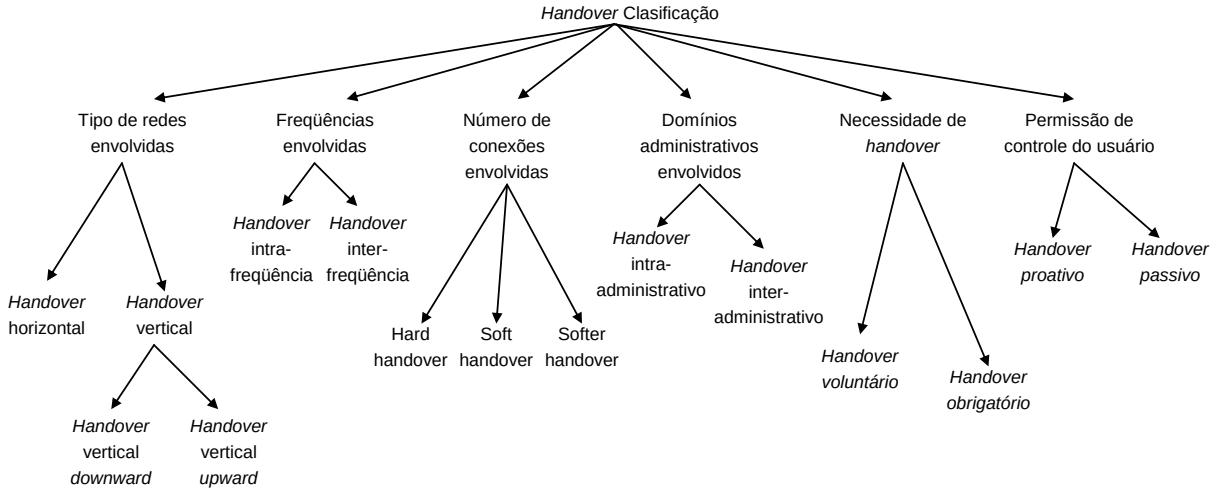


Figura 4.3 – Classificação de *Handovers* (Nasser, modificado [59])

A seguir são descritos cada um dos *handovers* mostrados na figura 4.3, seguindo as definições propostas em [59].

4.3.1 - *Handover* Horizontal

Primeiro fator de classificação baseado no tipo de rede envolvida. O *handover* horizontal ocorre quando uma estação móvel desloca entre pontos de acesso de uma mesma tecnologia.

4.3.2 - *Handover* Vertical

Segundo e último fator de classificação baseado o tipo de rede envolvida. O *handover* vertical ocorre quando uma estação móvel desloca entre pontos de acesso que implementam diferentes tecnologias.

Por envolver diferentes tecnologias, o *handover* vertical geralmente é iniciado pelo terminal após a conexão com a nova rede.

O cenário objeto em estudo neste trabalho considera a aplicação de *handover* vertical entre redes IEEE 802.11 e GSM.

4.3.3 – *Handover* Intra-frequência

Processo de *handover* de uma estação móvel através de pontos de acesso operando na mesma frequência. Presente, por exemplo, em redes CDMA (*Code-Division Multiple Access*) com FDD (*Frequency-Division Duplex*).

4.3.4 – *Handover* Inter-frequência

Processo de *handover* de uma estação móvel através de pontos de acesso operando em frequências diferentes. Este tipo é presente, por exemplo, em redes CDMA com TDD (*Time-Division Duplex*) e em redes GSM.

4.3.5 - *Hard Handover*

Relacionados com o fator número de conexões envolvidas. No procedimento de *hard handover* o enlace rádio do ponto de acesso antigo é liberado antes da conexão com o novo ponto de acesso, ou seja, antes de se completar o processo de *handover*.

4.3.6 - *Soft Handover*

Neste procedimento, também relacionado com o fator número de conexões envolvidas, a estação móvel mantém conexão rádio com pelo menos dois pontos de acesso na região de superposição de sinal. A conexão com o ponto de acesso antigo não é liberada enquanto o nível de sinal não decai até um valor definido ou até o processo de *handover* ser completamente encerrado. O *soft handover* é possível, por exemplo, em situações onde a estação móvel está movendo entre células operando na mesma frequência.

4.3.7 - *Softer Handover*

O *softer handover* é muito similar ao *soft handover*, a única diferença é que neste caso o terminal troca a conexão sobre enlaces de rádio que pertencem ao mesmo ponto de acesso.

4.3.8 - *Handover* Intra-Domínio Administrativo

Este é o primeiro fator relacionado aos domínios administrativos envolvidos. Um domínio administrativo pode ser entendido como um grupo de sistemas e redes operadas por uma

única organização com autoridade administrativa. Uma rede WWAN e um hot spot WLAN operado por um único provedor de serviço pode ser considerado como um domínio administrativo, sendo que este é um dos possíveis cenários para o estudo realizado neste trabalho.

O processo de *handover* intra-domínio administrativo ocorre quando o terminal transfere a conexão entre redes diferentes (suportando a mesma *interface* de rede ou não) gerenciadas pelo mesmo domínio administrativo.

4.3.9 - *Handover* Inter-Domínio Administrativo

O processo de *handover* inter-domínio administrativo ocorre quando o terminal transfere a conexão entre redes diferentes (suportando a mesma *interface* de rede ou não) gerenciadas por domínios administrativos diferentes.

4.3.10 - *Handover* Obrigatório

Primeiro processo de *handover* relacionado ao fator da necessidade. Em algumas situações é necessário que a estação móvel obrigatoriamente transfira a conexão para outro ponto de acesso para evitar desconexão.

4.3.11 - *Handover* Voluntário

Em algumas situações a transferência da conexão é opcional e pode ou não melhorar a qualidade do serviço. O *handover* voluntário pode ocorrer, por exemplo, na condição de transferência de conexão entre uma rede WWAN e um rede WLAN com cobertura inscrita na anterior. Neste caso o *handover* não é determinado pela necessidade de manter a conectividade com o terminal, mas por outros fatores, tais como custo da conexão.

4.3.12 - *Handover* Proativo

No *handover* proativo o usuário da estação móvel tem a permissão de decidir quando realizar o *handover*. A decisão pode ser baseada em um conjunto de preferências especificado pelo usuário.

4.3.13 - *Handover* Passivo

Neste processo o usuário não tem controle sobre o processo de *handover*. Este é o processo mais comum nas redes sem fio atuais.

5 – GERÊNCIA DE MOBILIDADE E AUTENTICAÇÃO EM REDES HETEROGÊNEAS

Nos capítulos precedentes foram explorados os conceitos gerais de gerência de mobilidade e as tecnologias de redes WWAN (3GPP GSM/UMTS) e WLAN (IEEE 802.11). Neste capítulo são tratados os aspectos específicos de gerência de mobilidade para cada uma destas tecnologias. O foco principal será sobre a descrição dos aspectos específicos da autenticação, que é um dos objetos do presente estudo.

5.1 - REDES WWAN BASEADAS NAS ESPECIFICAÇÕES 3GPP

Nas redes 3GPP (GSM e UMTS) descritas no capítulo 2, a gerência de mobilidade ou MM (*Mobility Management*) tem a finalidade de suportar a mobilidade da estação móvel na rede caseira (HPLMN) e nas redes visitadas (VPLMN) quando em condição de *roaming*. O suporte à mobilidade do usuário utiliza de procedimentos específicos do plano de sinalização entre a estação móvel e a rede núcleo (CN) e entre elementos da rede CN.

No plano de sinalização da *interface* aérea (*Um*) entre a estação móvel e uma rede de acesso GSM a gerência de mobilidade é uma das subcamadas dentro da camada 3 definida pelo 3GPP em [62]. Para o domínio comutado por circuitos (CS) as demais subcamadas são o *Radio Resource Management* (RR) e o *Connection Management* (CM), no domínio comutado por pacotes (PS) esta última é substituída pela subcamada *Session Management* (SM). Na rede CN o protocolo MAP (*Mobile Application Part*) [51] é responsável pela sinalização relacionada com os procedimentos de gerência de mobilidade, ou seja, os procedimentos e mensagens de MM da *interface Um* são traduzidos para o protocolo MAP pela central MSC, conforme ilustrado na figura 5.1 para o domínio CS.

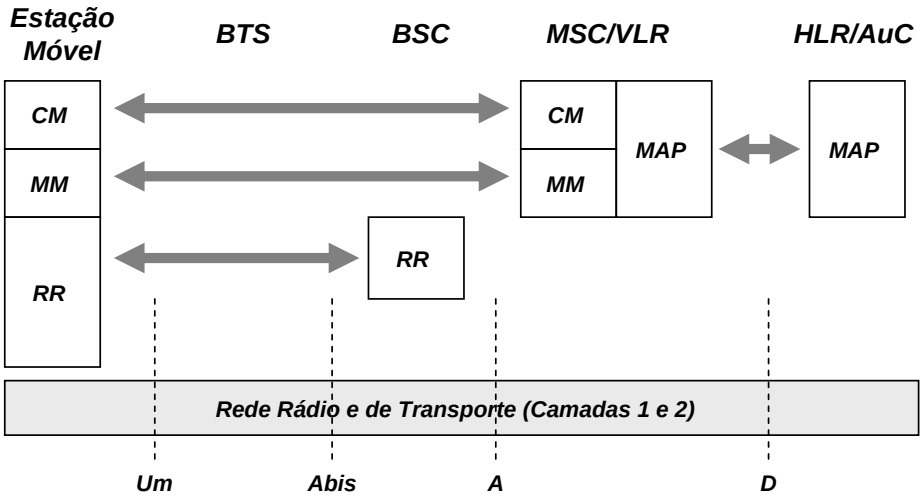


Figura 5.1 – Arquitetura de Sinalização GSM para Gerência de Mobilidade (Eberspächer, modificado [60])

Na rede GSM todos os procedimentos de MM da estação móvel são tratados sem o envolvimento da rede de acesso, ou seja, diretamente entre o terminal e a central MSC. A subcamada de gerência de mobilidade possui entidades diferentes para tratar os procedimentos de mobilidade entre os domínios CS e PS. No domínio CS as atividades de gerência de mobilidade são tratadas pela entidade MM e no domínio PS as atividades de gerência de mobilidade são tratadas pela entidade GMM (*GPRS Mobility Management*) [61].

5.1.1 - Gerência de Localização

Na rede GSM as funções para relatar a localização atual do terminal e para identificação e autenticação dos usuários são o *Location Updating* e o *Location Registration*. A autenticação do usuário ocorre sempre que há o registro do terminal na rede, a atualização de localização e o estabelecimento de chamadas.

Antes de o terminal móvel ter acesso aos serviços da rede caseira ou visitada o usuário deve registrar sua localização na rede móvel. Este processo de registro é necessário somente quando há uma mudança de rede, ou quando o terminal ainda não recebeu sua identificação temporária de assinante ou TMSI (*Temporary Mobile Subscriber Identity*) [60]. Isso significa que o terminal tem que inicialmente se comunicar com a rede utilizando a sua identificação de assinante real ou IMSI (*International Mobile Subscriber Identity*)

que é armazenada no cartão SIM utilizado pelo usuário. O processo de registro de localização (*Location Registration*) é parte do procedimento de conexão inicial à rede WWAN.

Na sequência de operações que ocorrem durante o registro, o terminal envia um pedido de atualização de área (*Location Update*) informando seu IMSI e a área de localização atual (LAI – *Location Area Identity*). Antes de registrar a localização do terminal o VLR realiza a autenticação do usuário, requisitando um vetor de autenticação para o HLR/AuC com o IMSI do usuário e utilizando o procedimento descrito no próximo seção.

Após autenticação bem sucedida, o terminal recebe um número de *roaming* ou MSRN (*Mobile Subscriber Roaming Number*) que é armazenado com a informação de localização (LAI) no HLR. O VLR também aloca um novo TMSI para o terminal e envia, junto com uma chave de criptografia (*Kc*), para a central MSC responsável. A chave de criptografia *Kc* é utilizada para iniciar o processo de cifrar os dados de usuário na *interface* aérea. Após o processo de cifrar os dados ter iniciado, o TMSI e a mensagem de reconhecimento do registro na rede são enviados para o terminal de forma cifrada. O terminal reconhece o recebimento do TMSI e o processo de registro é completado [60]. O procedimento de registro de localização é ilustrado de forma simplificada na figura 5.2.

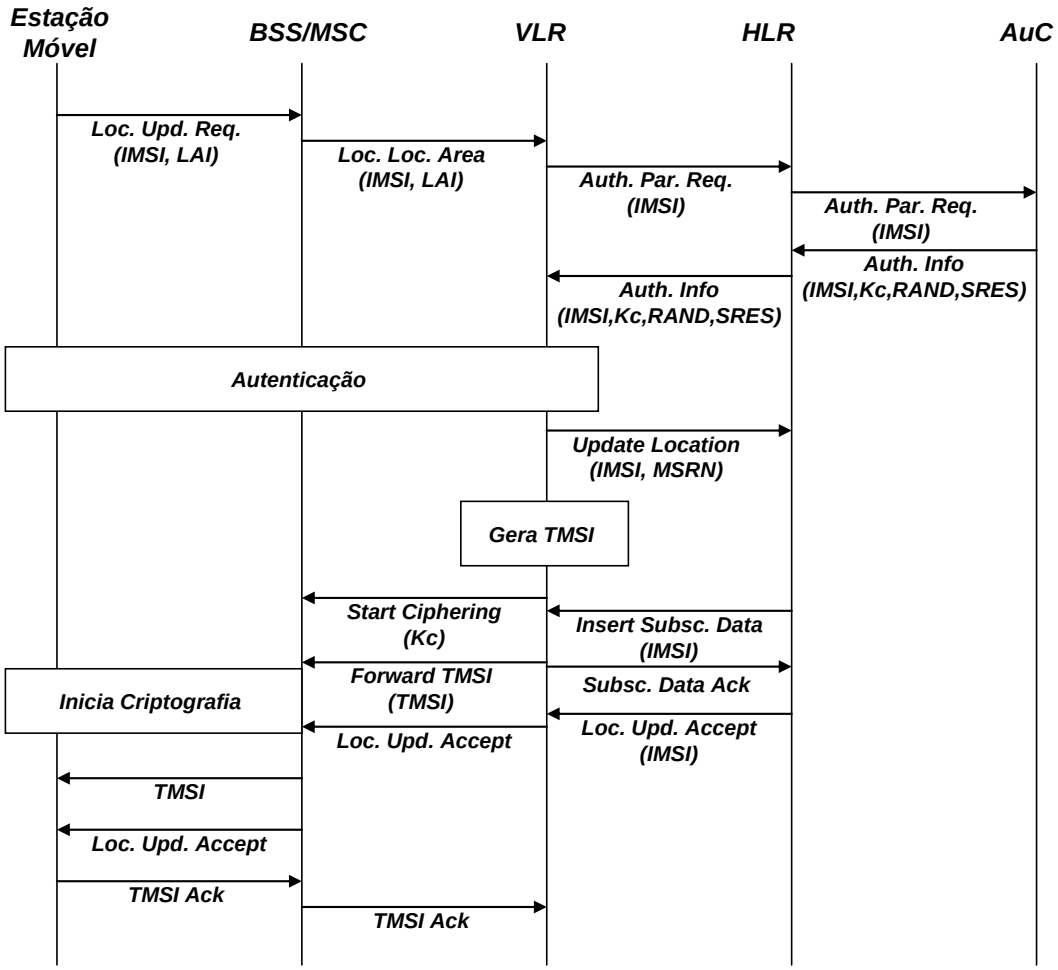


Figura 5.2 – Procedimento de Registro de Localização GSM (Eberspächer, modificado [60])

O procedimento de atualização de localização (*Location Update*) é executado quando o terminal reconhece que está em uma nova área de localização, através da verificação da informação de LAI recebida pelo canal de controle, e tem o objetivo de atualizar a informação de localização no registro do HLR. Este procedimento pode ocorrer também de forma periódica em intervalos de tempo determinados pela rede móvel. A diferença entre o procedimento de *Location Update* e de *Location Registration* é que no primeiro caso o terminal já possui um TMSI designado. O TMSI tem validade em conjunto com o LAI e é armazenado na memória não volátil do cartão SIM. A cada novo procedimento de atualização de localização pode ser designado um novo TMSI e novas chaves de criptografia ao terminal. O terminal é também novamente autenticado, com o VLR utilizando um novo conjunto de vetor de autenticação, composto dos campos: RAND, SRES e *Kc* [60]. A figura 5.3 ilustra o procedimento de atualização de localização.

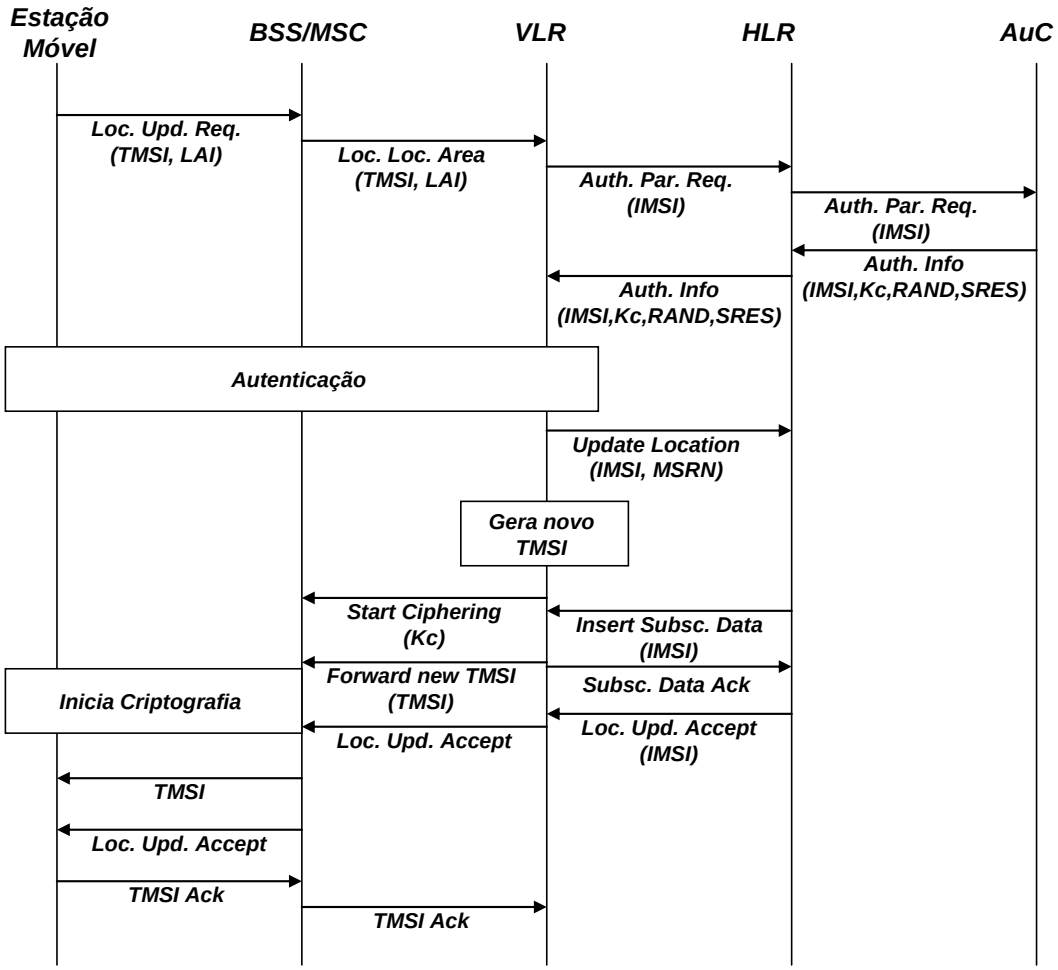


Figura 5.3 – Procedimento de Atualização de Localização GSM (Eberspächer, modificado [60])

No caso do terminal mover para uma área de localização servida por outro VLR o procedimento de atualização de localização ocorre da mesma forma exceto pelo fato de antes da autenticação o VLR novo requisitar informações do terminal no VLR antigo, através do TMSI e LAI, e receber como resposta o IMSI e um novo conjunto de vetor de autenticação [60].

5.1.2 – Autenticação GSM

Quando um assinante é habilitado na rede caseira pela primeira vez uma chave de autenticação de assinante (*Ki*) é designada, em conjunto com o IMSI para permitir a verificação da identidade do usuário durante sua autenticação. Todas as premissas de segurança são baseadas no segredo desta chave. No lado da rede ela é armazenada no

elemento AuC (*Authentication Center*) da rede caseira do assinante. No lado do assinante ele é armazenado em um arquivo na área segura do cartão SIM.

O processo de autenticação é baseado no algoritmo A3 que é executado no lado da rede e no lado do assinante. Este algoritmo calcula de forma independente, na rede e no terminal, uma assinatura de resposta (SRES – *Signature Response*) obtida com a chave *Ki* e com o número randômico (RAND) oferecido pela rede. O terminal transmite o SRES calculado para a rede que compara com o seu próprio. Caso ambos os valores sejam iguais a autenticação foi bem sucedida. Cada nova execução do algoritmo A3 é realizada com um novo valor de RAND, evitando fraude por reenvio de dado previamente gravado [60]. A figura 5.4 mostra o princípio básico da autenticação.

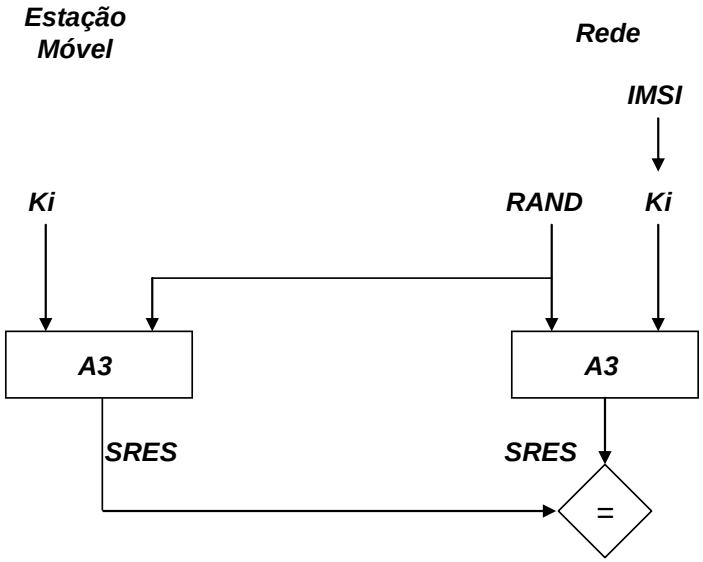


Figura 5.4 – Princípio da autenticação de usuário GSM (Eberspächer, modificado [60])

O número RAND é também utilizado para a geração da chave de criptografia dos dados de usuário (*Kc – Cipher Key*) em conjunto com a chave *Ki* e o algoritmo A8. A chave *Kc* é utilizada pelo algoritmo A5 no processo de criptografia simétrica dos dados de usuário. O valor de *Kc* é calculado pelo elemento AuC simultaneamente com o valor de SRES. Os valores de *Kc*, RAND e SRES correspondem ao vetor de autenticação (*3-tuples* ou *triplets*) que é fornecido sob demanda em caso de requisição de informação de autenticação pela rede.

O processo de autenticação ocorre com o recebimento de RAND, SRES e *Kc* pelo VLR e o envio de RAND do VLR para o terminal. O terminal calcula SRES com base no algoritmo A3 no cartão SIM e devolve para o VLR o valor de SRES calculado. Caso o SRES do terminal e do AuC sejam iguais o VLR aceita a autenticação [60].

Os algoritmos A3 e A8 não foram originalmente padronizados, somente suas *interfaces* e os procedimentos gerais de autenticação. As operadoras de telefonia móvel têm a responsabilidade de estar definindo os mesmos para uso na sua rede própria [10]. Inicialmente existiam alguns exemplos fornecidos pela GSMA (*GSM Association*). Em 2002 o 3GPP padronizou também um exemplo de algoritmo A3/A8 chamado de GSM MILENAGE [69].

5.1.3 – Autenticação UMTS

O método de autenticação e criptografia GSM oferece algumas fragilidades que foram levadas em conta nos princípios para o desenvolvimento da solução para redes 3G baseadas em UMTS (*Universal Mobile Telecommunications System*). As funcionalidades principais de segurança de acesso nas redes UMTS são [61]:
a) Autenticação mútua do usuário e da rede;
b) Uso de identidades temporárias;
c) Criptografia da rede de acesso rádio (RAN);
d) Proteção da integridade da sinalização dentro da rede de acesso UMTS.

Com o processo de autenticação mútua a rede verifica a identidade do usuário e o usuário verifica se a rede que ele está conectando é autorizada pela sua rede caseira. O fundamento do mecanismo de autenticação UMTS é uma chave mestre (*K*) que é compartilhada entre a rede caseira e o cartão USIM do usuário. Esta chave possui 128 *bits* e deve ser mantida em segredo.

O procedimento de autenticação é mostrado na figura 5.5. Quando um terminal realiza uma tentativa de registro na rede informando sua identidade permanente (IMSI) ou temporária (TMSI) o VLR envia uma requisição de autenticação ao elemento AuC identificando o IMSI do usuário. O AuC recupera a chave *K* do usuário e, com a mesma, gera um ou mais conjuntos de vetores de autenticação de volta para o VLR. Um vetor de autenticação

contém os seguintes componentes: número randômico (RAND), resposta esperada (XRES), chave de criptografia (CK), chave de integridade (IK) e *authentication token* (AUTN).

O VLR retorna para o terminal somente os componentes RAND e AUTN. O terminal utiliza o algoritmo no cartão USIM, em conjunto com *K*, AUTN e RAND, para validar a rede, verificando o AUTN, e para calcular o resultado (RES) e as chaves CK e IK. O RES é retornado ao VLR que compara com o XRES armazenado, caso sejam coincidentes a autenticação do usuário é aceita.

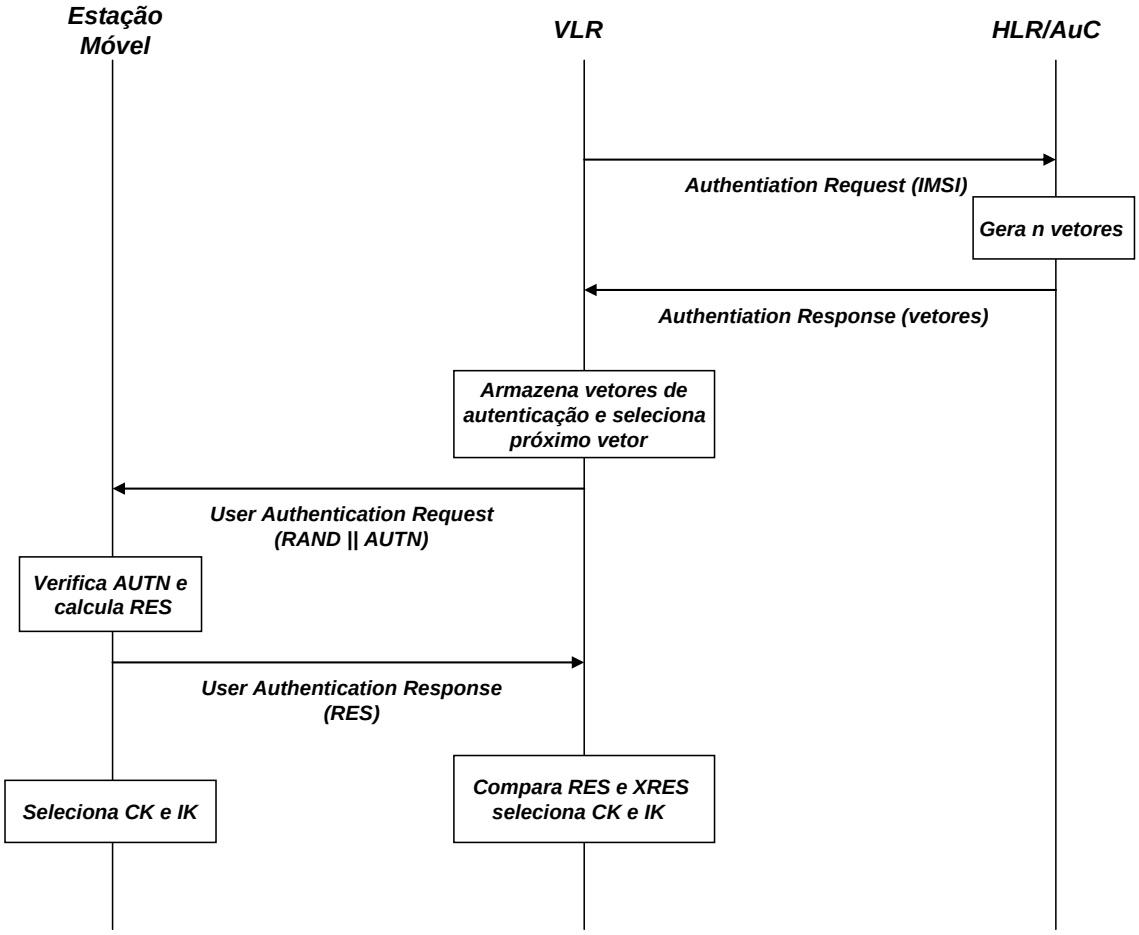


Figura 5.5 – Procedimento de autenticação do usuário UMTS (Bannister, modificado [66])

A figura 5.6 ilustra o processo de geração do vetor de autenticação no AuC. Este inicia com a seleção de um número de sequência (SQN) correto. O SQN deve ser utilizado sempre em ordem crescente de valores para cada vetor gerado. Em paralelo é gerado um número randômico (RAND) de 128 *bits*.

O conceito de chave utilizado é o de função de mão única (*one-way function*), que é uma função matemática relativamente simples de calcular, mas praticamente impossível de ser invertida. Para computar o vetor de autenticação são utilizadas cinco funções de mão única, denominadas f1, f2, f3, f4 e f5. A função f1 recebe como parâmetros de entrada: chave mestre (*K*), RAND, SQN e um campo administrativo chamado de *Authentication Management Field* (AMF). As funções f2 a f5 têm somente *K* e RAND como entradas. A saída de f1 é *Message Authentication Code* (MAC) com 64 *bits*. A saída de f2 é XRES (32-128 *bits*). A saída de f3 é CK (128 *bits*). A saída de f4 é IK (128 *bits*). A saída de f5 é AK (64 *bits*). O vetor de autenticação são os valores concatenados de RAND, XRES, CK, IK e AUTN. AUTN é obtido pela concatenação de SQN, somado *bit* a *bit* com AK, AMF e MAC.

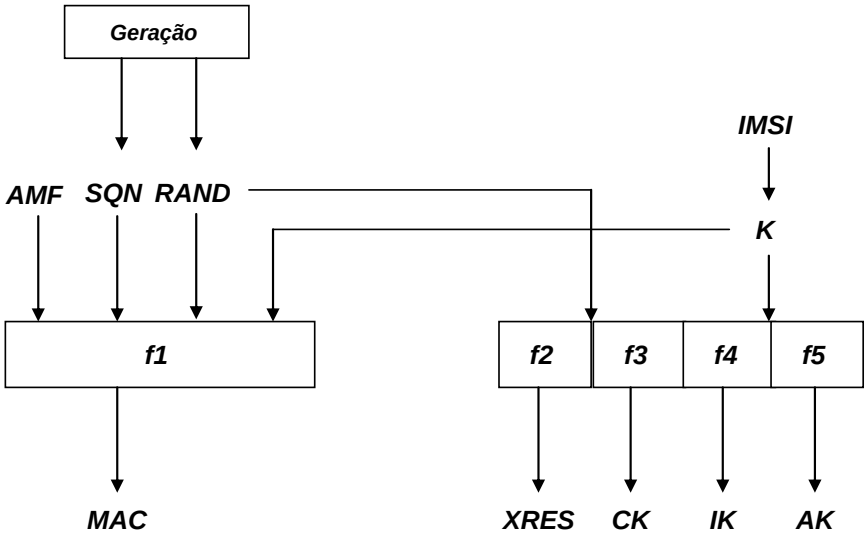


Figura 5.6 – Geração do vetor de autenticação UMTS (Kaarenen, modificado [61])

O tratamento da autenticação no USIM é ilustrado na figura 5.7 e descrito a seguir. As mesmas funções f1-f5 são utilizadas, mas em ordem diferente. A função f5 deve ser computada antes da função f1, devido ao fato da função f5 ser utilizada para ocultar SQN. A função f1 calcula o XMAC que é comparado com o MAC recebido no AUTN. Caso XMAC e MAC sejam iguais significa que o vetor foi enviado por uma entidade que conhece a chave secreta *K* do usuário. Para verificar se o vetor não é uma retransmissão de fonte maliciosa o valor de SQN é verificado e deve ser maior que qualquer outro recebido

anteriormente. As chaves CK e IK e o resultado RES são calculados com as demais funções [61].

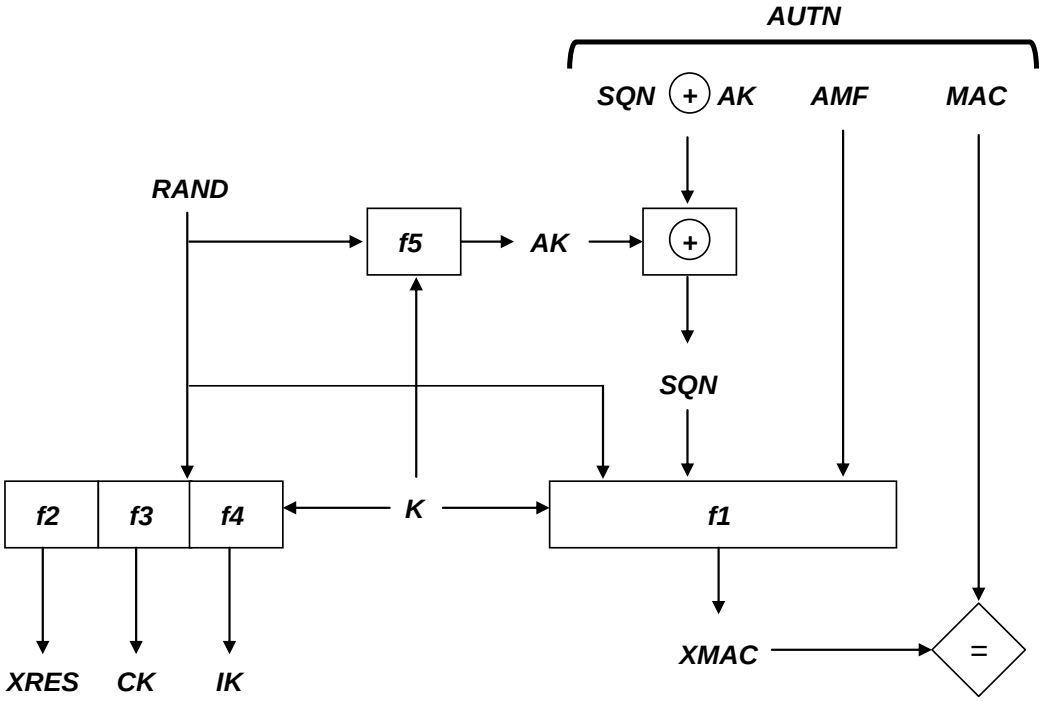


Figura 5.7 – Tratamento da autenticação no USIM (Kaarenen, modificado [61])

Os algoritmos para as funções f1-f5 são de responsabilidade e específicos de cada operadora móvel. O 3GPP padronizou um conjunto de algoritmos exemplo na especificação TS 35.206 [70], conhecidas como MILENAGE, que podem ser utilizados pelas operadoras que não desejam desenvolver seu conjunto próprio de algoritmos.

De forma similar ao realizado pela rede GSM, as redes UMTS definem identidades temporárias com significância local, dentro de uma área de localização, para o terminal registrado. Para o domínio CS é designado um TMSI (*Temporary Mobile Subscriber Identity*) e para o domínio PS um P-TMSI (*Packet-TMSI*).

A chave CK é utilizada para criptografia dos dados na *interface* aérea e a chave de integridade IK é utilizada para verificação da integridade de cada mensagem recebida pelas pontas do enlace [61].

5.1.4 – *Handover*

Em sistemas GSM o *handover* é uma decisão realizada pela rede e não pelo terminal móvel. O *handover* é baseado em critérios do sistema BSS, tais como: nível de sinal recebido; qualidade do canal; distância entre o terminal e a BTS, e, em critérios de operação de rede, tais como: tráfego percebido na célula; e, atividades de manutenção [60].

As funções para preparação do *handover* são parte do controle de enlace do subsistema de rádio. Este inclui a medida do canal, realizada pelo terminal móvel. Estas medidas incluem o nível de sinal da célula atual e das vizinhas. O relatório das medidas é enviado para a estação rádio base atual. No lado da rede o sinal de *uplink* é também monitorado, os registros das medidas são avaliados e as decisões de *handover* são tomadas.

Como uma questão de princípio e padronização, o *handover* é realizado somente entre estações rádio base da mesma PLMN. *Handover* entre BSS em diferentes redes GSM/UMTS não é permitido [60]. Dois tipos de *handover* são distinguíveis:
a) *Intracell handover*: o terminal é assinalado para um novo canal dentro da mesma célula, ocorre por razões administrativas ou por degradação na qualidade do canal. A decisão é tomada localmente pela gerência de recursos de rádio (RR) do BSS e executada internamente ao BSS;
b) *Intercell handover*: a conexão do terminal é transferida sobre o limite da célula para uma nova BTS. A MSC pode participar na seleção da nova BTS e célula. Este *handover* ocorre principalmente devido a degradação do sinal ou qualidade do canal.

De acordo com a participação ou não da central MSC na sequência de sinalização da execução do *handover* podem ser evidenciados dois casos. Como o módulo de RR reside no BSS, *handovers* que ocorrem entre células controladas pelo mesmo elemento BSC podem ser executados sem a participação da MSC e são chamados de *handover* interno. Neste caso a MSC é somente informada da execução bem sucedida do *handover*. Todos os demais *handovers* dependem da participação de pelo menos uma MSC, e são conhecidos como *handover* externo [60].

A MSC (MSC-A) que executa o estabelecimento inicial da conexão realiza o ancoramento da chamada e mantém o controle da mesma pelo tempo de duração da conexão. Desta

forma com o *handover* pode ocorrer também a extensão da conexão da chamada da MSC-A para a MSC (MSC-B) vinculada à nova BTS.

5.1.5 – *Intra-MSC Handover*

A estrutura básica para um *handover* externo é o realizado entre duas células da mesma MSC, conforme fluxo de sinalização mostrado na figura 5.8. O terminal móvel continuamente transmite relatórios de medidas com dados monitorados do canal de rádio para a estação base atual (BSC1). Baseado nos resultados das medições a BSS decide quando deve ser executado o *handover* e requisita o mesmo para a MSC através de mensagem específica (*Handover Required*). Os resultados das medidas podem ser enviados nesta mensagem para permitir a participação da MSC na decisão de *handover*. A MSC sinaliza o novo BSS para reservar um canal para o *handover* e libera o *handover* para o terminal móvel (*Handover Command*), tão logo a confirmação da reserva é recebida. O terminal então se reporta para o novo BSS (*Handover Access*) e recebe a informação com as propriedades do novo canal físico. Quando o terminal é capaz de ocupar o canal com sucesso, ele sinaliza com a mensagem *Handover Complete* e os recursos do BSS antigo podem ser liberados.

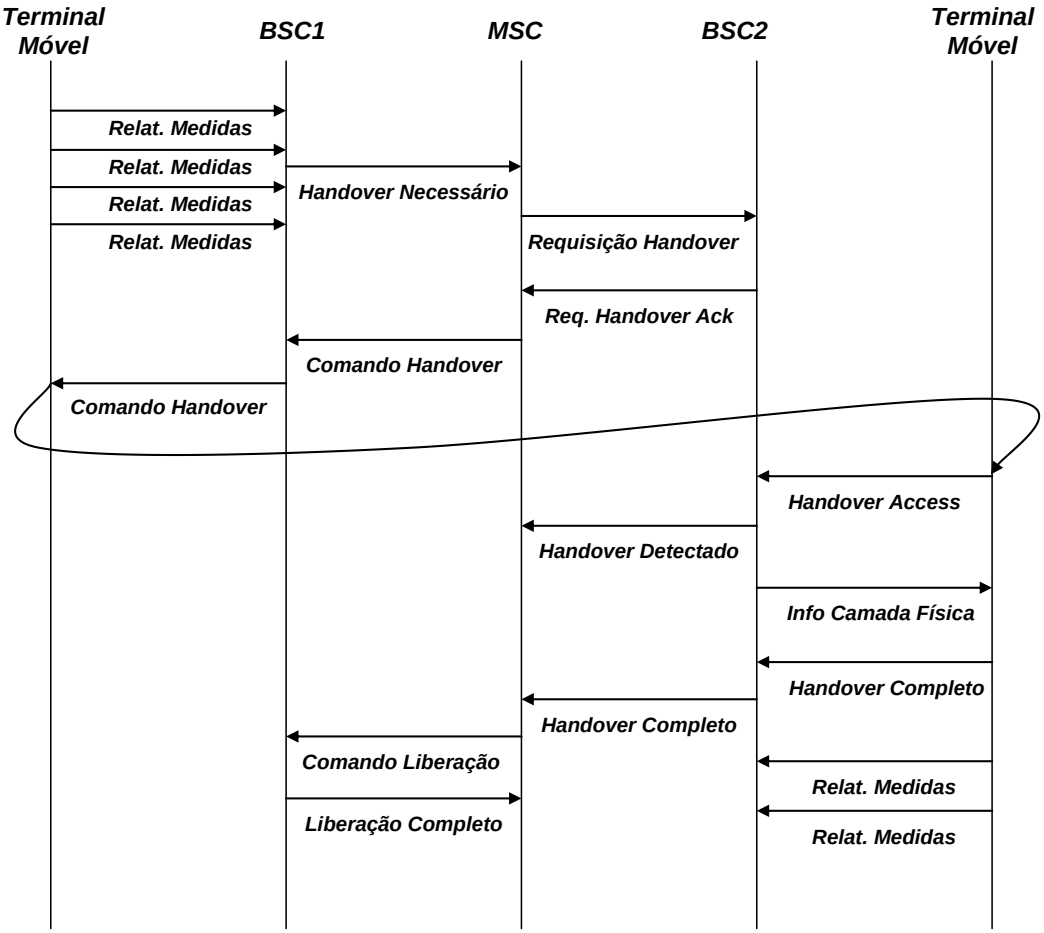


Figura 5.8 – Sinalização pra *intra-MSC handover* (Eberspächer, modificado [60])

5.1.6 - *Inter-MSC Handover*

Esta é a forma mais geral de *handover*. Ocorre quando o terminal move sobre o limite de uma célula e entra na área de responsabilidade de outra MSC. O *handover* provocado por este movimento requer comunicação entre as MSC envolvidas, esta comunicação ocorre via sinalização SS7 através do protocolo MAP (*Mobile Application Part*) [60].

A sequência principal de operações para o *handover* básico entre duas MSC é mostrada na figura 5.9. O sistema BSS requisita o *handover* para a MSC-A com base nas condições indicadas pelo terminal. A MSC-A decide pelo *handover* e envia mensagem (*Perform Handover*) para MSC-B, a mensagem identifica o BSS para receber a conexão e contém os dados necessários para a MSC-B reservar o canal de rádio para o terminal. A MSC-B determina um número de *roaming* e tenta alocar um canal para o terminal. Caso haja canal disponível retorna mensagem (*Radio Channel Acknowledge*) com a designação do canal e

o novo número MSRN do terminal. Caso não haja canal disponível a MSC-A também é informada e o procedimento de *handover* é terminado.

Em caso do canal ter sido reservado com sucesso, uma conexão de chamada é estabelecida entre as duas MSC, normalmente através de sinalização SS7 ISUP (mensagens IAM e ACM na figura 5.9), e ambas as MSC enviam sinalização para o terminal (*HA Indication, HB Indication*). O terminal recupera a conexão no novo canal (*HB Confirm*). Então a MSC-B sinaliza para a MSC-A que libera o canal de rádio antigo.

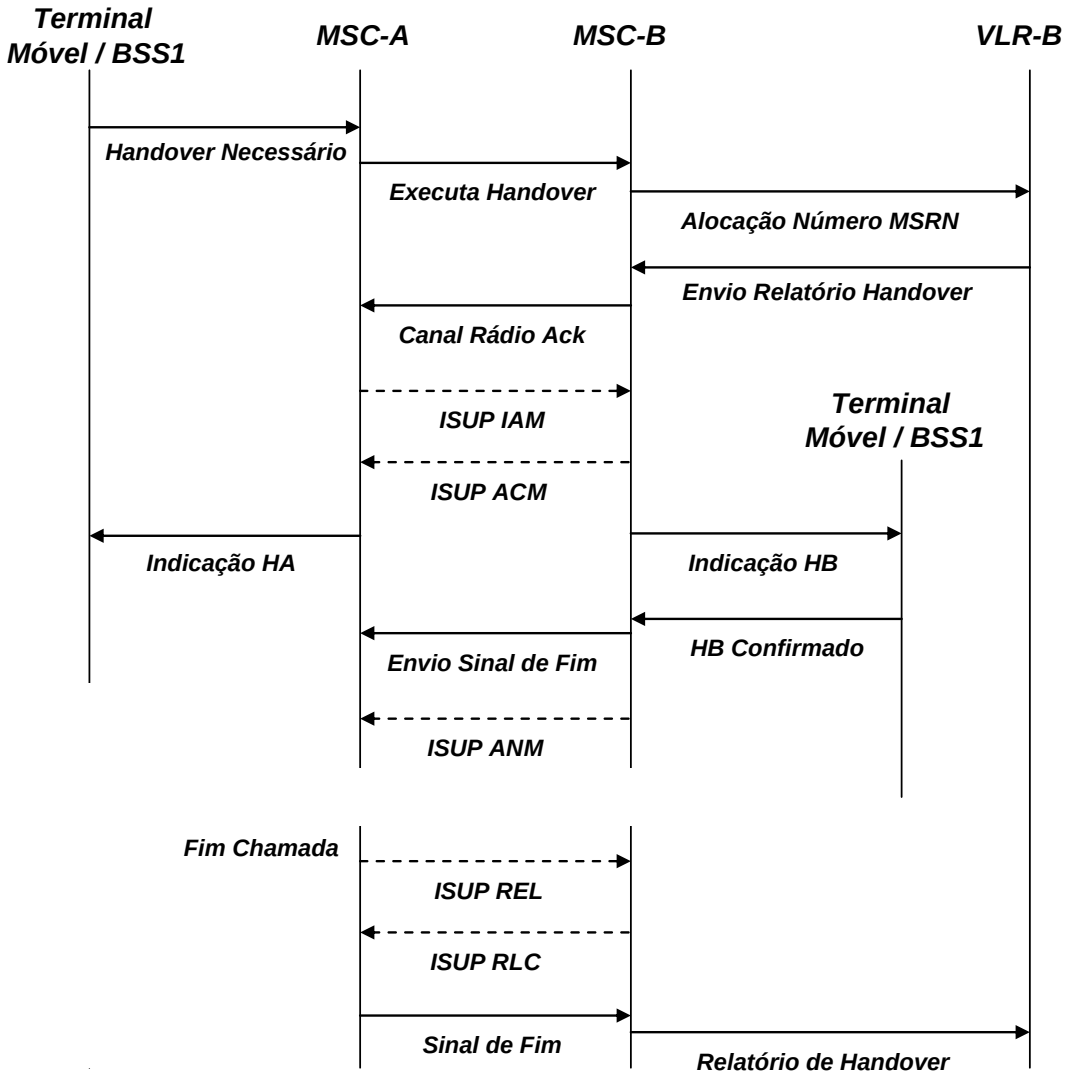


Figura 5.9 – Sinalização pra *inter-MSC handover* (Eberspächer, modificado [60])

5.1.7 - *Handover* Subsequente

Handover subsequente é executado quando o procedimento de *handover* envolve o retorno da chamada para a MSC original ou para uma terceira MSC, após execução do primeiro *inter-MSC handover*. Após o *handover* da MSC-A para MSC B, caso seja necessário um novo *handover* para MSC C ou retornando para MSC A o procedimento de *handover* subsequente é iniciado. Neste procedimento a conexão é sempre reencaminhada pela MSC-A, ou seja, após o *handover* entre MSC-B e MSC-C a conexão da MSC-A com a MSC-B é desfeita, restando a conexão entre a MSC-A e MSC-C. Este procedimento é possível devido a MSC-A ser responsável por ancorar a conexão inicial do terminal. No caso de retorno para a MSC-A (ou *handback*) a conexão da MSC-A com a MSC-B também é desfeita após o *handover* ser completado com sucesso [60].

5.2 – REDES WLAN IEEE 802.11 / Wi-Fi

O padrão IEEE 802.11 oferece suporte a mobilidade através dos mecanismos de associação e de reassociação. Quando um terminal entra na área de cobertura de um ou mais ponto de acesso IEEE 802.11, ou AP, ele decide o melhor ponto de acesso para se associar. A associação entre o terminal e o ponto de acesso é baseada em alguns fatores, tais como a intensidade e qualidade do sinal recebido. Depois de conectado, autenticado e associado, o terminal periodicamente procura por outros canais 802.11 para verificar se outro ponto de acesso oferece uma intensidade de sinal mais forte. Caso algum ponto de acesso oferecer sinal melhor que o anterior, o terminal pode mudar a sintonia para o canal deste novo ponto de acesso. Este processo é conhecido como reassociação e normalmente acontece devido à mobilidade do terminal em relação ao ponto de acesso no qual ele está associado, dentro de uma mesma rede de pontos de acesso ou área de serviço estendia (ESS) [16].

Dentro de uma área de serviço estendida o padrão IEEE 802.11 provê mobilidade na camada MAC. Estações conectadas ao DS podem enviar quadros destinados ao endereço MAC de um terminal e deixar para os APs tratarem o último segmento para a estação móvel. Estações em um DS não necessitam ter conhecimento da localização de uma dada estação móvel enquanto esta estiver dentro da mesma área de serviço estendido [57].

Transições de BSS requerem a cooperação dos pontos de acessos. Neste cenário, quando uma estação se move da área do AP1 para a área do AP2, o AP2 necessita informar o AP1 que aquela estação móvel está agora associada com ele. O padrão IEEE 802.11 não define

os detalhes do protocolo de comunicação entre os pontos de acesso durante transições de BSS. Devido a esta falta de padronização, a mobilidade entre pontos de acesso fornecidos por fabricantes diferentes não é garantida [57].

5.2.1 – Procedimentos de Conexão, Autenticação e Associação

Dentro da etapa de conexão de uma estação móvel a uma rede IEEE 802.11 temos o processo de identificação das redes existentes, chamado de *scanning*, que pode ser passivo ou ativo [57].

O *scanning* passivo não requer transmissão de sinal do terminal e oferece economia de bateria para as estações portáteis. No *scanning* passivo, o terminal seleciona cada canal da sua lista de canais e aguarda por quadros de gerência específicos (*Beacon*). Cada quadro *Beacon* recebido é armazenado para permitir a extração das informações necessárias sobre o BSS que o enviou.

No *scanning* ativo a estação móvel tem um papel mais atuante. Neste modo, para cada canal é usado um quadro de *Probe Request* para solicitar respostas de uma rede com um dado nome. Ao invés de escutar a rede realizar seu anúncio, no modo ativo o terminal tenta encontrar a rede. Estações móveis utilizando o *scanning* ativo empregam os seguintes procedimentos, por canal:
a) Selecionar o canal e esperar pela indicação de um quadro de entrada. Caso seja detectado algum quadro o canal está em uso e pode ser testado, caso contrário o terminal aguarda até a expiração de uma temporização específica;
b) Ganhar o acesso ao meio utilizando os procedimentos básicos do DCF [27] e enviando um quadro *Probe Request*;
c) Aguarda por resposta via quadro *Probe Response* ou aguarda até expirar uma temporização específica.

Os quadros de *Probe Response* são gerados pela rede quando estas escutam um quadro *Probe Request* a procura do ESS da qual a rede pertence. Após verificar os resultados do *scanning*, o terminal pode eleger uma BSS para se conectar. A conexão é precursora dos passos de autenticação e associação.

No padrão original IEEE 802.11 [31] foi definido dois tipos de autenticação: autenticação de sistema aberto ou *open-system* e autenticação com chave compartilhada ou *shared-key*. A autenticação original com chave compartilhada é baseada no algoritmo simétrico *Wired Equivalent Privacy* (WEP) que deve ser implementado em ambas as estações conectadas [57]. O padrão IEEE 802.11 não restringe a autenticação a um cenário particular, ou seja, qualquer estação pode se autenticar com qualquer outra, apesar de que o processo de autenticação é mais prático em uma rede de infraestrutura, ou seja, entre um terminal e um AP.

Nas especificações originais do padrão 802.11 a autenticação não é mútua, ou seja, as estações móveis se autenticam na rede, mas a rede não possui obrigação de se autenticar para a estação móvel. Este fato cria algumas lacunas de segurança, permitindo que um atacante possa se passar por uma rede autêntica, simulando seu SSID, com o objetivo de roubar credenciais, em um método de ataque conhecido como *man-in-the-middle* [57] [16].

Na autenticação de sistema aberto o AP aceita a estação móvel sem verificar sua identidade. Esta autenticação é realizada com o envio de um quadro de autenticação com a identidade da estação móvel, indicada pelo seu endereço MAC, e a identificação de algoritmo igual à zero, de forma a indicar que está sendo utilizado o método *open-system*. O AP retorna o pedido com um quadro de autenticação informando o código de *status* do pedido realizado.

Na autenticação com chave compartilhada e com uso de WEP a chave de autenticação deve ser distribuída entre as estações antes da tentativa de autenticação, o método de compartilhamento da chave não é escopo da especificação do 802.11. A autenticação em si consiste na troca de quatro quadros de autenticação. O primeiro é similar ao enviado no caso de sistema aberto exceto pela informação de que se deseja utilizar autenticação com chave compartilhada. No segundo quadro o AP pode aceitar o pedido e retornar um texto desafio de 128 *bytes* criado pelo gerador de número pseudoaleatório do WEP (PRNG – *Pseudo-Random Number Generator*). Na resposta da estação o terceiro quadro é enviado com o texto desafio cifrado pelo WEP com o uso da chave compartilhada. Por fim o AP retorna o último quadro com o resultado da requisição de autenticação, após verificação de integridade e do conteúdo cifrado.

Após a autenticação com chave compartilhada ter sido realizada com sucesso os dados são transferidos de forma cifrada pelo algoritmo WEP pela *interface* aérea do 802.11.

A utilização do método WEP tal como definido originalmente pelo padrão IEEE 802.11 não é mais recomendada devido às fragilidades que podem ser exploradas, tais como, forma de compartilhamento da chave, chave frágil com somente 40 *bits*, reuso da chave durante a sessão e outros [57][56][16][32]. Outros mecanismos padrões foram criados posteriormente pelo WFA e incorporados pelo IEEE e publicados como o suplemento 802.11i [32] ao padrão original. As definições relativas à autenticação baseada no suplemento 802.11i são descritas brevemente em seção específico deste capítulo.

Após a autenticação ser completada a estação móvel pode associar com o AP para ter acesso pleno à rede. Associação é um procedimento que permite o DS traçar a localização de cada estação móvel, de forma que os quadros destinados para uma determinada estação móvel possam ser encaminhados para o AP correto. O procedimento de associação é realizado através da troca de quadros '*association request*' e '*association response*' entre a estação móvel e o AP.

O procedimento de associação bem sucedido é condição necessária para iniciar o processo de autenticação baseado no padrão IEEE 802.1x, que é base para os métodos definidos no IEEE 802.11i.

5.2.2 – Autenticação EAP

O padrão IEEE 802.1x (consequentemente o IEEE 802.11i) é baseado no protocolo *Extensible Authentication Protocol* (EAP) [9] desenhado especificamente para realizar autenticação entre duas pontas: o *supplicant* ou *peer* e o *authenticator*.

EAP é especificado pelo IETF na recomendação RFC 3748 [9] e é um protocolo simples de encapsulamento que pode ser utilizado sobre qualquer camada de enlace e que suporta uma grande variedade de mecanismos de autenticação. O EAP foi desenvolvido para ser transportado diretamente sobre os protocolos da camada de enlace e provê seu próprio mecanismo de retransmissão, mas não suporta fragmentação, remontagem e pacotes

recebidos fora de ordem. A figura 5.10 mostra a arquitetura do protocolo, e sua flexibilidade em selecionar mecanismos de autenticação específicos.

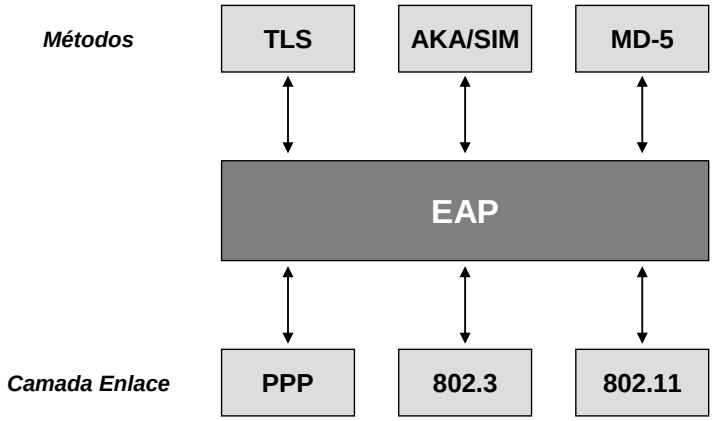


Figura 5.10 – Arquitetura EAP (Gast, modificado [57])

O pacote EAP possui quatro tipos de campos que podem ser carregados sobre qualquer tipo de quadro. Os campos no pacote EAP são [57]:

a) Código: primeiro campo no pacote e com um *byte* de comprimento, identifica o tipo de pacote EAP e é usado para interpretar o conteúdo do campo de dados do pacote. Somente quatro códigos são designados: *Request* (1), *Response* (2), *Success* (3) e *Failure* (4);

b) Identificador: com um *byte* de comprimento, contêm um valor inteiro sem sinal usado para casar requisições com respostas. Requisições retransmitidas utilizam o mesmo valor de identificador, mas novas requisições devem utilizar sempre novos números de identificadores.

c) Comprimento: com dois *bytes* este campo indica o comprimento em *bytes* do pacote EAP, incluindo os campos de código, identificador, comprimento e dados;

d) Dados: campo de dados com comprimento variável, podendo ter zero *byte* de comprimento ou mais dependendo do tipo de pacote, conforme o valor do campo de código.

As trocas de dados EAP são compostas de requisições e respostas. A requisição é enviada pelo *authenticator* para o *supplicant* do sistema buscando acesso. Baseado na resposta recebida o acesso pode ser permitido ou proibido. O campo de dados é utilizado para troca de informações durante as requisições e respostas, cada campo de dado carrega um tipo de informação, distribuído em dois campos:

a) Tipo: campo de um *byte* que indica o tipo de requisição e resposta. Os tipos de código 1 a 3 significam: Identidade, Notificação e NAK (utilizado para sugerir novo método de autenticação). Os campos de tipo com valores maiores ou iguais a 4 identificam o método de autenticação;
b) Tipo-Dado: campo variável cujo valor varia de acordo com o tipo de requisição e a resposta associada.

Na conclusão da troca de dados EAP o usuário poder ter sido autenticado com sucesso ou pode ter falhado na autenticação. Uma vez que o *authenticator* determina que a troca de dados esteja completa ele pode enviar um pacote de sucesso (código igual a 3) ou de falha (código igual a 4) para finalizar o diálogo.

As figuras 5.11 e 5.12 ilustram os pacotes EAP genéricos e os pacotes EAP de requisição e resposta.

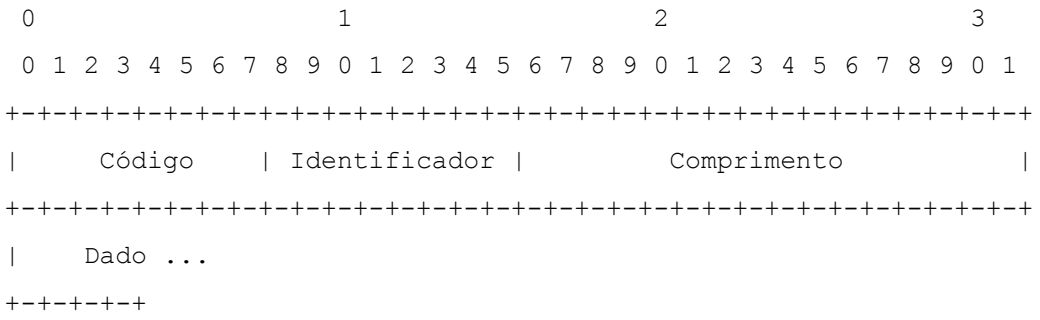


Figura 5.11 – Pacote EAP (IETF, modificado [9])

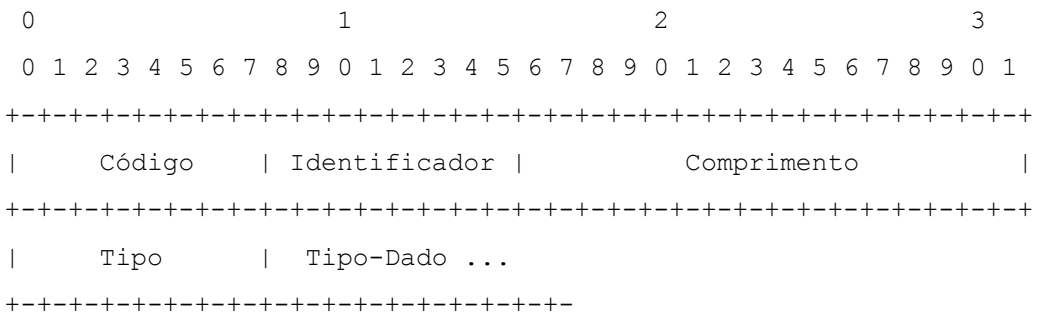


Figura 5.12 – Pacote EAP de requisição e resposta (IETF, modificado [9])

Os pacotes de sucesso ou de falha possuem o campo de dados com comprimento igual a zero.

5.2.3 – Autenticação EAP-SIM

O protocolo EAP-SIM [10] é um mecanismo que utiliza o protocolo EAP para autenticação e distribuição de chaves utilizando o cartão SIM e o processo de autenticação definido para a rede GSM.

O EAP-SIM utiliza o mecanismo de desafio e resposta definido para o GSM, utilizando o algoritmo A3/A8 de autenticação e derivação de chave que roda no cartão SIM. O desafio dado ao cartão SIM é um número randômico de 128 *bits* (RAND). O algoritmo do cartão SIM utiliza o RAND e a chave *Ki*, armazenada internamente, como entrada para produzir uma resposta de 32 *bits* (SRES) e uma chave longa de 64 *bits*, *cipher key* (*Kc*), como saída. A chave *Kc* na rede GSM é utilizada para criptografia da *interface* aérea e no protocolo EAP-SIM é utilizada para derivar outras chaves. Um dos pontos fundamentais deste protocolo é a manutenção do segredo a chave *Kc* para garantir a segurança geral do sistema.

Uma das fraquezas da autenticação GSM é a falta de autenticação mútua, no protocolo EAP-SIM o cliente no terminal oferece um número randômico para a rede (NONCE_MT) de forma a contribuir para a derivação de chaves e também como um desafio do terminal para a rede. A chave *Kc* de 64 *bits* derivada originalmente não é forte o bastante para rede de dados de suporte dos acessos IEEE 802.11, desta forma, no EAP-SIM diversos números desafio RAND são utilizados para gerar diversas chaves *Kc* que são combinadas para constituir um conjunto mais forte de chave.

A figura 5.13 ilustra o procedimento de autenticação completa EAP-SIM. Geralmente na arquitetura utilizada com o protocolo EAP-SIM o *authenticator* se comunica com um servidor EAP localizado em um servidor AAA remoto, através de algum protocolo AAA. Na figura 5.13 o *authenticator* simplesmente encaminha as mensagens EAP para o servidor EAP remoto, mas esta comunicação não é mostrada. O procedimento completo de autenticação utilizando o servidor AAA baseado em protocolo RADIUS [11], tal como utilizado para a modelagem realizada neste trabalho, está descrito no capítulo 6 deste documento e ilustrado na figura 6.4.

Figura 5.13 – Autenticação completa EAP-SIM (IETF, modificado [10])

A primeira mensagem enviada pelo *authenticator* requisita a identidade do cliente, através de um pacote *EAP-Request* com tipo *Identity*. No procedimento de autenticação completa a resposta do *supplicant* inclui o valor do IMSI do cartão SIM no formato *Network Access Identifier* (NAI) definido pelo IETF em [63] e que geralmente consiste no valor numérico do IMSI seguido do domínio da operadora de rede do cartão SIM. O *authenticator* continua o diálogo enviando o primeiro pacote EAP-SIM, com subtipo *Start*, *EAP-Request/SIM/Start* com atributo (AT_VERSION_LIST) listando as versões de EAP-SIM suportadas pelo servidor EAP. O cliente responde com um número randômico no atributo NONCE_MT e com o número de versão suportado selecionado no atributo AT_SELECTED_VERSION. Com a identidade do *supplicant* o servidor EAP requisita dois ou três vetores de autenticação (*GSM triplets*) ao elemento AuC da rede GSM. Os

vetores de autenticação contêm os valores RAND, *Kc* e SRES. Os *triplets* podem ser armazenados no servidor EAP, mas não podem ser reutilizados [10].

A próxima requisição é um pacote *EAP-Request/SIM/Challenge* que contêm o desafio RAND e o atributo de código de autenticação AT_MAC. O *supplicant* roda o algoritmo de autenticação GSM e calcula sua cópia do código de autenticação e verifica o valor contra o MAC recebido. Como a geração do código MAC utiliza o valor NONCE_MT com uma das entradas o *supplicant* é capaz de verificar que a mensagem recebida não é uma cópia e que o servidor EAP possui os *triplets* corretos. Estando os valores corretos, o *supplicant* retorna o desafio com um atributo AT_MAC cobrindo o valor SRES calculado pelo cartão SIM. O servidor EAP verifica se o valor MAC está correto e retorna uma mensagem *EAP-Success* em caso afirmativo.

As chaves da sessão não são passadas do servidor EAP para o terminal, pois o *supplicant* é capaz de derivar as mesmas com base nos atributos recebidos.

O pacote EAP-SIM tem o campo Tipo dentro do campo de Dados preenchido com o valor decimal 18. A seguir, o cabeçalho EAP-SIM possui o campo Subtipo de 1 *byte*, que indica o subtipo da mensagem e 2 *bytes* de campo reserva, conforme figura 5.14.

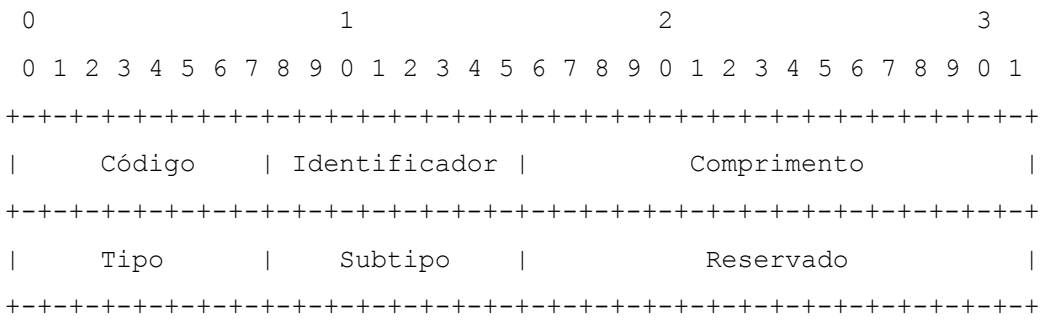


Figura 5.14 – Cabeçalho pacote EAP-SIM (IETF, modificado [10])

O restante do campo Tipo-Dado que segue o cabeçalho EAP-SIM consiste nos atributos que são codificados nos campos Tipo, Comprimento e Valor. A figura 5.15 mostra o formato genérico de um atributo.

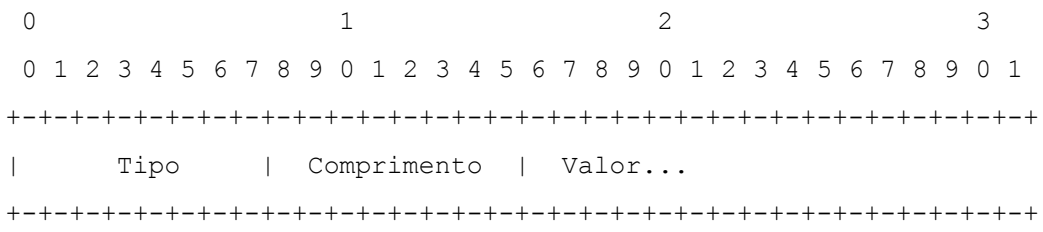


Figura 5.15 – Formato atributo EAP-SIM (IETF, modificado [10])

O padrão definido pelo IETF para o EAP-SIM [10] descreve também um método opcional de realizar a re-autenticação do *supplicant* sem a necessidade do servidor EAP buscar novos vetores de autenticação no HLR/AuC. Este método, chamado de re-autenticação rápida ou *fast re-authentication*, pode ser utilizado por usuários que retornam de forma frequente a mesma rede WLAN e além de não necessitar de novos *triplets*, não faz uso dos algoritmos A3/A8. A sua implementação é opcional tanto no *supplicant* quando no servidor EAP e caso alguns dois elementos não deseje, o processo de autenticação pode retornar para o processo de autenticação completa.

A re-autenticação rápida é baseada nas chaves derivadas do procedimento de autenticação completo anterior. Ele utiliza também um contador de 16 *bits* sem sinal, cujo valor é incluído no atributo AT_COUNTER. Este contador tem três objetivos básicos: limitar o número de re-autenticações rápidas consecutivas; contribuir com a derivação de chaves; e, proteger o servidor EAP e o *supplicant* contra fraude de reenvio de mensagem de autenticação. Na primeira re-autenticação o contador deve ter o valor de pelo menos um e nas tentativas consecutivas o contador deve ter o valor sempre maior que qualquer das tentativas anteriores.

No procedimento de re-autenticação rápida o *supplicant* utiliza uma identidade separada e distinta que é informada pelo servidor EAP no atributo AT_NEST_REAUTH_ID na mensagem *EAP-Request/SIM/Challenge* trocada na autenticação anterior. Cada nova identidade de re-autenticação rápida deve ser utilizada somente uma vez pelo *supplicant*. O atributo de identidade retornado ao *supplicant* contém também um *flag* que indica que o servidor EAP suporta re-autenticação rápida e que deseja continuar a utilizá-la dentro do contexto corrente. O uso da identidade de re-autenticação rápida indica o desejo do *supplicant* de realizar uma re-autenticação rápida. Caso o *supplicant* utilize a identidade

permanente ou o pseudônimo na autenticação, a mesma será realizada via os procedimentos de autenticação completa.

O procedimento de re-autenticação rápida é ilustrado na figura 5.16. O *supplicant* retorna a identidade na mensagem *EAP-Response/Identity*. Caso o servidor reconheça a identidade como uma identidade válida e aceite realizar a re-autenticação rápida ele reponde com uma mensagem *EAP-Request/SIM/Re-authentication*. Esta mensagem deve incluir o atributo cifrado AT_COUNTER, com um valor novo do contador, o atributo cifrado AT_NONCE_S, com um número randômico escolhido pelo servidor, os dados usados para criptografia nos atributos AT_ENCR_DATA e AT_IV e o atributo AT_MAC calculado sobre o pacote EAP completo. A mensagem pode também incluir o atributo AT_NEXT_REAUTH_ID com a próxima identidade para re-autenticação rápida.

O *supplicant* verifica se o valor do AT_MAC está correto e que o valor do contador recebido é novo. Caso as verificações estejam bem sucedidas o supplicant responde com uma mensagem *EAP-Response/SIM/Re-authentication*, incluindo o atributo AT_COUNTER recebido e o atributo AT_MAC. O servidor verifica estes valores e em caso de sucesso o servidor retorna uma mensagem *EAP-Success* para indicar ao *supplicant* que a re-autenticação rápida foi bem sucedida.

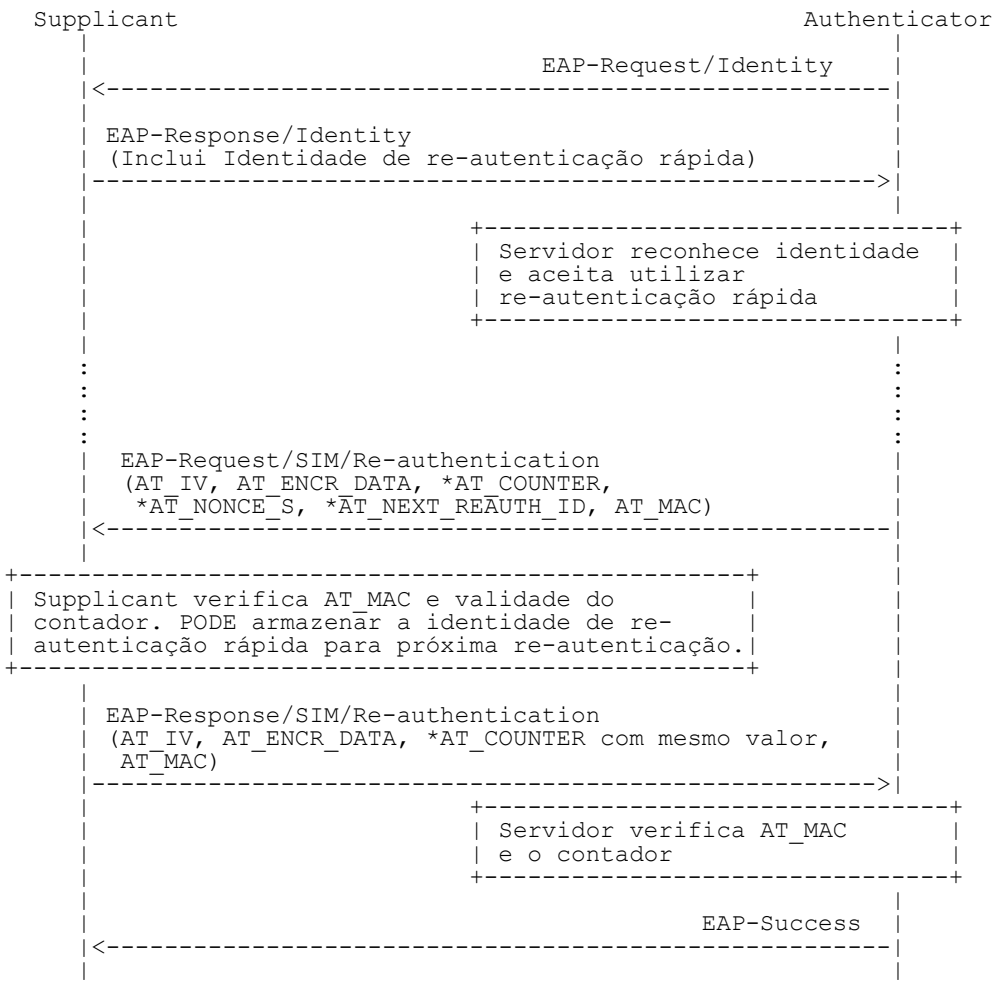


Figura 5.16 – Procedimento de re-autenticação rápida (IETF, modificado [10])

5.2.4 – Autenticação EAP-AKA

O protocolo EAP-AKA [28] é um mecanismo que utiliza o protocolo EAP para autenticação que utiliza o método *Authentication and Key Agreement* (AKA). O método AKA é baseado em mecanismo de chaves simétricas, no paradigma de desafio e resposta, e é utilizado em redes UMTS e CDMA2000. O AKA tipicamente roda sobre o cartão USIM (*UMTS Subscriber Identity Module*) e foi originalmente desenvolvido pelo 3GPP na especificação TS 33.102.

A arquitetura para o EAP-AKA é a mesma da utilizada com o EAP-SIM, com o *supplicant* no terminal utilizando as chaves e algoritmos do cartão USIM, um *authenticator* na rede WLAN, geralmente integrado no AP, e um servidor EAP remoto, implementando AAA e

capaz de requisitar vetores de autenticação do HLR/AuC da rede UMTS caseira do usuário [16].

Quando realiza o procedimento de autenticação completa pode haver uma troca de mensagens de requisição/resposta de identidade entre o terminal e o servidor EAP. Geralmente a identidade é o valor do IMSI do cartão USIM seguindo o formato NAI [63] e orientações dadas em [28].

Após obter a identidade do assinante o servidor EAP requisita o vetor de autenticação para o elemento AuC da rede móvel do usuário. O vetor de autenticação é composto dos valores RAND, AUTN, RES, CK e IK conforme descrito anteriormente neste capítulo. Diversos vetores do mesmo assinante podem ser requisitados ao mesmo tempo e eles podem ser armazenados no servidor EAP, mas não podem ser reutilizados [28].

Segundo a recomendação IETF RFC 4187 [28], o servidor EAP realiza a concatenação dos valores de identidade, IK e CK e aplica uma função *hash* referenciada em [28] para derivar uma *Master Key* (MK). A MK é alimentada em uma função de número pseudoaleatório que gera chaves transientes EAP (TEKs) para proteção dos pacotes EAP, uma *Master Session Key* (MSK) de 64 *bytes* para segurança da camada de enlace e uma *Extended Master Session Key* (EMSK) de 64 *bytes*.

O EAP-AKA necessita de duas chaves TEKs para uso próprio, uma chave de autenticação *K_aut* (128 *bits*) para ser utilizada com o atributo AT_MAC e uma chave de criptografia *K_encr* (128 *bits*) para ser utilizada com o atributo AT_ENCR_DATA [28].

Após, o servidor EAP inicia o protocolo AKA com o envio de pacote *EAP-Request/AKA/Challenge*, contendo o número randômico RAND no atributo AT_RAND, um atributo com *token* de autenticação de rede ou parâmetro AKA AUTN no atributo AT_AUTN, e mensagem de código de autenticação no atributo AT_MAC.

O *supplicant* roda o algoritmo AKA presente no cartão USIM e verifica o valor AUTN recebido, como forma de autenticar o servidor EAP. Em seguida, calcula o parâmetro RES e envia pacote *EAP-Response/AKA/Challenge* com os atributos AT_RES e AT_MAC para poder ser autenticado pelo servidor EAP.

O servidor EAP verifica se os valores de RES e MAC recebidos estão corretos e em caso afirmativo retorna pacote *EAP-Success* para o *supplicant*. Tal como no EAP-SIM, o EAP-AKA não realiza troca de chaves entre o terminal e o servidor EAP, pois as mesmas são derivadas com base na chave predefinida no AuC e no cartão USIM. O servidor EAP pode incluir alguma informação de chave nas mensagens de AAA trocadas com o *authenticator* [28].

A figura 5.17 ilustra um procedimento bem sucedido de autenticação completa, conforme descrito acima.

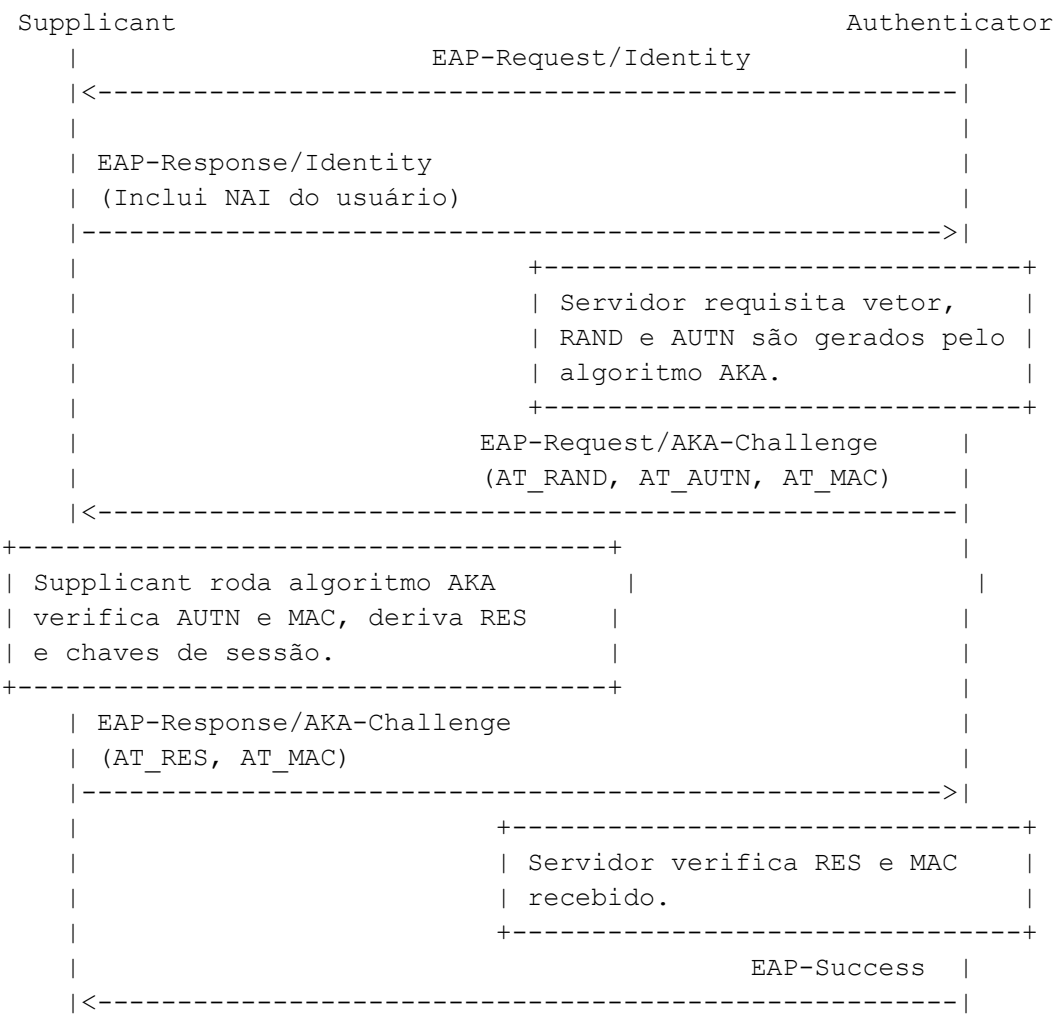


Figura 5.17 – Autenticação completa EAP-AKA (IETF, modificado [28])

O formato do cabeçalho e atributos do pacote EAP-AKA são os mesmos definidos para EAP-SIM e ilustrados nas figuras 5.14 e 5.15. Para o EAP-AKA o campo Tipo dentro do campo de Dados do pacote EAP é preenchido com o valor decimal 23.

5.2.5 – AAA RADIUS

O acrônimo AAA significa autenticação, autorização e contabilização (*Authentication, Authorization* e *Accounting*) e RADIUS (*Remote Authentication Dial In User Service*) é um protocolo definido pelo IETF [11] para transportar as funções de AAA. O protocolo RADIUS permite que um servidor de acesso de rede possa acessar um servidor centralizado e compartilhado para buscar serviços de AAA [66].

A arquitetura RADIUS define um cliente RADIUS, geralmente localizado no servidor de acesso da rede, que se comunica com um servidor RADIUS em nome do usuário final. Um exemplo típico é a arquitetura do domínio PS de uma rede 3GPP, nela, o elemento GGSN age como um servidor de acesso de rede e é, entretanto um cliente RADIUS que comunica com o servidor RADIUS da rede GPRS [21]. O protocolo RADIUS é não é utilizado para o transporte fim a fim de dados de autenticação, o mecanismo real de autenticação entre a rede de acesso cliente e o servidor de acesso é algum outro protocolo, tais como: autenticação PPP utilizando CHAP [66] ou algum dos métodos definidos para EAP [9].

O protocolo RADIUS provê as seguintes funções [66]:
a) Autenticação: determinação da identidade de um usuário através de segredo compartilhado;
b) Autorização: permitir ou rejeitar o acesso de usuário na rede baseado no seu perfil e nas políticas vigentes de segurança;
c) Configuração de *host*: prover dados de configuração para usuários conectando no servidor de acesso à rede, por exemplo: informando endereço IP para uso pelo *host*;
d) Contabilização: controle de estatísticas de uso para efeito de contabilização.

A arquitetura RADIUS permite que o usuário conectando na rede requisite uma gama de serviços diferenciados, por exemplo: conexão direta a um servidor via *telnet*.

A autenticação e autorização ocorre com o servidor de acesso de rede, ou cliente RADIUS, construindo uma mensagem *access-request* para envio ao servidor RADIUS. Esta mensagem contém a identificação do usuário, senha e informação sobre o tipo de serviço sendo requisitado. A senha é mandada de forma oculta como uma chave codificada.

Ao receber o *access-request,* o servidor RADIUS pesquisa a identidade do usuário em um bando de dados e recupera a senha para comparação de autenticidade. Em caso de confirmação da identidade do usuário uma mensagem *access-accept* é retornada para o cliente RADIUS. Em caso de não atendimento de alguma condição de acesso informada uma mensagem *access-reject* é retornada. Caso a identidade do usuário não seja encontrada na base de dados a requisição de acesso é descartada silenciosamente.

Há também a possibilidade do servidor RADIUS gerar uma mensagem *access-challenge* em resposta à requisição original. Neste caso se espera que o cliente RADIUS reenvie mensagem original de requisição respondendo o desafio encontrado na mensagem *access-challenge*. Como resposta, o servidor RADIUS pode aceitar ou rejeitar o pedido de acesso [66].

5.2.6 – Padrão IEEE 802.1x

O padrão IEEE 802.1x [7] foi desenvolvido com o objetivo de definir um método padronizado para permitir autenticação e autorização de dispositivos conectados em uma porta de rede LAN com características de conexão ponto-a-ponto, de forma a prevenir o acesso a esta porta em caso de falha no processo de autenticação e autorização.

O padrão IEEE 802.1x define três componentes para autenticação, conforme mostrado na figura 5.18. O *supplicant* é o equipamento na ponta final que necessita utilizar os recursos de rede. O *authenticator* que controla o acesso à rede. O *supplicant* e o *authenticator* são também referenciados como *Port Authentication Entities* (PAEs). O *authenticator* termina a camada de enlace nas trocas de autenticação e não mantêm nenhuma informação de usuário, sendo que toda requisição de entrada é passada para um servidor de autenticação para processamento [57]. O servidor de autenticação pode ser um servidor RADIUS ou similar.

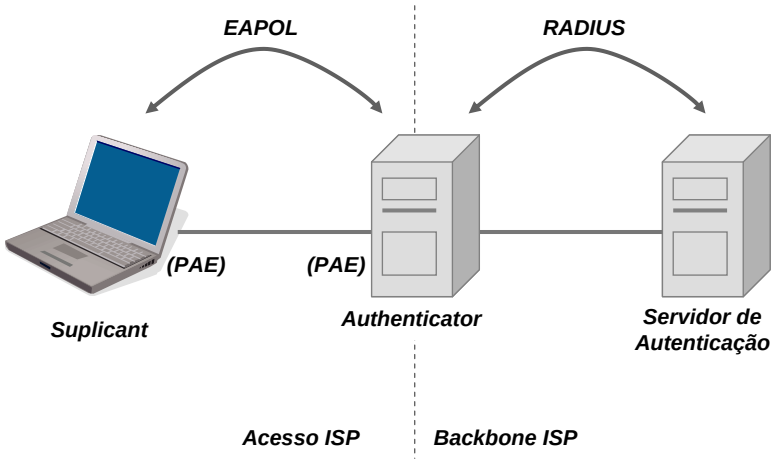


Figura 5.18 – Arquitetura IEEE 802.1x (Gast, modificado [57])

O *authenticator* controla o conjunto de portas através das quais os *supplicants* podem se autenticar. O padrão define dois tipos de portas: a porta controlada, que permite a troca de dados somente se estiver no estado autorizado, e; a porta não controlada, que permite a troca de dados que forma indistinta e é utilizada para acesso a recursos específicos (por exemplo: servidor de DHCP) [57]. As portas na qual pode ser desejável a utilização de autenticação incluem as portas utilizadas para conectar servidores e roteadores na infraestrutura LAN e associações entre estações móveis e AP em redes WLAN 802.11 [7].

O processo de autenticação entre o *supplicant* e o servidor de autenticação é definido para ser feito sobre o protocolo EAP, descrito anteriormente neste capítulo. Entre o *authenticator* e o servidor de autenticação a mensagem EAP é encapsulada em protocolo AAA, tal como RADIUS. Para o transporte e encapsulamento de pacotes EAP sobre rede LAN entre o *supplicant* e o *authenticator* o padrão 802.1x define o protocolo *EAP over LAN* (EAPOL).

O formato do pacote EAPOL para ser utilizado em redes *Ethernet* LAN com ou sem fio é representado na figura 5.19, sendo o mesmo transportado diretamente sobre o quadro *Ethernet* apropriado. Os tipos de pacotes que podem ser transportados pelo EAPOL são indicados no campo *Packet Type* do protocolo e são encapsulados no campo *Packet Body*, conforme descritos na tabela 5.1.

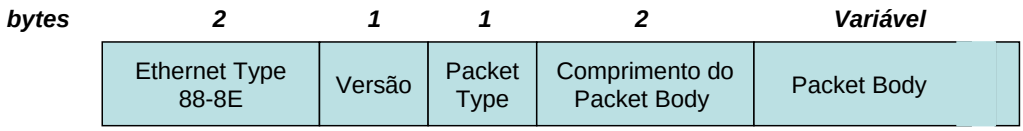


Figura 5.19 – Formato do pacote EAPOL (Gast, modificado [57])

Tabela 5.1 – Tipos de mensagens EAPOL (Gast, modificado [57])

Packet Type	**Nome**	**Descrição**
00	*EAP-Packet*	Indica que o *Packet Body* contém um pacote EAP.
01	*EAPOL-Start*	Utilizado pelo *supplicant* para avisar o *authenticator* que deseja iniciar a autenticação. Como resposta o *authenticator* envia pacote *EAP-Request/Identity*.
02	*EAPOL-Logoff*	Informa para retornar a porta para o estado de não autorizado.
03	*EAPOL-Key*	Pode ser usado para troca de chaves criptográficas.
04	*EAPOL-Encapsulated-ASF-Alert*	Permite que alertas, tais como *traps* SNMP, sejam enviadas por portas em estado não autorizado. Segue definição do *Alerting Standards Forum* (ASF).

O padrão IEEE 802.1x é um *framework* e não uma especificação completa. O padrão 802.1x fornece um mecanismo para prover desafios e confirmar ou bloquear acesso, mas não realiza nenhum julgamento sobre as credenciais oferecidas. Mudanças nos métodos de autenticação não requerem alterações complexas nos dispositivos ou infraestrutura de rede. O real mecanismo de autenticação é implementado pelo servidor de autenticação [57].

5.2.7 – Padrão IEEE 802.11i

O padrão IEEE 802.11i [32] é um suplemento do padrão 802.11 definindo mecanismos de segurança. Sua arquitetura utiliza como componente para autenticação o padrão IEEE 802.1x, incluindo o uso de protocolo EAP e servidor de autenticação.

O 802.11i define uma arquitetura robusta e segura de rede, chamada de *Robust Security Network* (RSN), capaz de estabelecer associação robusta ou *RSN Association* (RSNA) entre suas entidades. A RSN define os seguintes recursos de segurança adicionais ao WEP [32]:

a) Mecanismos melhorados de autenticação para as estações;
b) Algoritmos de gerenciamento de chaves;
c) Estabelecimento de chaves criptográficas;
d) Mecanismo melhorado de encapsulamento de dados com protocolo CCMP e, opcionalmente, protocolo TKIP.

O protocolo *Temporal Key Integrity Protocol* (TKIP) é uma melhoria do WEP e foi desenvolvido para utilizar os equipamentos existentes, sem necessidade de troca de *hardware*. Este protocolo foi primeiramente utilizado pelo mecanismo *Wi-Fi Protected Access* (WPA) definido pela entidade *Wi-Fi Alliance* (WFA) como uma alternativa às fragilidades descobertas no WEP anterior à finalização dos trabalhos do grupo de trabalho (*Task Group*) do IEEE 802.11i [57].

O protocolo *CTR with CBC-MAC Protocol* (CCMP), onde CTR significa *counter mode* e CBC-MAC significa *cipher-block chaining with message authentication code*, é mandatório para atendimento da arquitetura RSN e provê confidencialidade, autenticação, integridade e proteção contra *replay* para os dados encapsulados transmitidos. O CCMP é baseado no algoritmo de criptografia *Advanced Encryption Standard* (AES) e combina CTR para confidencialidade e CBC-MAC para autenticação e integridade [32].

O 802.11i prevê o uso do padrão IEEE 802.1x, EAPOL e de um mecanismo de gerência de chaves chamado de *4-Way Handshake* para autenticação das estações e gerência de chaves de criptografia, de maneira a evitar o reuso de chaves compartilhadas de forma indefinida. A forma geral de operação é ilustrada na figura 5.20. Inicialmente a estação realiza o *scanning* da rede WLAN, após conectar no AP selecionado a estação realiza autenticação utilizando o método de sistema aberto (*open-system*) e a associação. Quando a associação é estabelecida, a estação móvel e a rede se autenticam entre si utilizando um dos métodos descritos no padrão 802.1x. Na sequência a estação móvel ou *supplicant* e o servidor de autenticação ou servidor EAP geram a chave *Pairwise Master Key* (PMK) que é enviada do servidor de autenticação para o AP ou *authenticator* via um canal seguro. Por fim o *4-Way Handshake* é executado, utilizando quadros *EAPOL-Key*, entre o AP e a estação móvel para derivar e instalar uma chave transiente, *Pairwise Transient Key* (PTK), e a chave *Group Temporal Key* (GTK). Toda esta comunicação é realizada através da porta 802.1x não controlada, visto que a porta controlada está ainda em estado não autorizado. O

estabelecimento de associação segura e a autorização para uso da porta controlada é alcançado com a realização do *4-Way Handshake*. Em caso do *authenticator* alterar a GTK o protocolo *Group Key Handshake* é encarregado de atualizar a estação móvel [32].

A definição da autenticação e protocolo seguro entre o *authenticator* e o servidor de autenticação está fora do escopo do padrão 802.11i, mas devem ser atendidas as seguintes premissas: autenticação mútua entre o *authenticator* e servidor de aplicação, e garantir a integridade e confidencialidade da chave passada para o *authenticator* [32].

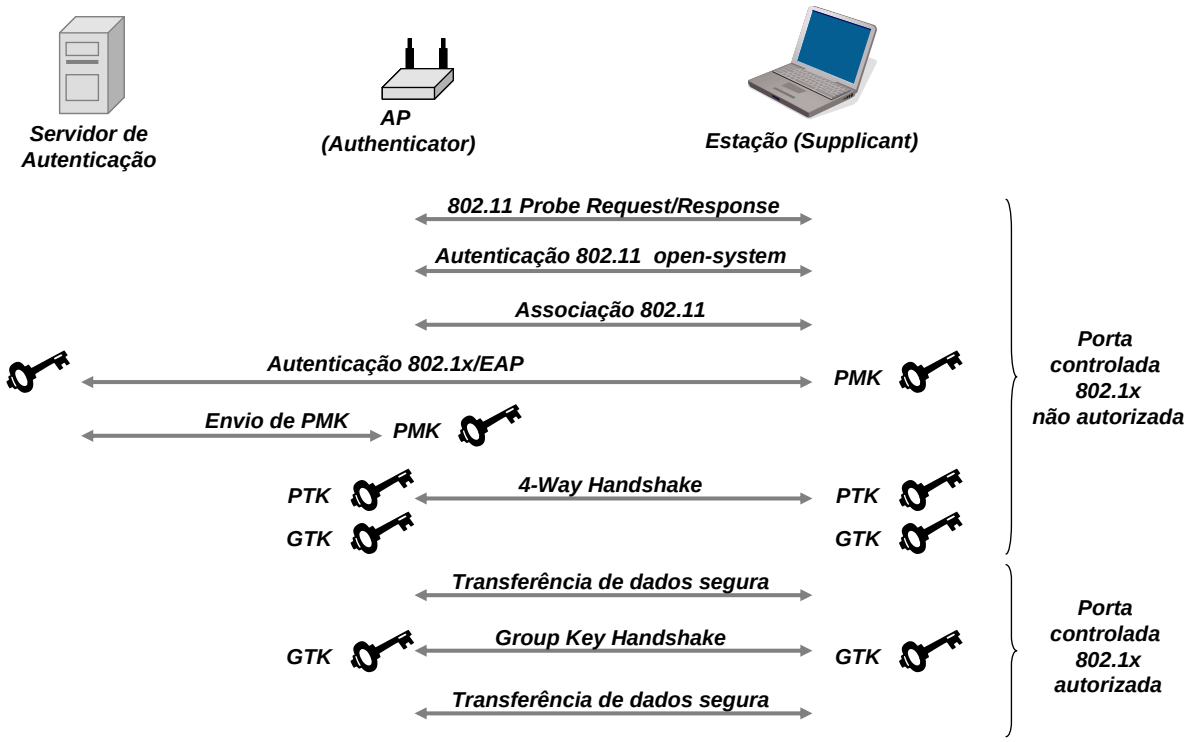


Figura 5.20 – Autenticação e Gerência de Chaves IEEE 802.11i (Al Naamany, modificado [64])

As chaves PTK e GTK são usadas para extrair chaves temporais para os protocolos CCMP e TKIP, de acordo com a configuração da rede, com o objetivo de proteger os tráfegos de dados *unicast*, *multicast* e *broadcast* [32].

5.3 – ARQUITETURAS PARA ROAMING WLAN

Com a abrangência das redes WLAN surgiu necessidade de se definir arquiteturas para permitir *roaming* entre as diferentes redes. Tomando como base o arcabouço de

padronização oferecido pelo IEEE e IETF, algumas iniciativas surgiram para definir um escopo mínimo de requerimentos e interfaces. Entre estas, podemos citar a iniciativa IRAP (*International Roaming Access Protocols*), descrita abaixo, e as orientações propostas pelo GSMA (*GSM Association*) no documento IR.61 [80].

O programa original para o desenvolvimento da iniciativa IRAP começou como uma colaboração entre o fabricante *Intel* e o a autoridade de desenvolvimento de Singapura IDA (*Infocomm Development Authority of Singapore*). A iniciativa original previa o desenvolvimento e validação de uma arquitetura completa fim-a-fim, baseada em padrões reconhecidos, para *roaming* de dispositivos entre redes WLAN e entre redes WLAN e WWAN [65]. Esta iniciativa original se transformou em uma entidade formada por fabricantes e operadoras de redes WLAN que foi responsável pela definição da arquitetura IRAP, descrita em [19].

A arquitetura IRAP visa definir um *framework* e as *interfaces* para redes de acesso WLAN (*hot spots*) com o objetivo de permitir *roaming* entre redes WLAN públicas, eliminado as barreiras técnicas para autenticação do usuário visitante na sua rede caseira e para cobrança do mesmo quando utilizar uma rede visitada [19]. Um dos princípios que norteiam especificação do IRAP é a utilização dos padrões existentes ou em desenvolvimento entre diferentes órgãos de padronização, tais como 3GPP, ETSI, IEEE, IETF e GSMA, em uma arquitetura concisa e prática.

Nenhum novo protocolo foi definido, mas sim reutilizado os trabalhos existentes com os padrões IEEE 802.1x [7] e 802.11i [32] em uma arquitetura de servidores AAA implementando o protocolo RADIUS [11]. O *framework* IRAP suporta métodos de autenticações baseadas no padrão IEEE 802.1x, bem como baseadas em UAM (*Universal Access Method*), que consiste no redirecionamento do tráfego HTTP para um portal de autenticação para o usuário se identificar manualmente através de informação de usuário e senha. A figura 5.21 ilustra o *framework* da arquitetura proposta e as premissas básicas adotadas.

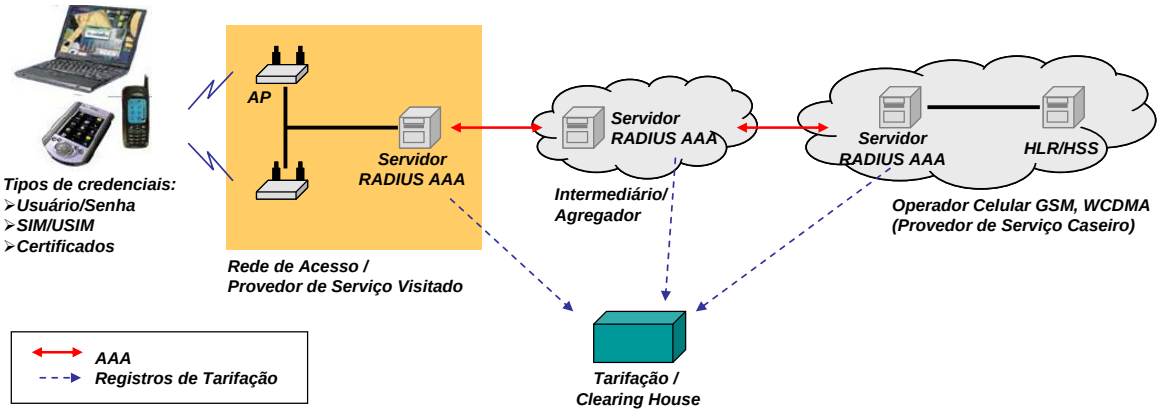


Figura 5.21 – *Framework* da arquitetura IRAP (IRAP, modificado [19])

Uma dos pontos principais da arquitetura é a definição de um conjunto de *interfaces* que possam suportar *roaming* seguro e com abrangência mundial. Estas *interfaces* devem definir um conjunto básico comum de recursos necessários para garantir interoperação e resolver ambiguidades no *roaming* em redes WLAN públicas. Um dos problemas atacados é a falta de perfil padronizado para interconexões AAA baseada em protocolo RADIUS. Este problema pode ser resolvido através de acordos bilaterais entre provedores de serviços interessados, mas esta solução não tem fator de escala, considerando um cenário de interconexão global entre múltiplos provedores de serviço. Um dos objetivos é evitar a existência de uma grande base instalada de redes fragmentadas e com implementações incompatíveis, conforme descrito em [19].

As *interfaces* padrões definidas preveem a troca de informações de autenticação, contabilização e gerência entre provedores de *roaming* em redes públicas WLAN. Na especificação IRAP, o termo *interface* é utilizado para indicar um protocolo ou um conjunto de protocolos e suas respectivas configurações e perfil entre dois sistemas [19].

Quatro *interfaces* foram propostas, conforme ilustrado na figura 5.22. Cada elemento de rede mostrado possui *interfaces* que podem necessitar se adequar ao padrão.

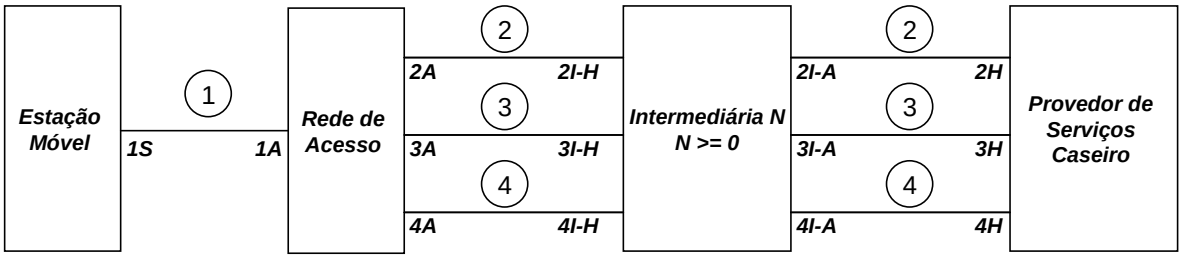


Figura 5.22 – *Interfaces* IRAP (IRAP, modificado [19])

Os termos “1S”, “1A” e assim por diante são utilizados para identificar as terminações das *interfaces*. “1S” refere à terminação da *interface* 1 que é suportada pela estação móvel e “1A” refere à terminação da *interface* 1 que é suportada pela rede de acesso. As demais terminações mostradas na figura 5.22 devem ser interpretadas de forma similar.

A descrição geral das *interfaces* é:
a) *Interface* 1: Estação Móvel para Rede de Acesso. Esta *interface* suporta clientes de autenticação baseados em navegadores *Web* e os métodos de nova geração definidos pelos padrões IEEE 802.1x e 802.11i;
b) *Interface* 2: Rede de Acesso para o sistema de autenticação da rede caseira do usuário. A *interface* 2 suporta conexões AAA para autenticação e autorização de serviços entre a rede visitada WLAN e a rede caseira do usuário em *roaming*.
c) *Interface* 3: Rede de Acesso para o sistema de tarifação da rede caseira do usuário. A *interface* 3 provê dados de contabilização para permitir a cobrança de forma escalar e consistente para múltiplas redes caseiras e modelos de cobrança. Devido à necessidade de suporte a auditoria, não-repudiação e gerência de fraude esta *interface* tem elementos comuns à *interface* 2;
d) *Interface* 4: Rede de Acesso para o sistema operacional da rede caseira do usuário. A *interface* 4 permite a segregação de falhas no momento em que elas ocorrem, via mecanismo de diagnóstico remoto.

Em muitos sistemas reais implantados podem ser envolvidos intermediários para os serviços de *roaming* e de contabilização. Estes intermediários também necessitam suportar as *interfaces* 2 e 3 e devem ser testados quanto à conformidade das mesmas.

A *interface* 3 trata dos aspectos de contabilidade do protocolo AAA e na maioria dos casos termina no servidor AAA da rede caseira do usuário final. Entretanto, a separação dos requerimentos de autenticação e autorização dos de contabilidade em duas *interfaces* possibilita à rede caseira realizar a terceirização dos aspectos de contabilização para outra entidade, através da *interface* 3 [19].

Para cada uma das *interfaces* listadas existe um conjunto de requerimentos definidos em [19], alguns dos quais são indicações de trabalhos em andamento dentro do IETF, principalmente no que diz respeito à necessidade de novos atributos no protocolo RADIUS.

A *interface* 1 tem como requerimento básico o suporte ao padrão IEEE 802.1x [7] e 802.11i [32], principalmente no que diz respeito à utilização de criptografia e segurança (WPA2). Outro requerimento fundamental é que todos os elementos a se interconectar através desta *interface* tenham certificação da WFA (*Wi-Fi Alliance*).

A *interface* 2 tem como requerimento básico o suporte ao protocolo RADIUS [11] e de algumas das extensões definidas para o mesmo, tais como: *accounting* e suporte a EAP. Um dos requisitos mais realçados é o suporte aos atributos *Idle-Timeout* e *Session-Timeout* para permitir a rede desconectar terminais sem atividade por longo período, bem como, terminais que tenha esgotado alguma temporização de sessão, como por exemplo: expiração de crédito de conta pré-paga. Estes requerimentos são válidos para a *interface* 2 da rede de acesso, da rede caseira e da rede intermediária.

A *interface* 3 tem como requerimento básico o suporte a RADIUS [11] e às extensões de *accounting*. Os requisitos principais a serem suportados são: mensagens de início e de fim de sessão (por desconexão, inatividade, temporização); envio de mensagens interinas de contabilização; identificação da sessão entre diferentes entidades físicas, e; envio de volta do atributo de identidade do usuário.

A *interface* 3 da rede intermediária necessita também ser capaz de realizar *proxy* da mensagens de *accounting*, podendo também introduzir algum atributo de classe caso necessário. Algumas extensões necessárias para a *interface* 3, prevendo suporte a contas pré-pagas e a localização do terminal ainda estão em discussão dentro do IETF [19].

A *interface* 4 ainda está em discussão no documento em referência [19], mas os requisitos a serem suportados são relacionados à monitoração e relatório de parâmetros de nível de serviço, ou SLA. A utilização de protocolos *in-band* tal como SNMP é prevista, bem como a notificação *out-of-band*, tal como com a utilização de mensagens via correio eletrônico.

A arquitetura IRAP é compatível com as recomendações do GSMA descritas no documento IR61[80] e foi utilizada como base para o padrão ETSI/TISPAN TS 183 020 [81] sobre roaming em acessos NGN. O que se verifica na prática é que as interfaces definidas pelo IRAP são muito complexas e foram resumidas para transportar as informações de autenticação, autorização e contabilização dos terminais em *roaming*. Como exemplo, no padrão ETSI referenciado acima, as interfaces entre a rede visitada, as redes intermediárias e a rede caseira são únicas, denominadas *e5*, e transportam somente informações de AAA (*Authentication, Authorization and Accounting*).

5.4 – ARQUITETURA 3GPP PARA INTERWORKING WLAN

Dentro do escopo dos trabalhos desenvolvidos pelo 3GPP está também incluída a definição de padrões para interoperação entre redes 3GPP e redes de acessos definidas por outras entidades de padronização, como por exemplo, redes de acesso WLAN. Estas definições e padrões têm o objetivo de definir arquiteturas e procedimentos para que terminais em redes não-3GPP, ou seja, não padronizadas pelo 3GPP, possam acessar serviços baseados em uma rede HPLMN que segue os padrões 3GPP.

A primeira padronização seguindo o exposto acima foi a definição de interfuncionamento de sistemas 3GPP e redes WLAN, como as baseadas no padrão IEEE 802.11. Este padrão é conhecido como I-WLAN ou *Interworking-WLAN* [4].

A especificação de arquitetura do I-WLAN [4] define dois novos procedimentos para sistemas 3GPP:
a) *WLAN Access, Authentication and Authorization*: que providencia que o acesso à rede WLAN e à rede IP localmente conectada possa ser autenticada e autorizada através de um sistema 3GPP;
b) *WLAN 3GPP IP Access*: permite que terminais WLAN possam estabelecer conectividade com redes IP externas através da rede de serviços de pacotes, ou domínio PS, do sistema 3GPP.

A arquitetura simplificada da rede I-WLAN é mostrada na figura 5.23.

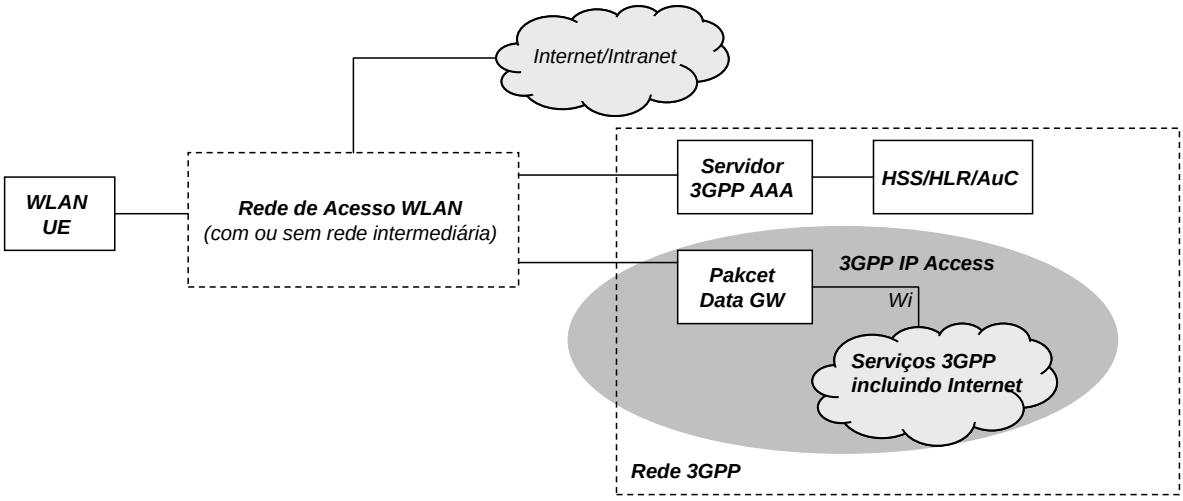


Figura 5.23 – Arquitetura I-WLAN simplificada (3GPP, modificado [4])

O elemento *Packet Data Gateway* (PDG) suporta acessos IP WLAN 3GPP para redes externas, a *interface* deste elemento para o acesso IP (*interface Wi*) é funcionalmente similar à *interface Gi* do domínio PS de um sistema 3GPP. A rede de acesso WLAN inclui pontos de acesso e elementos AAA intermediários, bem como elementos para garantir a conectividade IP. O WLAN UE (*User Equipment*) inclui todos os equipamentos em posse do usuário final, tais como computadores, terminais móveis, etc.

O padrão I-WLAN e concentra em definir as *interfaces* entre os elementos 3GPP e as *interfaces* entre o sistema 3GPP e a rede WLAN. A operação interna da rede WLAN é considerada somente para avaliação do impacto da arquitetura e requerimentos na WLAN. O I-WLAN deve ser independente da tecnologia de rádio da rede WLAN, segundo 3GPP [4].

Os requerimentos para o I-WLAN procuram minimizar os impactos na rede WLAN e nos sistemas 3GPP existentes, neste sentido é definido que os cartões SIM e USIM devem ser suportados, bem como os elementos HSS/HLR/AuC [4].

O procedimento de autenticação e autorização do terminal WLAN em uma arquitetura I-WLAN ocorre após o estabelecimento de conexão com a rede WLAN. A autenticação e autorização são baseadas na utilização de protocolo EAP-SIM [10] ou EAP-AKA [28] entre o terminal WLAN e o servidor 3GPP AAA, de acordo com os métodos descritos em [6]. O servidor 3GPP AAA realiza as funções de autenticação e autorização baseado nas

informações de autenticação e de perfil de serviços recuperadas do elemento HSS/HLR/AuC da rede 3GPP caseira do usuário.

O terminal informa a rede caseira de quais os serviços pretende utilizar através da utilização de APN (*Access Point Name*), descrito em [1], que neste caso é referenciado como W-APN [4]. O servidor 3GPP AAA autoriza o terminal a utilizar o serviço na rede 3GPP através da informação de W-APNs permitidas e subscritas informadas pelo elemento HSS/HLR. Caso o terminal selecione utilizar a conectividade direta da Internet pela rede de acesso WLAN nenhuma informação de seleção de serviço é informada para a rede caseira.

A conectividade IP para a rede de acesso WLAN 3GPP é realizada através do estabelecimento de túnel seguro entre o terminal WLAN e o PDG hospedado na rede 3GPP caseira do usuário, após a conclusão do procedimento de autenticação e autorização.

5.5 – EVOLUÇÕES PREVISTAS

Diversos organismos de padronização estão trabalhando na solução dos problemas evidenciados com a disseminação de redes heterogêneas e a necessidade de realização de *roaming* e *handover* entre as mesmas, tais como 3GPP, ETSI, IEEE e IETF.

O 3GPP tem concentrado seus esforços na definição de arquiteturas, protocolos e *interfaces* que permitam que os sistemas padronizados pelo 3GPP tenham interoperabilidade com outros sistemas e redes, tal como descrito previamente neste capítulo para a arquitetura I-WLAN.

O IEEE está definindo arquiteturas e protocolos para facilitar o *handover* de terminais em redes heterogêneas conforme é descrito na sequência para o padrão IEEE 802.21.

O IETF é responsável por definir vários protocolos para o desenvolvimento dos serviços de dados, incluindo as definições dos protocolos TCP/IP e, mais recentemente o protocolo SIP. Com relação ao aspecto de mobilidade, o IETF foi responsável pelas definições do padrão *Mobile IP* (MIP) adotado como solução de mobilidade de serviços de dados em redes móveis CDMA. O IETF possui atualmente o grupo HOKEY (*Handover Keying*) com

objetivo de detalhar os problemas relativos à derivação e distribuição de chaves de criptografia em redes que utilizam autenticação baseada em EAP e na definição de protocolos para re-autenticação e distribuição de chaves para o suporte a *roaming* e *handover*. O HOKEY está ainda evoluindo os trabalhos e maiores informações podem ser encontradas em [83].

5.5.1 – Padrão IEEE 802.21

O padrão 802.21 (*Media Independent Handover*) desenvolvido e publicado em 2009 pelo IEEE [8] [82] tem como objetivo definir especificação para prover inteligência na camada de enlace e informações para as camadas superiores de forma a otimizar os *handovers* entre redes heterogêneas. As camadas de enlaces previstas incluem as redes definidas pelo 3GPP, e as redes com fio e sem fio da família IEEE 802.x.

O padrão IEEE 802.21 prevê a cooperação entre os terminais móveis e a infraestrutura de rede para a realização do *handover* vertical. A infraestrutura de rede armazena em serviços de informação dados gerais de rede, incluindo lista de células vizinhas e localização de terminais móveis [71]. Desta forma, o processo de *handover* é sustentado por informações supridas da rede para o terminal, além das informações que o terminal coleta através da camada de enlace de rádio, tais como, medidas de qualidade de sinal, taxas de dados disponíveis, etc. O objetivo é suportar a decisão de *handover* com estes diversos dados de forma a contribuir para otimização dos algoritmos de *handover*.

O padrão IEEE 802.21 não define regras ou políticas para a decisão de *handover* nem determinar a forma de *handover* a ser utilizada, como por exemplo: iniciado pela rede ou iniciado pelo terminal. Sua finalidade é a de especificar uma arquitetura para facilitar esta decisão, mas as regras e políticas estão fora do escopo do padrão e sua definição é deixada a cargo do provedor de serviço [71].

A figura 5.24 mostra o modelo de referência para o *framework* proposto pelo IEEE com a localização das novas funções de MIH.

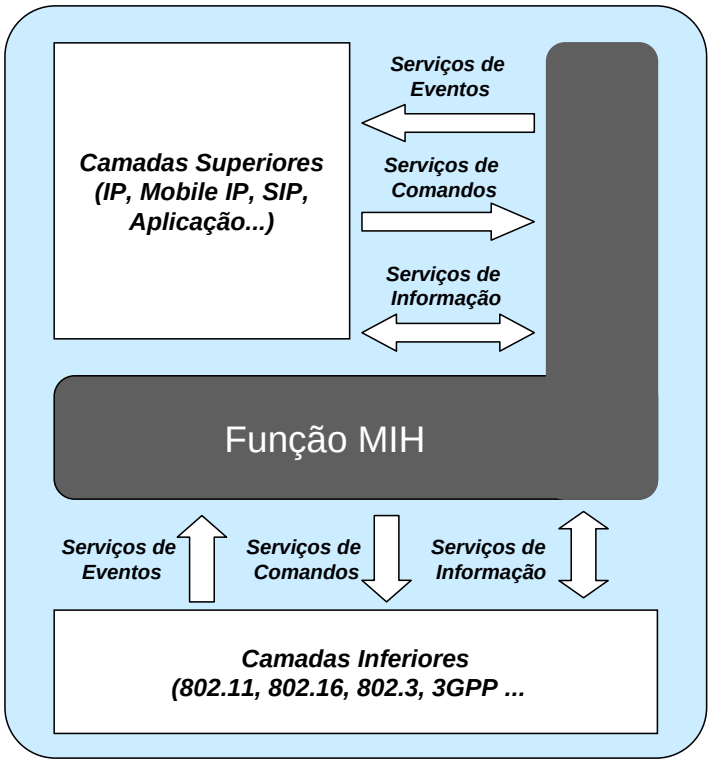


Figura 5.24 – Modelo de referencia 802.21 MIH (IEEE, modificado [8])

As funções do MIH provêm os seguintes serviços [8]:

a) Serviços de eventos (*Media Independent Event*) para detectar eventos e realizar disparos para as *interfaces* locais e remotas;

b) Serviços de comandos (*Media Independent Command*) oferecem um conjunto de comandos para usuários MIH controlar os estados de enlace relevantes para o *handover*;

c) Serviços de informação (*Media Independent Information*) provêm modelos e repositórios de informações para permitir a realização de decisões de *handover* de forma mais eficiente entre redes heterogêneas.

6 – ESTUDO DE CASO

No estudo de caso será verificado o atraso na execução de *handover* vertical entre redes WWAN e WLAN com o objetivo de avaliar e quantificar o tempo de interrupção do serviço decorrente do acréscimo do procedimento de:
a) Autenticação do terminal baseada nos padrões IEEE 802.1x [7] e IEEE 802.11i [32] com a utilização de protocolo EAP-SIM [10] pela rede WLAN.

O cenário acima será modelado analiticamente para várias condições e taxas de transmissão através da utilização dos modos IEEE 802.11b e IEEE 802.11g. Medidas realizadas em condições reais em redes comerciais serão utilizadas para gerar dados de entrada para a modelagem analítica.

O objetivo final é a avaliação do impacto da introdução na rede WLAN da autenticação baseada no padrão IEEE 802.11i no atraso da execução do *handover* vertical entre sistemas WWAN e WLAN oferecendo serviços convergentes multimídia, como por exemplo, os baseados na utilização do protocolo SIP. Este impacto pode ser responsável por efeitos indesejáveis do ponto de vista da percepção do serviço pelo usuário final, tais como interrupção da comunicação ativa e tempo elevado de indisponibilidade durante o processo de *handover*. Não é avaliado o tempo de *scanning* e de associação à rede WLAN, pois será adotada a premissa de que esta associação ocorrerá antes da desconexão do terminal da rede WWAN, este é um cenário típico de *soft handover* vertical entre redes heterogêneas e controlado pelo terminal. Com base nestas premissas temos que os tempos necessários para realização dos procedimentos de autenticação IEEE 802.1x e de conexão à camada 3 são diretamente responsáveis pelo atraso de *handover* e a interrupção da sessão.

A alternativa à proposta aqui apresentada é a não utilização de autenticação do terminal pela rede WLAN, via o padrão IEEE 802.11i, o que possibilita vantagens óbvias no tempo de resposta de *handover*, mas possui os seguintes problemas:
a) Necessidade o terminal/usuário saber as diferentes senhas de acesso para as redes protegidas unicamente por mecanismos de chave compartilhada, como por exemplo: WEP [31], e que são específicas de cada rede WLAN elegível de conexão;

b) Submissão do terminal aos mecanismos de segurança próprios implementados por cada rede WLAN, podendo ter estes diferentes níveis de segurança e proteção contra ataques e *eavesdropping* (interceptação da sessão por terceiros);
c) Necessidade de introdução manual de senha de acesso em redes utilizando UAM (*Universal Access Method*) [19], o que introduz significativo atraso e impede que o *handover* seja transparente (*seamless*) e automático para o usuário.

A inclusão de autenticação EAP-SIM nas redes WLAN em conjunto com a arquitetura IEEE 802.11i conforme proposto neste capítulo possibilita as seguintes vantagens na oferta de serviços convergentes:
a) Autenticação transparente do terminal sem necessidade de intervenção do usuário;
b) Autenticação mútua (rede-terminal e terminal-rede);
c) Autenticação através de mecanismo seguro de troca de chaves;
d) *Roaming* transparente entre redes WLANs de diferentes prestadoras de serviço.

A autenticação transparente na rede WLAN é um fator fundamental para permitir que o *handover* vertical também seja efetuado de forma transparente. O *roaming* transparente e automático assim possibilitado permite a abrangência da oferta do serviço e simplifica a utilização de redes WLAN pelo usuário, visto que ele não é mais obrigado a estabelecer relação comercial com cada novo prestador de serviço Wi-Fi dentro da sua área de movimento, nem a configurar diferentes senhas de acesso para cada rede WLAN visitada.

O processo de autenticação em redes WWAN baseadas nos padrões 3GPP, tais como GSM, UMTS e GPRS, utiliza de processos e algoritmos bem definidos pela literatura e padronizados pela indústria [26]. Os algoritmos A3 e A8 historicamente utilizados nas redes GSM são reutilizados com a introdução com o protocolo EAP-SIM. Devido a este fato, a introdução de autenticação EAP-SIM nas redes WLAN permite o reuso dos métodos já aplicados, mas não altera o processo de autenticação das redes WWAN baseadas nos padrões 3GPP.

Diferentemente do procedimento definido para o padrão IEEE 802.11i na rede WLAN [32], a autenticação na rede WWAN baseada nos padrões 3GPP ocorre durante o procedimento de conexão e registro do terminal à rede de acesso [60]. Sendo assim o

terminal somente é considerado conectado à rede após o procedimento de registro, cuja autenticação é uma das etapas.

Com a utilização do padrão IEEE 802.11i em redes WLAN, o terminal realiza a autenticação de sistema aberto antes da associação do terminal à rede, como parte do procedimento de conexão do terminal. Somente após a associação, ou seja, a conexão do terminal à rede WLAN ter sido realizada é que são iniciados os procedimentos de autenticação definidos pelo padrão IEEE 802.1x, conforme descrito no capítulo 5 do presente documento. Este mecanismo foi assim definido para manter a compatibilidade reversa com a máquina de estado definida para o padrão original IEEE 802.11 e para reutilização das estações móveis preexistentes [32].

Considerando o ponto acima, e a premissa inicial do terminal continuar conectado à rede anterior até o término da conexão ou associação à nova rede, verificamos que, o procedimento de autenticação na rede WWAN não provoca influência no tempo de atraso de *handover* e, devido a isso, o processo de *handover* no sentido WLAN para WWAN não será deduzido analiticamente. Valores medidos em rede real do atraso de conexão e autenticação em redes WWAN serão utilizados somente como referência de comparação.

6.1 – ARQUITETURA E ELEMENTOS FUNCIONAIS

Os requisitos básicos para este estudo de caso foram selecionados como o objetivo de permitir a aplicação em redes reais. Parte deste estudo foi realizada com base em modelagens analíticas, com a utilização de dados medidos em elementos operando em redes reais de telecomunicações como fonte de entrada. Como resultado, se espera que os resultados alcançados possam ser de auxilio para a definição de especificações técnicas e a implantação comercial de redes convergentes na futura oferta de serviços de dados e voz em redes heterogêneas.

6.1.1 – Arquitetura Alvo

A arquitetura de rede escolhida para este estudo é completamente baseada nos padrões descritos nos capítulos iniciais deste trabalho e é descrita abaixo.

Para rede WWAN HPLMN será utilizada uma rede comercial GSM/GPRS/IMS, baseada nas especificações do 3GPP [21], e operada pela empresa Brasil Telecom GSM, com sede em Brasília, DF.

Para rede WLAN será utilizada rede baseada nos padrões IEEE 802.11b/g e autenticação baseada nos padrões IEEE 802.1x [7] e IETF EAP-SIM [10]. Serão considerados os cenários de autenticação e os princípios gerais de arquitetura definidos pelo 3GPP I-WLAN [4], mas a arquitetura utilizada será simplificada, considerando *interface* IP direta entre a rede de acesso WLAN e a rede HPLMN, de forma a não necessitar de procedimentos de estabelecimento de túneis fim a fim, como por exemplo: com o estabelecimento de conexões IPSec , para conexão entre o terminal e a rede HPLMN. Esta arquitetura está também alinhada com as recomendações e padrões para *roaming* WLAN discutida no capítulo anterior. A arquitetura utilizada segue também o conceito de acoplamento *loose coupling* descrito por Bresil em [16] e por ETSI em [20].

Como protocolo de autenticação da rede WLAN pode ser utilizado também o EAP-AKA [28], que oferece recursos se segurança melhorados ao EAP-SIM. O protocolo EAP-AKA é baseado nos algoritmos de autenticação definidos para as redes com tecnologia UMTS e em chaves gravadas em cartões UICC (*Universal Integrated Circuit Card*) com aplicação USIM (*Universal Subscriber Identity Module*) utilizado nos terminais móveis. Na elaboração deste trabalho, não eram conhecidos pelo autor implementações comerciais em terminais móveis que utilizavam o protocolo EAP-AKA.

Como o cenário previsto neste trabalho considera somente redes WWAN baseadas na tecnologia GSM e terminais que utilizam cartões baseados em aplicações SIM (*Subscriber Identity Module*), a utilização do protocolo EAP-AKA não será escopo do mesmo. Porém, os métodos desenvolvidos no presente trabalho são facilmente adaptados para o cenário de integração de redes WWAN baseadas em UMTS e de redes WLAN com autenticação baseada em EAP-AKA, o que será particularmente útil quando estas redes estiverem comercialmente disponíveis no cenário nacional.

O serviço sendo acessado pelo terminal durante o *handover* vertical é provido por uma rede 3GPP IMS [3] pertencente à HPLMN, com controle de sessão via protocolo SIP [14]. O atraso devido o novo registro SIP (via mensagem SIP REGISTER) ao serviço da rede

IMS após a conexão com a rede WLAN, durante o processo de *handover* vertical, não está incluído no escopo do estudo de caso, por não ser alterado pelo novo processo de autenticação, mas será descrito com o fim de servir de referência para trabalhos futuros. O novo registro SIP no serviço faz parte do procedimento de manutenção da informação de localização definido para a arquitetura IMS e é base do mecanismo de gerência de mobilidade baseado na utilização do protocolo SIP, como por exemplo, proposto por Wedlund e Schulzrinne em [15]. Uma avaliação deste atraso foi feita por Banerjee em [12].

O processo de manutenção da continuidade da sessão SIP é baseado em procedimentos disparados pelo terminal (SIP UPDATE ou RE-INVITE) diretamente para o destino ou para uma aplicação responsável pela função de transferência de domínio e é posterior ao *handover* vertical. No caso de continuidade de chamadas de voz entre os domínios CS e IMS foi desenvolvido e padronizado o serviço VCC (*Voice Call Continuity*) pelo 3GPP [2]. A aplicação VCC utiliza de um elemento lógico específico para realizar a função de transferência de domínio e facilitar a interoperação entre os domínios de circuito comutado e de multimídia (IMS). Com a utilização da funcionalidade VCC o *handover* vertical entre redes WLAN e WWAN significa também a troca da rede de transporte baseada comutação de pacotes IP para uma rede de transporte baseada em circuito comutado [2]. A arquitetura alvo utilizada neste estudo de caso comporta também os cenários de utilização da aplicação VCC, mas os procedimentos específicos de transferência de domínio para manutenção da continuidade da sessão estão além do escopo deste trabalho.

A figura 6.1 ilustra os blocos funcionais da arquitetura alvo do estudo de caso.

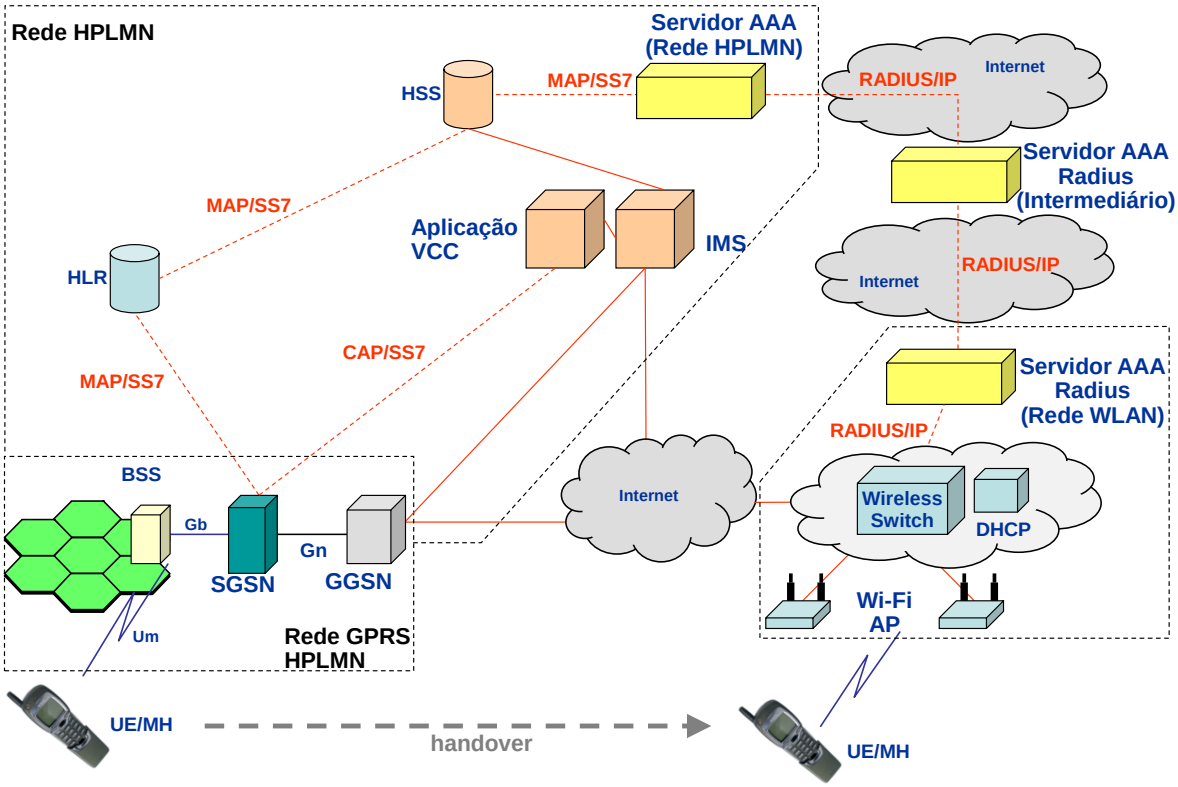


Figura 6.1 – Arquitetura alvo para o estudo de caso

O serviço de autenticação do terminal é oferecido através de servidor AAA (*Authentication, Authorization and Accounting*) baseado em protocolo RADIUS [11]. A rede de acesso WLAN é responsável por encapsular os pacotes EAP de autenticação gerados pelo terminal em pacotes RADIUS e direcioná-los para o servidor AAA. O servidor AAA identifica o terminal como sendo pertencente à rede HPLMN e é responsável por disparar requisição de autenticação para o HSS/AuC, como detalhado no seção 6.1.2.2.

Em condições de *roaming* entre redes WLAN e WWAN de operadores distintos o processo de autenticação é realizado entre os servidores AAA de cada operadora, ficando a cargo do servidor pertencente à operadora WWAN realizar a consulta ao HSS/AuC, para geração dos vetores de autenticação. Em casos mais complexos em que há acordos de *roaming* entre diversas operadoras WWAN e diversas operadoras distintas de WLAN, pode ainda existir um servidor intermediário pertencente a uma empresa responsável por realizar função de *clearing house* na contabilização dos registros de *accounting* e de roteamento das mensagens de autenticações, conforme descrito no capítulo 5 para a arquitetura de *roaming* WLAN. Os servidores da rede WLAN e intermediário de AAA são responsáveis

por realizar a função de *proxy* RADIUS, conforme definido em [11], e também por realizar registros das sessões ativas para efeito de cobrança. A figura 6.2 ressalta esta arquitetura.

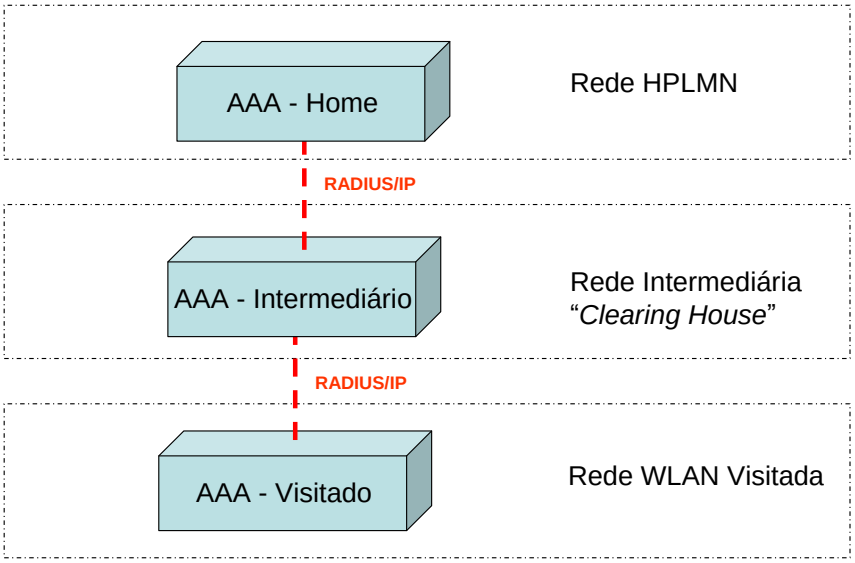


Figura 6.2 – Arquitetura de servidores AAA para cenário de *roaming*

A interconexão entre os servidores mostrados na figura 6.2 é realizada via rede IP dedicada ou via a Internet, podendo também utilizar mecanismo de segurança adicionais aos do protocolo RADIUS, como tunelamento baseados em protocolo IPSec [73]. A utilização de rede intermediária é prevista principalmente para os casos em que há um número muito elevado de operadoras WWAN e WLAN com interesse em realizar acordos de *roaming*, com o objetivo de simplificar a interconexão entre as diversas empresas, evitando a realização de conexões ponto a ponto entre elas.

Neste trabalho foi modelado matematicamente o cenário completo, incluindo o servidor AAA intermediário e como forma de conexão entre os servidores AAA foi considerada a utilização da Internet.

6.1.2 – Diagrama de Fluxos / Sinalização

A seguir são detalhados e descritos os fluxos de sinalização para os eventos entre o terminal e a rede Wi-Fi e IMS durante o processo de *handover* vertical entre as redes GSM/GPRS (WWAN) e WLAN. No Apêndice B são registrados os códigos binários dos fluxos de sinalização capturados e utilizados na avaliação do atraso.

6.1.2.1 - Conexão Wi-Fi e DHCP

Banerjee [12] considera somente a contribuição devida ao processo de registro DHCP [29] no cálculo do atraso de conexão em redes Wi-Fi, o que não é verdade quando são utilizados os procedimentos de autenticação definidos pelo padrão IEEE 802.11i [32]. O processo de registro DHCP tem a finalidade de configurar os parâmetros associados à *interface* IP (camada 3) do terminal móvel.

De acordo com as medidas efetuadas durante a elaboração deste trabalho, o atraso real tem também contribuições devidas a: o processo de associação definido para redes IEEE 802.11 [31], que envolve processos relacionados à camada física e MAC (*Medium Access Control*) e que ocorrem antes do processo de registro DHCP, e; o envio de uma sequência de mensagens do protocolo ARP [29], como forma do terminal determinar que o endereço IP designado não esteja em uso pela rede, que ocorre após o ciclo de registro DHCP [29].

O processo de associação à rede IEEE 802.11 tem seu atraso relacionado a diferentes fatores dependentes da condição da rede e da configuração adotada para o acesso WLAN, como por exemplo: o *broadcast* (ou não) da informação de identificação da rede (SSID). O processo adotado para selecionar a rede WLAN também afeta o atraso de associação. Diversos trabalhos têm sido realizados para determinar a melhor estratégia de seleção de redes WLAN em cenários de redes heterogêneas, tais como o padrão IEEE 802.21 MIH (*Media Independent Handover*) [82] descrito no capítulo anterior. Como estes trabalhos não foram concluídos na realização e não têm relação com o escopo do presente estudo, ou seja, não são afetados pelos procedimentos subsequentes de autenticação, o atraso relativo ao processo de associação à rede IEEE 802.11 não será considerado na modelagem realizada. Isso significa que a condição básica necessária neste estudo para o início do processo de *handover* entre a rede WWAN e WLAN é a associação bem sucedida com a rede IEEE 802.11.

Após o procedimento de configuração da *interface* IP via protocolo DHCP foi verificado que há o envio de: até três mensagens ARP [30] consecutivas, com os campos *sender IP* e *target IP* preenchidos com o mesmo valor (mensagem *Gratuitous ARP*), com o objetivo atualizar o *cache* ARP dos demais *hosts* da rede local WLAN e testar se o endereço IP

obtido não está em uso pela rede local, e; o envio de uma mensagem ARP adicional requisitando o endereço MAC do elemento informado como *Default Gateway* da rede local. As três mensagens *Gratuitous ARP* possuem um atraso específico e crescente entre elas e o diálogo de requisição do endereço MAC do *Default Gateway* acrescenta dois atrasos de transmissão ao processo de conexão à rede WLAN.

O comportamento descrito acima foi verificado em medidas realizadas em terminais com sistemas *Microsoft Windows XP* e *Microsoft Windows Mobile*. Em sistemas operacionais voltados para aplicações móveis, tais como *Microsoft Windows Mobile*, a mensagem ARP de requisição do endereço do *Default Gateway* ocorre imediatamente após a primeira mensagem de *Gratuitous ARP*, de forma a reduzir o tempo de conexão à rede WLAN.

O padrão do protocolo DHCP conforme definido na RFC2131 [29] recomenda que seja utilizado algum mecanismo, como por exemplo: utilização de protocolo ARP, para o terminal verificar se o endereço informado via mensagem DHCP ACK não está em uso pela rede. Como não há definição explícita nos padrões sobre como deve ser utilizado o protocolo ARP para verificar duplicidade de endereços na rede local, a implementação realizada pelo sistema operacional *Microsoft Windows Mobile* será considerada como base inicial neste estudo, por ser a que consome mais tempo e causa o maior impacto no tempo de *handover*. Em outros terminais com sistemas operacionais proprietários, o comportamento acima (envio de três mensagens ARP com a temporização crescente entre elas) não foi verificado.

A figura 6.3 descreve a sequência de mensagens descritas acima.

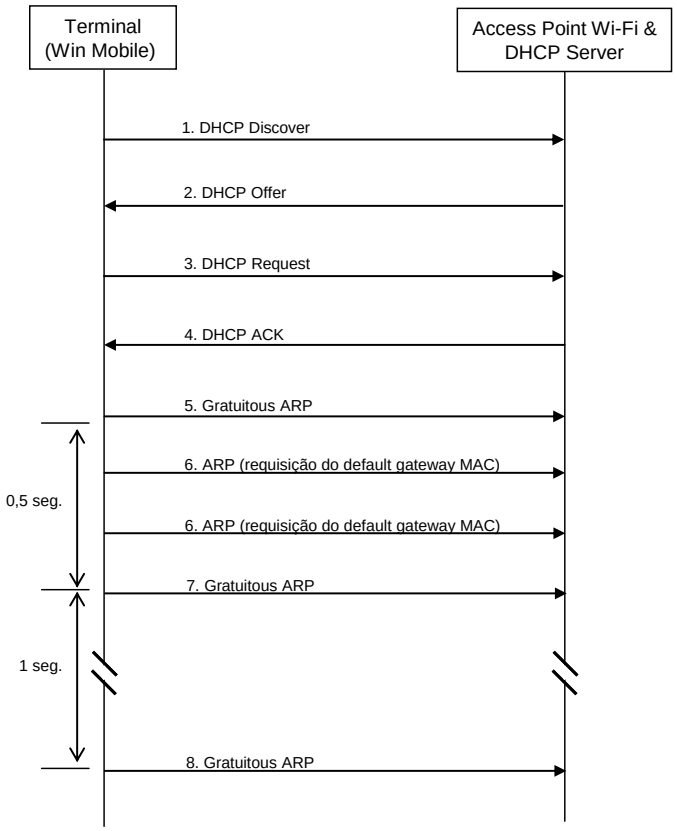


Figura 6.3 – Processo de Requisição DHCP

6.1.2.2 - Autenticação EAP-SIM

A figura 6.4 representa a troca de sinalização entre o terminal e as redes WLAN e IMS durante o processo de autenticação mútua baseada em EAP-SIM [10]. O pré-requisito para esta etapa é a associação bem sucedida entre o terminal e a rede WLAN. A autenticação através do protocolo EAP ocorre antes da configuração da *interface* IP, via protocolo DHCP, conforme definido pelo padrão IEEE 802.11i [32] e descrito no capítulo anterior.

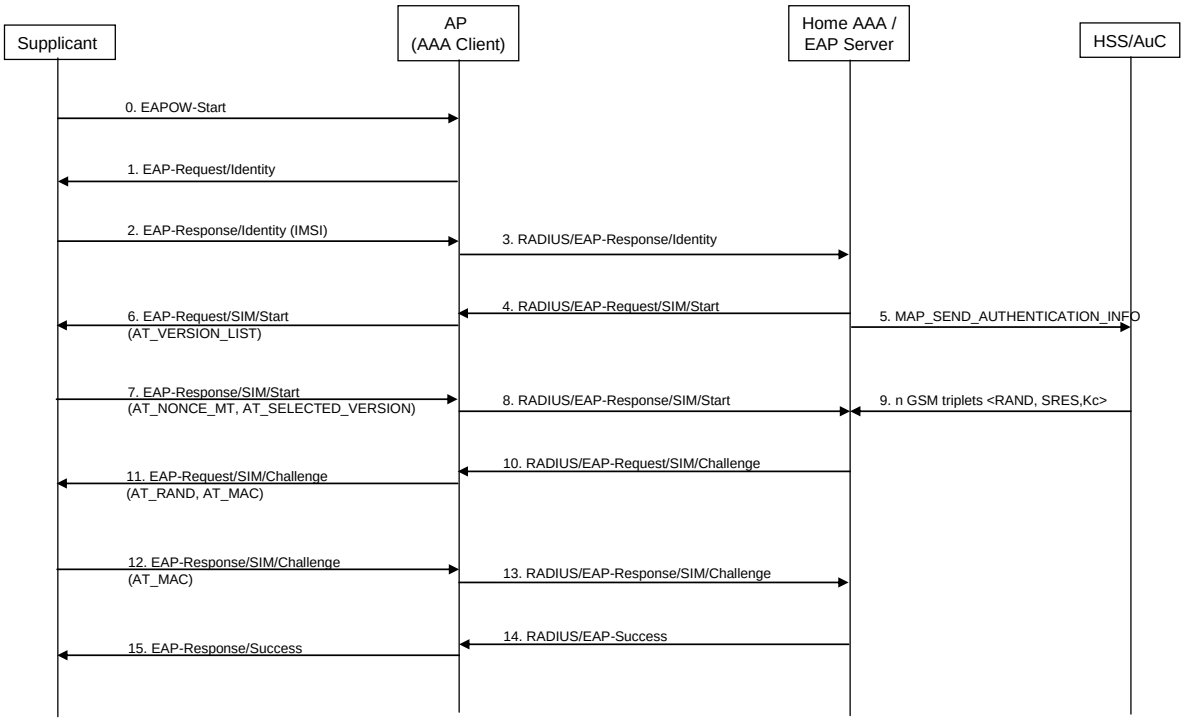


Figura 6.4 – Autenticação EAP-SIM (Zivkovic [13], modificado)

Descrição dos eventos:

0. O terminal móvel com cliente EAP *supplicant* (IEEE) inicia a sessão de autenticação com o envio da mensagem *EAPOW-Start*, conforme definido pelo IEEE 802.1x;

1. O AP retorna uma mensagem *EAP-Request/Identity* [9] requisitando a identidade do terminal;

2. O *supplicant* fornece sua identidade, contendo um pseudônimo ou o IMSI (em caso de primeira autenticação). A identidade segue o padrão NAI definido na RFC 4282 e o formato descrito pela especificação 3GPP TS 23.003 [1];

3. O AP encapsula a mensagem EAP em uma mensagem RADIUS *Access-Request* [11] e envia para o servidor AAA da rede caseira do usuário;

4. O servidor AAA/EAP utiliza a informação de NAI recebida para localizar o perfil do usuário e determinar se há necessidade de autenticação via EAP-SIM. O servidor EAP envia para o AP mensagem *EAP-Request/SIM/Start* encapsulada em mensagem RADIUS *Access-Challenge*. Esta mensagem marca o início da sessão EAP-SIM. A mensagem EAP é enviada com o atributo AT_VERSION_LIST o qual inclui lista de versões EAP-SIM suportadas;

5. O servidor AAA/EAP envia mensagem MAP SEND_MAP_AUTH_INFO para o HLR/AuC, de forma a requisitar *n* (onde *n* varia de 1 a 5) *triplets* GSM para o IMSI

informado. Dependendo da implementação adotada a troca de mensagens entre o servidor EAP e o HLR/AuC pode ser feito via protocolo DIAMETER [41];

6. O AP desencapsula a mensagem EAP e encaminha para o terminal;

7. O cliente EAP *supplicant* envia mensagem de resposta *EAP-Response/SIM/Start* com a versão selecionada no atributo AT_SELECTED_VERSION e o desafio NONCE, N1, para o autenticador no atributo AT_NONCE_MT;

8. A resposta é encapsulada e encaminhada para o servidor AAA, via mensagem RADIUS *Access-Request*;

9. O HLR/AuC encaminha os *triplets* (RAND, SRES, *Kc*) requisitados na mensagem 5 para o servidor AAA, via uma única mensagem MAP SAI (*Send Authentication Info*) [51];

10. O servidor AAA envia, encapsulado na mensagem RADIUS *Access-Challenge*, a mensagem *EAP-Request/SIM/Challenge* contendo os *n* GSM RAND no atributo AT_RAND e o *byte string Message Authentication Code* (MAC) calculado no atributo AT_MAC. O valor de MAC tem a finalidade de permitir o terminal autenticar a rede e é calculado como: pacote EAP | NONCE_MT [10], onde "|" significa concatenação;

11. A mensagem 10 é desencapsulada e encaminhada para o terminal;

12. O terminal verifica o AT_MAC antes de continuar. O terminal roda o algoritmo GSM A3, conforme descrito em 5.1.2, sobre *n*RAND* para obter *n*SRES* e calcula novo valor de MAC como sendo: pacote EAP | *n*SRES*. O terminal então envia mensagem *EAP-Response/SIM/Challenge* somente com o valor de MAC no atributo AT_MAC;

13. O AP encapsula a mensagem EAP em uma mensagem RADIUS *Access-Request* e envia para o servidor AAA;

14. O servidor EAP verifica o valor de MAC, usando o SRES armazenado, e envia mensagem *EAP-Response/Success* encapsulada em mensagem RADIUS *Access-Accept*, em caso de sucesso. Ele também inclui o segredo mestre da sessão nos atributos MS-MPPE-RECV e MS-MPPE-SEND (extensões proprietárias *Microsoft* – utilizadas para envio de chave de sessão, mencionado na RFC 4186 [10] página 45);

15. O AP remove os atributos com o segredo mestre da sessão para disparar processo de derivação das chaves 802.11i e encaminha a mensagem EAP-*Response*/*Success* para o terminal.

6.1.2.3 Registro IMS

Na arquitetura considerada, o terminal é atendido por um serviço baseado na rede 3GPP IMS [21]. Para ter acesso a esta rede, a primeira operação que deve ser realizada é o de registro SIP na infra-estrutura IMS, conforme descrito abaixo.

A figura 6.5 representa a troca de sinalização no processo de registro do terminal (UE) na rede IMS, conforme definido pelas especificações do 3GPP em [3].

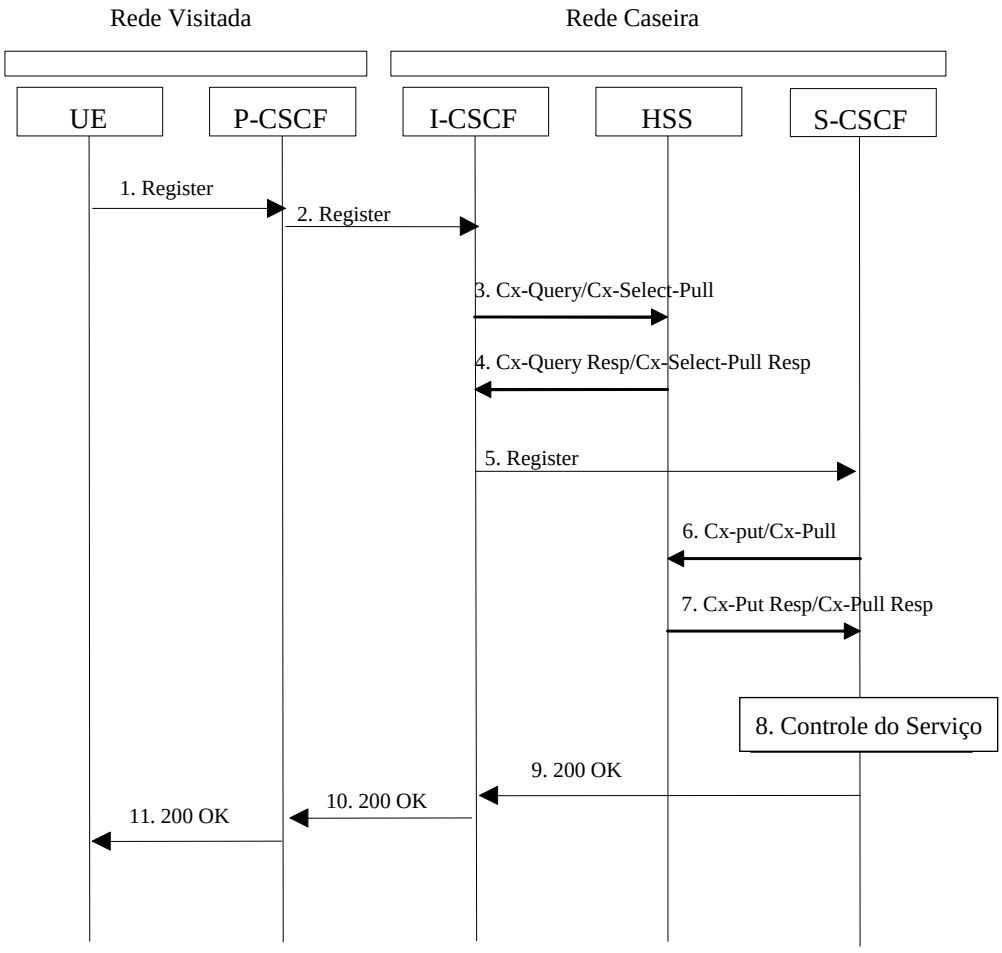


Figura 6.5 – Registro IMS (3GPP [3], modificado)

O registro IMS ilustrado na figura 6.5 considera que o acesso utilizado pelo terminal é um dos definidos pelo 3GPP, como por exemplo: redes UTRAN (*Universal Terrestrial Radio Access Network*) [21], e não considera os requisitos de segurança que devem ser tomados em conta no processo de autenticação na rede de acesso sendo utilizada.

O processo de registro completo de um terminal em uma rede IMS, incluindo a autenticação é ilustrado na figura 6.6. Neste processo há a troca de chaves entre a rede IMS e o terminal para permitir a criação de uma associação segura entre eles, necessário antes de se realizar o acesso a qualquer serviço IMS. O mecanismo de autenticação mútua definido foi derivado do utilizado em redes UMTS e é chamado de IMS AKA, onde o método de cálculo dos parâmetros é o mesmo, mas a forma de transporte é ligeiramente diferente, principalmente no envio da resposta do terminal, que não é em formato aberto como nas redes UMTS [18].

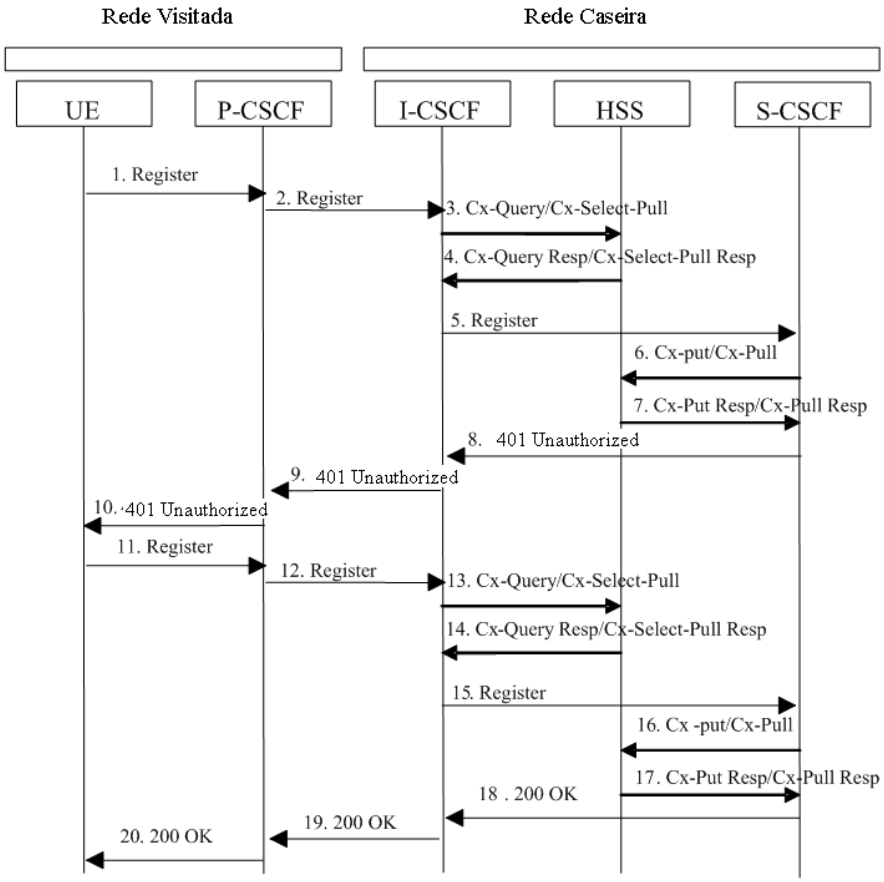


Figura 6.6 – Autenticação e Registro IMS (3GPP [18], modificado)

6.1.3 – Análise do Atraso de Autenticação no *Handover*

Para a análise do atraso de *handover* são considerados os cenários descritos no início deste capítulo. Na modelagem destes atrasos serão definidos os atrasos devidos à: rede de acesso

WLAN e o tempo de enfileiramento e processamento nos elementos responsáveis pela autenticação.

6.1.3.1 Atraso de Transmissão em WLAN

As redes GPRS possuem elevada vulnerabilidade a ruído e elevada taxa de erro de *bit* (BER) devido ao seu uso externo (*outdoor*) [12]. Para melhorar o desempenho destas redes com relação à BER são utilizados mecanismos de retransmissões baseados na camada de enlace, tais como, *Radio Link Protocol* (RLP) que é utilizado sobre a camada MAC. Como as redes WLAN possuem uma largura de banda maior que as redes atuais WWAN e utilização geralmente interna (*indoor*), estes mecanismos de retransmissão não são considerados, à semelhança da abordagem em [12].

Nos enlaces WLAN mecanismos de retransmissão podem também ser implementados pelos protocolos superiores aos da camada de enlace, tais como: TCP, DHCP, EAP, etc. Para o estudo realizado neste documento, as seguintes premissas são feitas para as sessões fim a fim, relativas aos protocolos de camada de transporte [17] com controle de retransmissão: funcionamento em modo interativo; e sem execução de *fast retransmit*, ou seja, um pacote perdido sempre esgota o temporizador de *round-trip* (RTO).

As deduções a seguir são baseadas nos diversos modelos de atraso de transmissão de pacote proposto por Das em [17]. Segundo o algoritmo de Karn, para os protocolos com controle de retransmissão, o valor de RTO é multiplicado por um fator constante *c* após cada retransmissão devido ao esgotamento do temporizador. Então, $RTO_{i+1} = c * RTO_i$, onde RTO_i é o *i*-ésimo valor do temporizador de retransmissão. Este efeito provoca o crescimento exponencial do RTO após cada retransmissão. Felizmente, os protocolos da camada de transporte não permitem um número infinito de retransmissão, em sua grande maioria. Então, considerando que *n* retransmissões são necessárias para transmitir um pacote com sucesso, o atraso médio para transmitir um pacote é dado por:

$$T = T' + RTO_1 + RTO_2 + \cdots + RTO_n$$
$$T = T' + cRTO_o + c^2 RTO_o + \cdots + c^n RTO_o$$
$$T = T' + cRTO_o \sum_{i=0}^{n-1} c^i \qquad \text{Eq. 6.1}$$
$$T = T' + cRTO_o \frac{(1-c^n)}{(1-c)}$$

onde T' é o atraso de propagação fim a fim do pacote e RTO_o é o valor inicial do temporizador de retransmissão.

A taxa de perda de pacotes é dada por $q = 1-(1-p)^k$, onde p é a probabilidade de um quadro (*frame*) estar com erro no enlace aéreo (FER) e k é o número de quadros do enlace aéreo contidos no pacote. A probabilidade de transmitir um pacote com sucesso pode ser calculada como $(1-q)+(1-q)q+\cdots+(1-q)q^{N_m-1} = 1-q^{N_m}$. Utilizando a equação anterior e a equação 6.1 podemos obter o atraso médio para transmitir um pacote com controle de retransmissão sobre *interface* WLAN com não mais que N_m tentativas de retransmissão como:

$$D' = (1-q)\left[D + (k-1)\tau\right] + (1-q)q\left[D + cRTO_0 \frac{1}{(1-c)} + (k-1)\tau\right] + \cdots$$
$$+ (1-q)q^{N_m-1}\left[D + cRTO_o \frac{(1-c^{N_m-1})}{(1-c)} + (k-1)\tau\right]$$
$$D' = [D + (k-1)\tau](1-q^{N_m}) + cRTOo\frac{(1-q)}{(1-c)}\left[\frac{(1-q^{N_m})}{(1-q)} - \frac{(1-q^{N_m}c^{N_m})}{(1-qc)}\right] \qquad \text{Eq. 6.2}$$

onde D é o atraso de propagação fim a fim do quadro sobre enlace WLAN e τ é o tempo inter-quadro. A figura 6.7 ilustra o atraso médio calculado pela equação 6.2.

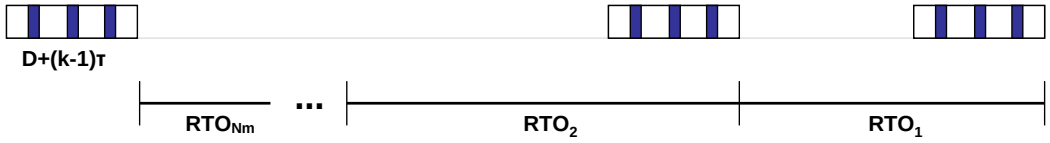


Figura 6.7 – Atraso médio para transmitir um pacote com controle de retransmissão sobre quadros da rede WLAN

O padrão IEEE 802.11 especifica o tamanho máximo do *payload* é de 8184 *bits*, ou 1023 *bytes*. Como para mensagens DHCP podemos ter um comprimento máximo de 548 *bytes*, isso significa que temos k = 1 tanto para 802.11b quanto para 802.11g. Para mensagens EAP temos um comprimento máximo de 280 *bytes*, como estas mensagens são transportadas diretamente sobre a camada de enlace na *interface* aérea WLAN e devido ao fato do protocolo EAP não suportar fragmentação, temos também k = 1. Considerando os dados acima e também que o valor típico de c é igual a 2, temos que a equação 6.2 pode ser simplificada para:

$$D' = D(1-q^{N_m}) + 2RTO_o(1-q)\left[\frac{(1-q^{N_m})}{(1-q)} - \frac{(1-2^{N_m}q^{N_m})}{(1-2q)}\right] \qquad \text{Eq. 6.3}$$

O atraso médio de transmissão fim a fim do canal WLAN (D) estimado é igual 1,4 ms para canal de 11Mbps (IEEE 802.11b) e de 0,4 ms para canal de 54Mbps (IEEE 802.11g), para *payload* de 1500 *bytes* e 10 terminais compartilhando o canal, segundo cálculos realizados utilizando a metodologia proposta por Bianchi em [27], e descritos no Apêndice A.

O valor inicial de *RTO* é estimado como sendo o valor de atraso de *round-trip*, conforme definido em [24]. O valor do número máximo de retransmissões (N_m) é estimado como dez, conforme indicado por Das em [17].

No processo de conexão à rede WLAN e de autenticação temos quatro troca de mensagens DHCP, cinco mensagens ARP (sendo três *Gratuitous ARP*, com intervalos de 0,5s e 1s entre elas, e um diálogo de requisição de endereço MAC – não considerado por ser realizado entre o tempo de espera de esgotamento de temporização das mensagens *Gratuitous ARP*) e 8 troca de mensagens EAP. Os tempos de atraso devido a estas trocas de mensagens podem ser calculados, respectivamente, como: $D_{DHCP} = 4D'_{DHCP}$; $D_{ARP} = (3D'_{ARP} + ARP_{wait})$ e $D_{EAP} = 8D'_{EAP}$. Os valores D'_{DHCP}, D'_{ARP} e D'_{EAP} são calculados a partir da equação 6.3 com os valores de RTO_o e N_m específicos para cada um dos protocolos. O valor de ARP_{wait} total é de 1,5s (temporização de 0,5s mais 1s) para o cenário de utilização de terminais baseados em sistema operacional *Microsoft Windows Mobile*. O valor acima foi obtido segundo informação fornecida pela *Microsoft* em *http://support.microsoft.com/kb/199773/en-us*.

6.1.3.2 Atraso de Autenticação

No processo de *handover* do terminal as mensagens de autenticação são processadas por diversos elementos de rede e transportadas por diferentes protocolos, tais como EAP, RADIUS e MAP. O protocolo EAP é transportado diretamente sobre a rede 802.11, o protocolo RADIUS é transportado sobre IP em redes 802.3 e o protocolo MAP é transportado sobre rede de sinalização número 7 (SS7), através de enlaces TDM de 64 Kbps e de 2 Mbps (enlace E1).

O atraso introduzido pelos elementos de rede pode ser calculado pela utilização da teoria clássica de filas para o sentido terminal-rede e rede-terminal, conforme ilustrado pelas figuras 6.8 e 6.9.

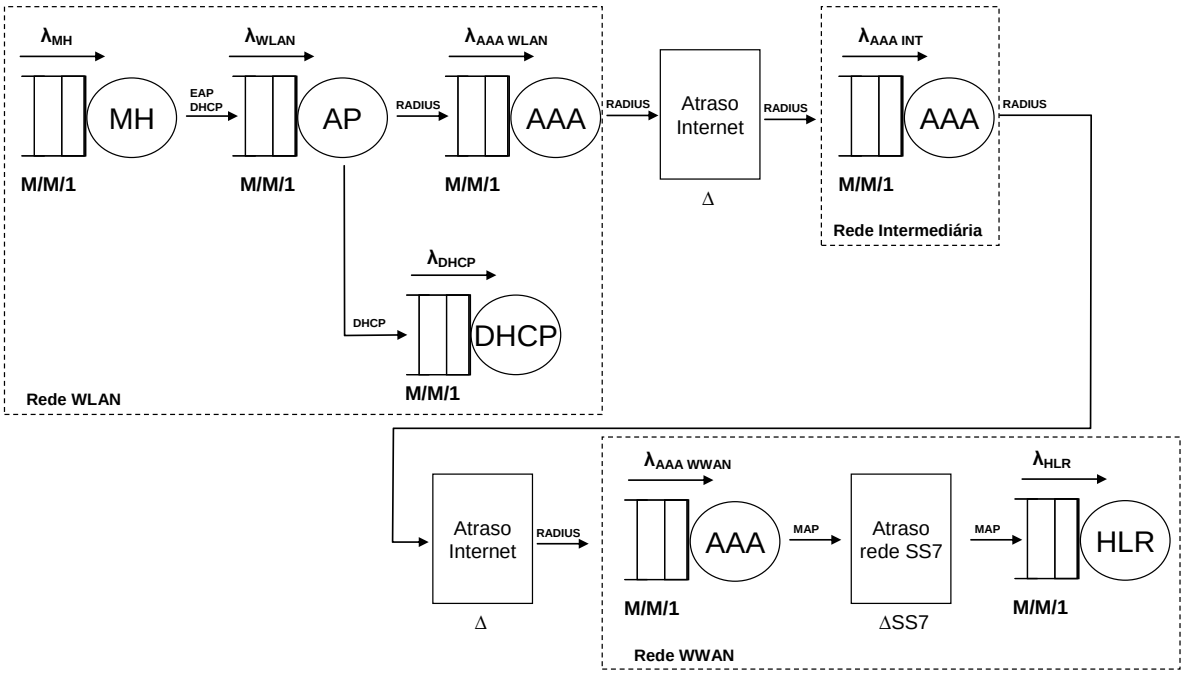


Figura 6.8 – Modelo de filas para análise do atraso no sentido terminal-rede

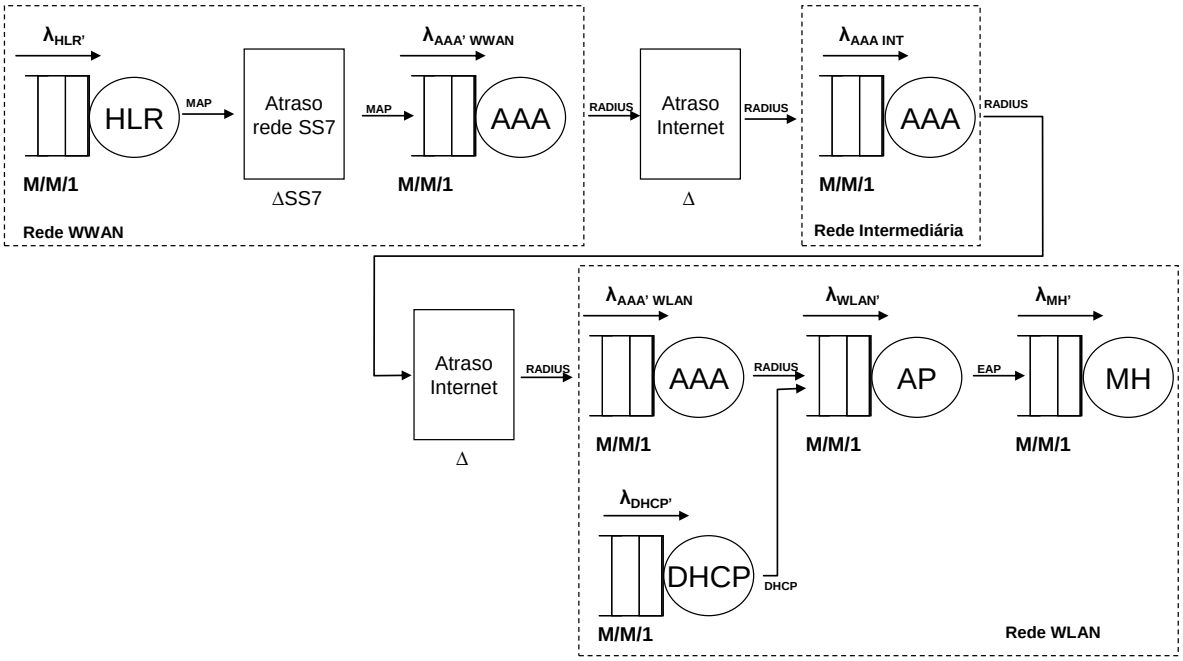


Figura 6.9 – Modelo de filas para análise do atraso no sentido rede-terminal

Temos para ambos os casos, duas redes de filas abertas sem realimentação. Seguindo o proposto pelo Teorema de Burke, o atraso total de cada rede de fila em um sistema aberto pode ser calculado como a soma dos atrasos individuais de cada nó. Adicionalmente a esta consideração, as taxas de entrada em cada servidor não são devidas exclusivamente ao fluxo de mensagens de autenticação dos terminais realizando *handover* entre redes WWAN e WLAN, há outros fluxos de dados utilizando os mesmos servidores simultaneamente.

O tempo de atraso total para o processo de conexão na rede WLAN pode ser descrito como:

$$D_{CON} = D_{MH} + D_{DHCP} + D_{ARP} + D_{AP} + D_{DHCP\_Server} \qquad \text{Eq. 6.4}$$

Considerando que o processo de autenticação envolve troca de sinalização bidirecional com os elementos da rede, tempo de atraso total para o processo de autenticação pode ser descrito como:

$$D_{AUT} = D_{MH} + D_{EAP} + D_{AP} + D_{AAA\_WLAN} + 4\Delta + D_{AAA\_INT} + D_{AAA\_WWAN} + D_{HLR} \qquad \text{Eq. 6.5}$$

O atraso de processamento devido ao terminal pode ser calculado como:

$$D_{MH} = \frac{1}{\mu - \lambda_{MH}} + \frac{1}{\mu' - \lambda_{MH'}} \qquad \text{Eq. 6.6}$$

Os atrasos de transmissão devido à *interface* WLAN são dados pelos componentes D_{DHCP}, D_{ARP} e D_{EAP} e são calculados conforme a equação 6.3 e segundo a descrição ao fim do seção 6.1.3.1.

O atraso de processamento devido aos elementos da rede de acesso WLAN pode ser calculado como:

$$D_{AP} = \frac{1}{\mu_{AP} - \lambda_{WLAN}} + \frac{1}{\mu_{AP'} - \lambda_{WLAN'}} \qquad \text{Eq. 6.7}$$

O atraso de processamento devido ao servidor de DHCP pode ser calculado como:

$$D_{DHCP\_Server} = \frac{\rho_{DHCP}}{(1 - \rho_{DHCP})}\left(\frac{2}{\lambda_{DHCP}}\right) \qquad \text{Eq. 6.8}$$

O atraso de processamento devido ao servidor AAA da rede WLAN para um par de mensagens de requisição e resposta pode ser calculado como:

$$D_{AAA\_WLAN} = \frac{1}{\mu_{AAA\_WLAN} - \lambda_{AAA\_WLAN}} + \frac{1}{\mu_{AAA'\_WLAN} - \lambda_{AAA'\_WLAN}} \qquad \text{Eq. 6.9}$$

O atraso de processamento devido ao servidor AAA da rede intermediária para um par de mensagens de requisição e resposta pode ser calculado como:

$$D_{AAA\_INT} = \frac{2}{\mu_{AAA} - \lambda_{AAA\_INT}} \qquad \text{Eq. 6.10}$$

O atraso de processamento devido ao servidor AAA da rede WWAN (HPLMN) para um par de mensagens de requisição e resposta pode ser calculado como:

$$D_{AAA\_WWAN} = \frac{1}{\mu_{SS7} - \lambda_{AAA'\_WWAN}} + \frac{1}{\mu_{AAA} - \lambda_{AAA\_WWAN}} \qquad \text{Eq. 6.11}$$

O atraso de processamento devido à rede SS7 e ao HLR/AuC da rede WWAN (HPLMN) pode ser calculado como:

$$D_{HLR} = 2\Delta_{SS7} + \frac{\rho_{HLR}}{(1-\rho_{HLR})}\left(\frac{1}{\lambda_{HLR}} + \frac{1}{\lambda_{HLR'}}\right) \qquad \text{Eq. 6.12}$$

O volume de tráfego inicial de autenticação via rede WLAN é muito menor que o existente na rede WWAN, pois a quantidade de usuários utilizando a rede WWAN é muito maior que a de usuários utilizando a rede WLAN. Devido a este fato, o atraso responsável pelo elemento HLR/AuC não é alterado pelo volume de tráfego de mensagens de autenticação incremental gerado pelos usuários na rede WLAN. Na implementação realizada, o valor do atraso relativo ao processamento do HLR foi medido em rede WWAN comercial, dimensionada para aproximadamente 3 milhões de assinantes. Nestas condições o atraso de processamento devido à rede SS7 e ao HLR/AuC da rede WWAN (HPLMN) para um par de mensagens de requisição e resposta pode ser alternativamente representado como:

$$D_{HLR} = 2\Delta_{SS7} + \Delta_{HLR} \qquad \text{Eq. 6.13}$$

Os parâmetros utilizados nas equações anteriores e seus significados estão listados na tabela 6.1.

Tabela 6.1 – Parâmetros usados no atraso de processamento

Parâmetro	Significado
μ	Taxa de processamento de mensagens do terminal para rede WLAN
μ'	Taxa de processamento de mensagens do terminal para aplicação
μ_{AP}	Taxa de processamento de mensagens da rede WLAN para Internet
$\mu_{AP'}$	Taxa de processamento de mensagens da rede WLAN para os terminais
μ_{AAA}	Taxa de processamento de mensagens dos servidores AAAs
μ_{SS7}	Taxa de processamento de mensagens do servidor AAA para mensagens SS7
λ_{MH}	Taxa de chegada de mensagens da aplicação para terminal
$\lambda_{MH'}$	Taxa de chegada de mensagens no terminal da rede WLAN
λ_{WLAN}	Taxa de chegada de mensagens na rede WLAN pelos terminais
$\lambda_{WLAN'}$	Taxa de chegada de mensagens na rede WLAN pela Internet
λ_{DHCP}	Taxa de chegada de mensagens no servidor DHCP
λ_{AAA_WLAN}	Taxa de chegada de mensagens no servidor AAA pela rede WLAN
$\lambda_{AAA'\_WLAN}$	Taxa de chegada de mensagens no AAA (WLAN) pela rede intermediária
λ_{AAA_INT}	Taxa de chegada de mensagens no servidor AAA da rede intermediária
λ_{AAA_WWAN}	Taxa de chegada de mensagens no AAA (WWAN) pela rede intermediária
$\lambda_{AAA'\_WWAN}$	Taxa de chegada de mensagens no servidor AAA pela rede SS7
λ_{HLR}	Taxa de chegada de mensagens no HSS/AuC pela rede SS7
$\lambda_{HLR'}$	Taxa de chegada de mensagens no HSS em direção à rede SS7
ρ_{DHCP}	Fator de utilização do servidor de DHCP
ρ_{HLR}	Fator de utilização do HLR
Δ_{SS7}	Atraso médio de mensagens na rede SS7
Δ_{HLR}	Atraso médio de processamento para consulta ao HLR/AuC
Δ	Atraso médio de mensagens pela Internet

O atraso total do processo de *handover* entre rede WWAN e WLAN é dado pela soma do atraso de conexão com o atraso de autenticação, ou seja:

$$D_{Handover} = D_{CON} + D_{AUT} \qquad \text{Eq. 6.14}$$

Com base nas equações demonstradas neste seção podemos calcular os atrasos de conexão e de autenticação de um terminal qualquer à rede WLAN, para diversas condições da rede de acesso. As modelagens analíticas efetuadas e seus resultados estão descritos no seção seguinte deste documento.

6.2 – IMPLEMENTAÇÃO

A implementação feita neste trabalho consistiu em uma abordagem mista, em que medidas práticas em redes reais foram realizadas com a finalidade de gerar dados de entrada para a modelagem analítica e para validar o resultado final alcançado. Em paralelo foi definida uma arquitetura prática para ser montada em laboratório de forma a verificar os procedimentos e protocolos definidos.

6.2.1 – Arquitetura Implementada

O diagrama de blocos da arquitetura geral da solução a ser implementada em redes comerciais está representado na figura 6.1.

Quanto ao servidor AAA que implementa o processo EAP-SIM, duas soluções técnicas de diferentes fornecedores foram avaliadas, com diferentes configurações na forma de implementar a conversação com o elemento HLR/AuC. Na solução de AAA provida pelo fabricante *Alcatel-Lucent*, chamada de *Navis Radius*, a *interface* SS7 (enlace E1) para o HLR/AuC é integrada diretamente no servidor, através de placa específica, conforme mostrado na figura 6.10.

A solução de AAA provida pelo fabricante *Cisco* possui somente *interface* baseada em IP para a consulta ao HLR/AuC, esta *interface* utiliza protocolo SIGTRAN, definido pelo IETF (RFC 4666), para simular os serviços promovidos pelos protocolos MTP (camada 2 e 3) da rede SS7 e transportar o protocolo de aplicação MAP. Um elemento adicional se faz necessário para converter o protocolo SIGTRAN/IP para o utilizado na *interface* SS7, a este elemento é dado o nome comercial de ITP (*Internet Transfer Point*) pelo fabricante *Cisco*, e consiste de um roteador IP com recursos para realizar *interface* com redes de sinalização SS7. Esta topologia é mostrada na figura 6.11. Durante a evolução deste trabalho o servidor AAA referenciado na figura 6.11 foi descontinuado pelo fabricante, desta forma somente a solução mostrada na figura 6.10 foi utilizada para avaliação.

Figura 6.10 – Solução AAA Alcatel-Lucent e conexão ao HLR/AuC

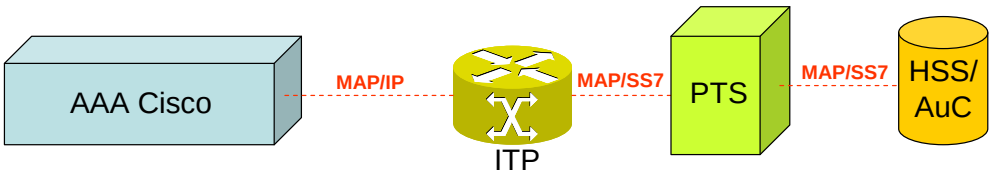


Figura 6.11 – Solução AAA Cisco e conexão ao HLR/AuC

As *interfaces* IP mostradas nas figuras 6.10 e 6.11 são baseadas em padrão 100BASE-T *Fast-Ethernet* e as *interfaces* SS7 mostradas nas mesmas figuras são baseadas em *time slots* TDM de 64 Kbps em enlace de 2 Mbps canalizado (E1). O elemento PTS (Ponto de Transferência de Sinalização) é um comutador de pacotes de sinalização responsável pela implementação da rede de sinalização SS7 e tem como função básica o roteamento de mensagens de sinalização entre os diferentes pontos dentro da rede SS7, baseado nas informações dos protocolos MTP de camada 2 e 3, conforme descrito em [33].

A topologia indicada na figura 6.10 foi reproduzida em laboratório com o objetivo de verificar a funcionalidade da arquitetura proposta e para extrair as informações relativas às mensagens de sinalização trocadas entre os elementos, tais como: tamanho, sequência e preenchimento dos campos. O cenário montado em laboratório e os resultados obtidos estão descritos no Apêndice C. Não foram realizada verificação em laboratório considerando a existência de servidores de AAA separados e distintos (para rede WLAN, intermediário e WWAN), conforme mostrado na figura 6.1 e 6.2, devido à indisponibilidade de recursos físicos.

6.3 – METODOLOGIA ADOTADA E RESULTADOS OBTIDOS

A arquitetura mostrada na figura 6.2 foi integralmente modelada matematicamente e calculada com a utilização de dados obtidos de elementos e redes reais, conforme é demonstrado nos resultados apresentados na sequência.

Para a realização das medidas em redes reais foram levantados os horários de maior movimento nestas redes, com base nos dados estatísticos disponibilizados pelo operador da rede. Para os dados de atraso do protocolo RADIUS foram feitas medidas do tráfego IP na *interface* de rede do servidor de AAA de produção da rede da operadora de telefonia Brasil Telecom. Este servidor é responsável pela autenticação de todos os usuários de banda larga da operadora e implementa as funções de: *proxy* para outros servidores AAA para usuários com conta em domínios não geridos pela operadora; autenticação para usuários com conta em domínios geridos pela operadora, e; contabilização das conexões e desconexões. A autenticação de usuários próprios é efetuada após a consulta a uma base de assinantes LDAP (*Lightweight Directory Access Protocol*) externa ao servidor. A metodologia de medição efetuada e os dados obtidos estão descritos no Apêndice D.

Para medidas de atraso na rede SS7 e de autenticação no elemento HLR/AuC foram feitas medidas nos enlaces de sinalização através da utilização de ferramenta de monitoração de tráfego disponível na rede móvel da operadora Brasil Telecom. Foram realizadas medidas distintas na rede de sinalização (elemento PTS) e em um elemento HLR, ambos os elementos são responsáveis pela rede móvel da operadora em toda a área de cobertura da mesma. As medidas foram tomadas no horário de maior movimento, conforme levantamento histórico disponível na operadora. A metodologia de medição efetuada e os dados obtidos estão descritos no Apêndice E.

6.3.1 – Modelagens Analíticas

Utilizando as equações 6.3 a 6.13 desenvolvidas no seção 6.1.3 podemos simular os atrasos de conexão e de autenticação de um terminal à rede WLAN para diversas condições da rede de acesso. A tabela 6.2 mostra os valores dos parâmetros utilizados nas modelagens analíticas realizadas, considerando as condições de acesso a taxas de 11 Mbps (IEEE 802.11b) e 54 Mbps (IEEE 802.11g).

Tabela 6.2 – Valores numéricos utilizados para modelagem analítica

Parâmetros	**802.11b (11Mbps)**	**802.11g (54Mbps)**
μ; $\mu_{AP'}$ *(nota 1)*	5,69 Mbps	14,42 Mbps
μ' *(nota 2)*	100 Mbps	100 Mbps
μ_{AP} *(nota 3)*	94,34 Mbps	94,34 Mbps
μ_{AAA}; μ_{AAA_WLAN}; μ_{AAA_WWAN} *(nota 8)*	160,14 pacotes/s	160,14 pacotes/s
$\mu_{AAA'\_WLAN}$ *(nota 8)*	79,761 pacotes/s	79,761 pacotes/s
λ_{MH} *(nota 5)*	15,22 Kbps	15,22 Kbps
$\lambda_{MH'}$ *(nota 1)*	5,69 Mbps	14,42 Mbps
λ_{DHCP} *(nota 6)*	1,20 Mbps	1,20 Mbps
λ_{WLAN}; $\lambda_{WLAN'}$ *(nota 7)*	100 Kbps	100 Kbps
λ_{AAA_INT}; λ_{AAA_WLAN} *(nota 8)*	124,27 pacotes/s	124,27 pacotes/s
$\lambda_{AAA'\_WLAN}$ *(nota 8)*	43,89 pacotes/s	43,89 pacotes/s
λ_{AAA_WWAN} *(nota 8)*	124,27 pacotes/s	124,27 pacotes/s
$\lambda_{AAA'\_WWAN}$ *(nota 11)*	3,93 Kbps	3,93 Kbps
ρ_{DHCP} *(nota 12)*	0,9	0,9
Δ_{SS7} *(nota 13)*	37,07 ms	37,07 ms
Δ_{HLR} *(nota 14)*	66,20 ms	66,20 ms
Δ *(nota 15)*	50 ms	50 ms

Notas: (1) Calculado de acordo com metodologia desenvolvida por Bianchi [27] e considerando 10 terminais utilizando simultaneamente o mesmo canal 802.11.

(2) Valor estimado para velocidade do barramento interno do terminal móvel.

(3) Valor efetivo (*goodput*) de taxa para *interface* 100BASE-T (*Fast Ethernet*) com MTU=1500 *bytes*, considerando o *overhead* devido ao protocolo TCP/IP e *Ethernet*.

(4) Múltiplo de 64Kbps (enlaces TDM) necessário para tratar o tráfego de autenticação entre servidor AAA da rede WWAN (HPLMN) e o HLR, via rede SS7, conforme Apêndice E.

(5) Calculado pelo tamanho total das mensagens de DHCP e EAP trocados pelo terminal, conforme Apêndice B.

(6) Considerado o tráfego gerado por um *hotspot* com 12 *Access Points* – dado histórico médio de dimensionamento para cobertura de *shopping-centers.*

(7) Tráfego Internet estimado para um *Access Point* com 10 terminais conectados – dado histórico para dimensionamento de acesso WLAN.

(8) Valor obtido através das medidas realizadas em servidor AAA em rede real de produção, conforme Apêndice D.

(11) Resposta do HLR (protocolo MAP) às autenticações RADIUS, sobre enlaces TDM de 64Kbps.

(12) Valor estimado de fator de utilização para servidor DHCP.

(13) Valor medido em rede de sinalização em operação comercial do atraso médio de transmissão das mensagens de autenticação MAP SAI (*Send Authentication Information*), conforme Apêndice E.
(14) Valor medido em elemento em operação comercial do tempo gasto pela consulta ao elemento HLR/AuC, conforme Apêndice E.
(15) Valor estimado de atraso médio na Internet para enlaces terrestres de longa distância, segundo dados históricos da operadora.

Para o cenário de autenticação completa há troca de três pares de mensagens de requisição e resposta RADIUS entre os servidores AAA, conforme mostrado na figura 6.4. Devido a este fato, a equação do atraso de autenticação (Eq. 6.5) deve ser alterada para:

$$D_{AUT} = D_{MH} + D_{EAP} + D_{AP} + nD_{AAA\_WLAN} + 4n\Delta + nD_{AAA\_INT} + D_{AAA\_WWAN} + D_{HLR} \quad \text{Eq. 6.15}$$

Onde *n* é o número de pares de mensagens de requisição e resposta RADIUS, igual a três para o cenário de autenticação completa. Devido o servidor AAA da rede WWAN (HPLMN) receber as mensagens RADIUS da rede visitada e realizar somente uma consulta ao HLR/AuC por tentativa de autenticação, a fórmula do tempo de atraso para ele deve ser também alterada para:

$$D_{AAA\_WWAN} = \frac{1}{\mu_{SS7} - \lambda_{AAA'\_WWAN}} + \frac{n}{\mu_{AAA} - \lambda_{AAA\_WWAN}} \quad \text{Eq. 6.16}$$

Com base nos valores da tabela 6.2 e nos valores deduzidos para o cálculo de atraso de transmissão WLAN (seção 6.1.3.1) pode ser calculado o valor de atraso de conexão e de autenticação para diversos valores de taxas de erro de quadro (FER). A tabela 6.3 ilustra alguns dos valores calculados para diversas taxas de FER e taxas de transmissão.

Tabela 6.3 – Atrasos de conexão e de autenticação, em segundos, versus FER e taxas de transmissão (ARP_{WAIT} = 1,5s)

Taxa WLAN	FER	Atraso Conexão	Atraso Autenticação
11Mbps	0,01	1,50339 s	1,16235 s
	0,02	1,50332 s	1,16227 s
	0,03	1,50324 s	1,16218 s
	0,04	1,50316 s	1,16209 s
	0,05	1,50308 s	1,16199 s
	0,06	1,50299 s	1,16190 s
	0,07	1,50290 s	1,16179 s
	0,08	1,50280 s	1,16168 s
	0,09	1,50270 s	1,16157 s
	0,10	1,50260 s	1,16145 s
54Mbps	0,01	1,50116 s	1,16002 s
	0,02	1,50113 s	1,15998 s
	0,03	1,50111 s	1,15995 s
	0,04	1,50108 s	1,15991 s
	0,05	1,50105 s	1,15988 s
	0,06	1,50102 s	1,15984 s
	0,07	1,50099 s	1,15979 s
	0,08	1,50096 s	1,15975 s
	0,09	1,50092 s	1,15971 s
	0,10	1,50089 s	1,15966 s

Verificamos que o atraso de conexão apresenta valores elevados e com pouca variabilidade, isso é devido ao atraso no envio das três mensagens *Gratuitous ARP* (1,5 segundos) e ocorre somente para o caso de terminais que utilizam o sistema operacional *Microsoft Windows Mobile*. Em outros sistemas operacionais, foi observado que este tempo de atraso entre o envio de mensagens ARP e o início do processo de autenticação é reduzido, sendo que um modelo *GF210* do fabricante *UTStarcom* apresentou um tempo medido de atraso de mensagens ARP de 500ms e o envio de somente duas mensagens *Gratuitous ARP*. Considerando este último resultado, a tabela anterior foi refeita para um atraso entre mensagens ARP de 500ms e um tempo $D_{ARP} = (2D'_{ARP} + ARP_{wait})$, o resultado está mostrado na tabela 6.4.

Tabela 6.4 – Atrasos de conexão e de autenticação, em segundos, versus FER e taxas de transmissão (ARP_{WAIT} = 0,5s)

Taxa WLAN	FER	Atraso Conexão	Atraso Autenticação
11Mbps	0,01	0,50339 s	1,16235 s
	0,02	0,50332 s	1,16227 s
	0,03	0,50324 s	1,16218 s
	0,04	0,50316 s	1,16209 s
	0,05	0,50308 s	1,16199 s
	0,06	0,50299 s	1,16190 s
	0,07	0,50290 s	1,16179 s
	0,08	0,50280 s	1,16168 s
	0,09	0,50270 s	1,16157 s
	0,10	0,50260 s	1,16145 s
54Mbps	0,01	0,50116 s	1,16002 s
	0,02	0,50113 s	1,15998 s
	0,03	0,50111 s	1,15995 s
	0,04	0,50108 s	1,15991 s
	0,05	0,50105 s	1,15988 s
	0,06	0,50102 s	1,15984 s
	0,07	0,50099 s	1,15979 s
	0,08	0,50096 s	1,15975 s
	0,09	0,50092 s	1,15971 s
	0,10	0,50089 s	1,15966 s

Com base nos resultados acima, pode ser verificado que o processo de autenticação proposto pela arquitetura padrão acrescenta um atraso médio de 1,163s para uma taxa WLAN de 11Mbps e de 1,160s para uma taxa WLAN de 54Mbps, considerando os atrasos reais existentes em servidores nas redes comerciais.

Estes resultados mostram que o atraso devido exclusivamente à conexão na rede WLAN pode variar de 0,5 a 1,5 segundos, dependendo do tipo de terminal sendo utilizado. A introdução da autenticação baseada no padrão IEEE 802.11i com o protocolo EAP-SIM pode acrescentar mais 1,2 segundos a este atraso, totalizando um atraso total entre 1,7 e 2,8 segundos antes do terminal poder iniciar o processo de registro na rede IMS (mensagem SIP *Register*) e iniciar o processo de transferência da chamada em curso para a nova rede, ou seja, realizar o *handover*. Segundo ETSI [36], é recomendado que em redes de telecomunicações móveis o serviço de voz não deve sofrer interrupções por mais de 40ms durante o processo de *handover* para não comprometer a qualidade da comunicação percebida pelo usuário do serviço. Nem o procedimento de conexão atual pode garantir o

tempo máximo de interrupção do serviço, quanto mais o procedimento com o incremento da autenticação baseado no uso de EAP-SIM.

Nas figuras 6.12 e 6.13 estão representados graficamente os resultados obtidos na tabela 6.4, para taxas de transmissão de 11 Mbps e 54 Mbps respectivamente.

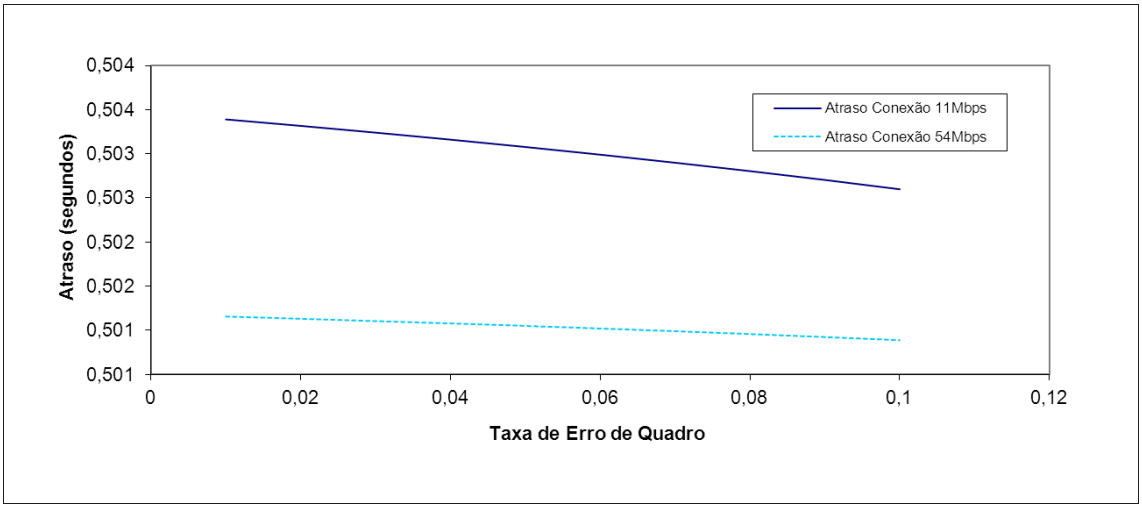


Figura 6.12 – Atraso de conexão na rede WLAN versus Taxa de Erro de Quadro (FER)

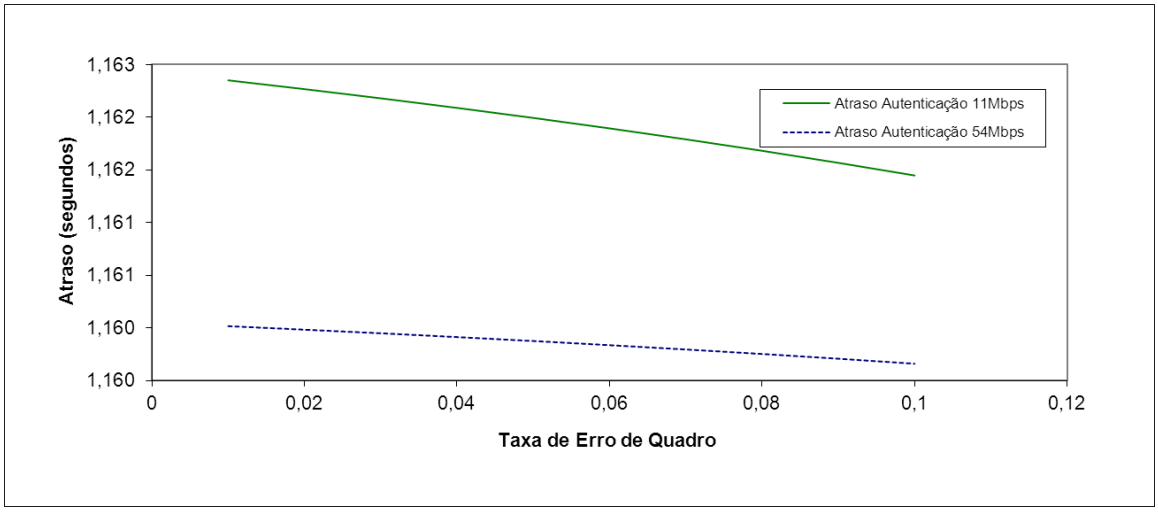


Figura 6.13 – Atraso de autenticação EAP-SIM versus Taxa de Erro de Quadro (FER)

A maior contribuição para este atraso de autenticação verificado é o atraso na Internet, devido ao elevado número de mensagens RADIUS trocada e à utilização da Internet para realizar a conexão ao servidor AAA Intermediário e deste para o servidor AAA da rede WWAN. Cada para par de mensagens de requisição e resposta passa por quatro enlaces da Internet, ou seja, duas vezes por cada trecho. Os trechos sobre a Internet contribuem com

um atraso acumulado, para todo o conjunto de mensagens trocados, de 0,6s para a condição modelada.

A segunda maior contribuição para o atraso de autenticação é o atraso na rede WWAN, representado pelo valor acumulado do processamento do servidor AAA da rede WWAN, do atraso de transmissão das mensagens de autenticação na rede SS7 e do atraso de processamento do HLR/AuC. Este atraso devido aos procedimentos de autenticação na rede WWAN contribui com um valor de atraso total de 0,224s para a condição modelada.

Os demais servidores AAA (intermediário e WLAN) contribuem com um valor de atraso total de 0,167s cada.

Nas figuras 6.14 e 6.15 estão representados graficamente a contribuição percentual de cada estágio utilizado para a conexão e para a autenticação do terminal para taxas de transmissão de 11 Mbps e 54 Mbps. Os dados utilizados foram calculados para a condição de FER de 10%.

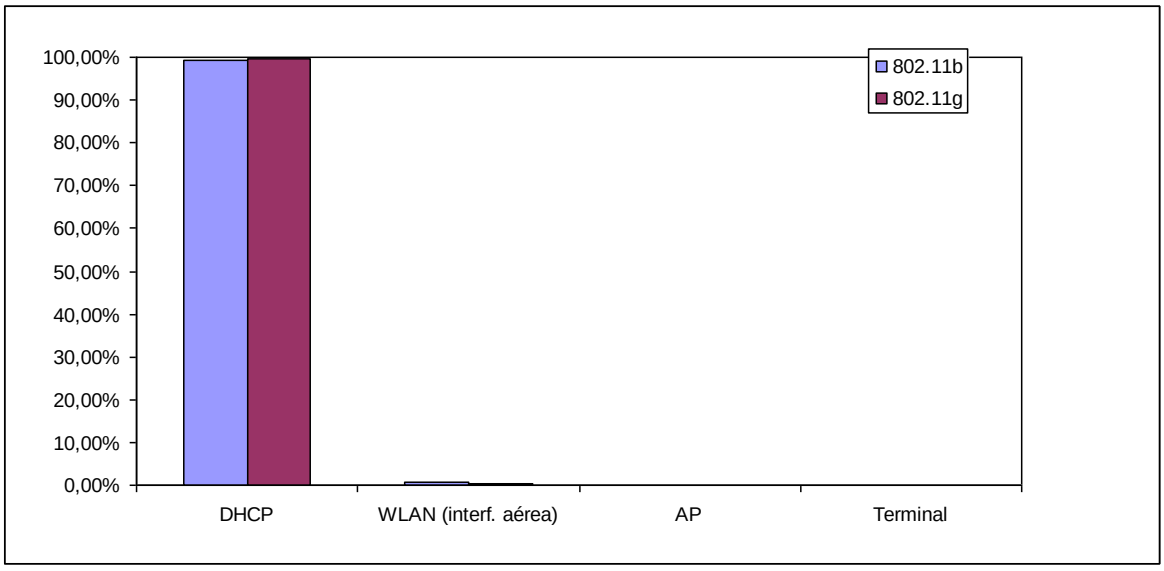


Figura 6.14 – Contribuição porcentual dos elementos funcionais para o atraso de conexão do terminal na rede WLAN

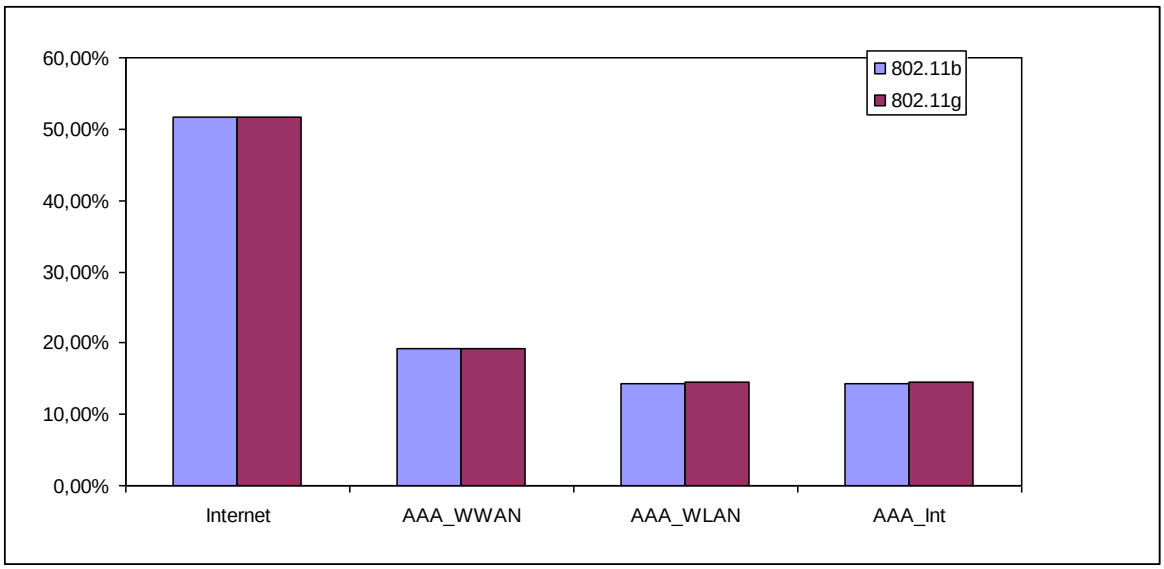


Figura 6.15 – Contribuição porcentual dos elementos funcionais para o atraso de autenticação EAP-SIM do terminal na rede WLAN

Outras análises podem ser realizadas com base nas medições e modelagens realizadas. Por exemplo, a contribuição do número de terminais compartilhando o mesmo canal da rede WLAN no atraso de conexão. Tendo em vista o resultado obtido, em que praticamente a única contribuição significativa para o atraso de conexão é devido ao processo de aquisição de endereçamento via DHCP (e o uso de protocolo ARP neste processo), outros fatores têm pequeno ou nenhum impacto neste atraso. A contribuição do número de terminais para o desempenho com base na taxa real de transmissão em uma rede WLAN baseada em IEEE 802.11 é descrita em detalhes em trabalhos previamente publicados, tais como [25], [27] e [34].

A utilização do procedimento opcional definido para o protocolo EAP-SIM de re-autenticação rápida não foi considerada na modelagem inicial, e não produz uma melhora significativa nos tempos verificados, a ponto de tornar o processo factível para serviços de tempo real, conforme será mostrado. Conforme visto no capítulo 5 deste documento, a re-autenticação rápida prescinde da consulta ao HLR/AuC para recuperação de vetores de autenticação, mas continua a depender das chaves derivadas da autenticação completa realizada anteriormente. Com base no fato acima, o uso de re-autenticação rápida na arquitetura sob teste tem o ganho de evitar os tempos da rede SS7 e de processamento do HLR/AuC, mas não evita o atraso de processamento nos servidores AAA da rede WLAN, Intermediária e WWAN, nem o atraso na rede Internet. Tanto para o caso de autenticação

completa quanto para o de autenticação rápida o servidor EAP é o servidor AAA da rede WWAN caseira. Um ganho adicional que pode ser obtido com a autenticação rápida é devido ao fato de que ela necessita somente de dois pares de mensagens RADIUS de requisição e resposta no diálogo entre o AP (*authenticator*) e o servidor AAA (servidor EAP). Isso é consequência do terminal trocar um par de mensagens EAP a menos com o servidor EAP [10] durante o processo de autenticação rápida, pois ele não necessita do processo de negociação de versão neste caso, conforme descrito no capítulo 5.

A modelagem do atraso de autenticação com o processo de re-autenticação rápida pode ser realizado com a utilização da equação 6.15, considerando as seguintes alterações: D_{EAP} deve ser corrigido para o cenário com somente a troca de seis mensagens EAP-SIM; o valor de n deve ser ajustado para dois; D_{HLR} deve ser desconsiderado, e; na fórmula de D_{AAA_WWAN} (Eq. 6.16) deve ser desconsiderado a primeira fração, que representa o atraso da sinalização recebida do HLR/AuC.

O gráfico comparando os valores de atraso de autenticação para a condição de autenticação completa com os valores de atraso de autenticação para a condição de re-autenticação rápida pode ser visto na figura 6.16 e os resultados obtidos na tabela 6.5.

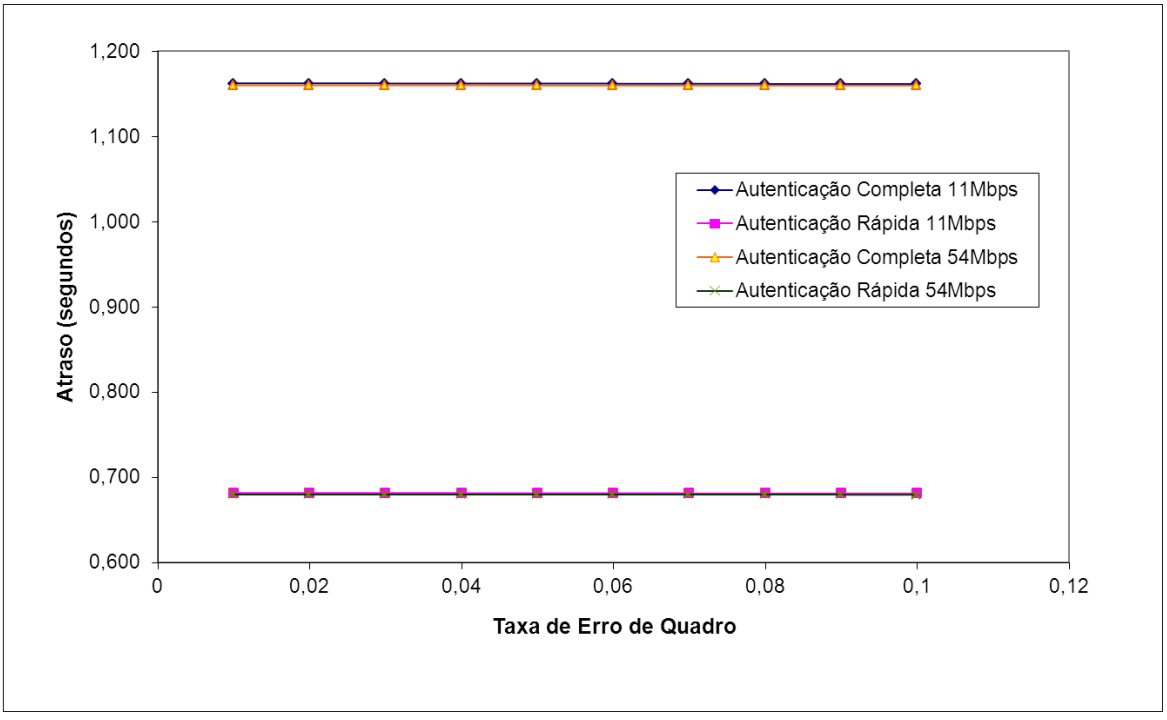


Figura 6.16 – Comparação do atraso de autenticação EAP-SIM completa e rápida versus Taxa de Erro de Quadro (FER)

Tabela 6.5 – Atrasos de autenticação completa e rápida, em segundos, versus FER e taxas de transmissão

Taxa WLAN	FER	Atraso Autenticação Completa	Atraso Re-Autenticação Rápida
11Mbps	0,01	1,16235 s	0,68165 s
	0,02	1,16227 s	0,68159 s
	0,03	1,16218 s	0,68152 s
	0,04	1,16209 s	0,68146 s
	0,05	1,16199 s	0,68139 s
	0,06	1,16190 s	0,68131 s
	0,07	1,16179 s	0,68123 s
	0,08	1,16168 s	0,68115 s
	0,09	1,16157 s	0,68107 s
	0,10	1,16145 s	0,68098 s
54Mbps	0,01	1,16002 s	0,67990 s
	0,02	1,15998 s	0,67988 s
	0,03	1,15995 s	0,67985 s
	0,04	1,15991 s	0,67982 s
	0,05	1,15988 s	0,67980 s
	0,06	1,15984 s	0,67977 s
	0,07	1,15979 s	0,67974 s
	0,08	1,15975 s	0,67970 s
	0,09	1,15971 s	0,67967 s
	0,10	1,15966 s	0,67963 s

Pode ser verificado que a re-autenticação rápida reduziu o atraso em aproximadamente 40%. O atraso médio calculado da autenticação rápida para rede WLAN operando a 11 Mbps foi de 0,682s e para rede WLAN operando a 54 Mbps foi de 0,680s. Apesar dos valores verificados mostrarem uma redução no atraso de autenticação com a utilização de re-autenticação rápida, esta continua uma ordem de grandeza acima do valor de interrupção de serviço recomendado para *handover* em [36].

6.3.2 – Medidas

As medidas realizadas em elementos da rede em operação comercial das operadoras de telefonia Brasil Telecom e Brasil Telecom GSM e os métodos estatísticos utilizados estão detalhados nos Apêndices D e E. As medidas de atraso nos servidores de AAA, rede de sinalização e HLR/AuC em operação foram utilizados para estabelecer os valores práticos

dos parâmetros utilizados para a modelagem analítica. Os valores obtidos com as medidas foram utilizados nos parâmetros listados na tabela 6.2.

Em condições de laboratório foi construída uma rede com elementos em condições controladas, conforme mostrado na figura 6.10, para obter detalhes funcionais e de conformidade dos protocolos e da arquitetura proposta pelo padrão.

Com base na estrutura de laboratório, foram obtidos os seguintes dados:
a) Verificação da conformidade das mensagens de autenticação trocadas em os diversos elementos da rede;
b) Verificação da funcionalidade geral da arquitetura proposta.

Para os testes em laboratório foram utilizados os elementos descritos no seção 6.2.1 e mostrado na figura 6.10 com terminais *Nokia* modelo *N70,* a descrição da topologia e os resultados obtidos estão descritos no Apêndice C.

Como referência comparativa foi também realizada uma medida do tempo de autenticação e conexão à rede durante o *handover* horizontal verificado em rede WWAN comercial. O resultado desta medida e o traçado da sinalização obtido estão listados no Apêndice F.

6.4 – AVALIAÇÃO DOS RESULTADOS

Não é de conhecimento do autor valores publicados de simulação ou medidas realizadas no processo de autenticação de rede WLAN com o uso de protocolo EAP-SIP. Mishra em [49] realizou medidas de autenticação em rede WLAN utilizando os procedimentos definidos no padrão IEEE 802.11i, mas com utilização do protocolo EAP-TLS [50]. Nestas condições a latência observada foi de 1,1s para o procedimento de autenticação completa, este valor está na mesma ordem de grandeza dos valores observados no presente trabalho. Zrelli e Shinoda realizaram estudo com base em autenticação EAP-PEAP em redes sem fio e servidores AAA integrados através da Internet e alcançaram resultados similares [84].

O atraso de autenticação foi devido principalmente à latência dos enlaces utilizados sobre a Internet e ao tempo de processamento dos diversos servidores das diferentes redes envolvidas no processo. O atraso de conexão na camada 3 da rede de dados foi devido

principalmente aos procedimentos de alocação dinâmica de endereço IP (DHCP) e de verificação de duplicidade de endereço IP (ARP).

Pode ser verificado que mesmo sem considerar o atraso da autenticação na rede intermediária e na rede WWAN somente o atraso do servidor AAA na rede WLAN responde por 167ms. Este valor em si já é incompatível com o requisito de tempo máximo de interrupção do serviço recomendado [36] e é devido ao fato da topologia utilizada para o servidor sob teste usar servidores centralizados. O servidor medido era responsável por todas as requisições de AAA geradas pelos os acessos de dados na área de abrangência do serviço, sendo responsável por tratar cerca de 460.000 requisições de autenticação por hora, conforme detalhado no Apêndice D em anexo. Este fato indica claramente que a utilização de arquitetura centralizada de servidor AAA não é recomendada para aplicações que exigem pequenos tempos de resposta de autenticação.

A quantificação do ganho em utilizar servidores AAA descentralizados e da adoção de protocolos AAA mais avançados, tal com DIAMETER [41], fica como sugestão para trabalhos futuros, entre outras listadas no capítulo 8.

Outra observação importante é o fato de que o atraso relativo à *interface* aérea não foi significativo em frente ao atraso total, mesmo em condições de elevada taxa de erro de quadro. Isto é devido principalmente ao fato das mensagens de autenticação utilizando protocolo EAP e das mensagens de requisição de endereço IP (DHCP/ARP) terem pequeno comprimento em *bytes*.

Por fim deve ser ressaltado que a utilização do método de re-autenticação rápida definido no padrão [10], com o objetivo de re-autenticar o usuário frequente que retorna à rede WLAN, não mostrou uma melhora suficiente para resolver o problema identificado. Este resultado se deve principalmente ao fato do terminal na rede WLAN visitada continuar necessitando realizar a autenticação no servidor AAA da rede caseira (servidor EAP) e a utilizar os enlaces da Internet para esta conexão.

7 – ARQUITETURAS ALTERNATIVAS PROPOSTAS

Com base nos resultados obtidos no capítulo 6 ficou claro que devem ser alteradas as arquiteturas utilizadas nos processos de conexão e no processo de autenticação, como premissa básica para permitir a implementação de sistemas capazes de realizar o *handover* vertical entre redes WWAN baseadas em padrões 3GPP [21] e WLAN baseada no padrão IEEE 802.11 [31]. Com os tempos verificados neste trabalho o *handover* vertical no sentido WWAN para WLAN implica na interrupção da comunicação por um tempo significativo o suficiente para ser perceptível, resultar em baixa qualidade e perda de informação pelos usuários do sistema, principalmente para aplicações de comunicação multimídia em tempo real tal como voz e vídeo.

Uma solução normalmente adotada para solucionar o problema verificado é utilizar o método de *soft handover*, mantendo a *interface* aérea da rede WWAN do terminal móvel ligada simultaneamente à *interface* aérea WLAN. Desta forma é possível realizar a transferência da sessão ativa e realizar o *handover* somente depois de o terminal móvel ter capacidade de encaminhar os pacotes IP pela *interface* aérea WLAN, sem dependência dos tempos de atraso verificados no presente trabalho. Mas este método possui os seguintes problemas associados:

a) Elevado consumo de energia no terminal móvel ao manter os dois estágios rádio ligados simultaneamente, reduzindo o tempo de duração da carga da bateria;

b) Complexidade e custo elevado no projeto e fabricação do terminal móvel, pois as duas *interfaces* aéreas necessitam ser totalmente independentes, com capacidade de encaminhar pacotes de forma independente e os procedimentos de conexão e autenticação em uma das *interfaces* devem ocorrer enquanto a sessão continua ativa na outra;

b) Potencial interrupção ou perda da comunicação caso haja um rápido decaimento do sinal da rede de origem antes de completada a realização do *handover*, visto que não há necessidade de otimizar o tempo de conexão e autenticação na nova rede.

A forma mais elegante e eficiente de atacar o problema verificado é a alteração das arquiteturas de conexão e de autenticação à rede WLAN de forma a reduzir o tempo de indisponibilidade da comunicação durante o *handover* para um valor inferior ao

perceptível pelos usuários do sistema. Com esta alteração se evitaria também os problemas inerentes de alternativas, conforme descrito acima.

As alterações propostas nas arquiteturas de conexão e autenticação à rede WLAN são descritas a seguir.

7.1 – ARQUITETURA PROPOSTA PARA PROCEDIMENTO DE CONEXÃO

A utilização de mensagens *Gratuitous* ARP no procedimento de conexão da camada 3 tem como finalidade verificar se o endereço IP atribuído por DHCP não está sendo utilizado, como recomendado pela RFC 2131 [29]. Mas este protocolo introduz um atraso no processo de conexão a redes WLAN não compatível com os requisitos mínimos para manutenção de sessões multimídia ou de voz. O atraso devido a este procedimento pode variar de 0,5 segundo a mais de 1,5 segundos dependendo da implementação realizada. Este comportamento não foi considerado por Banerjee no estudo de gerência de mobilidade em redes SIP descrito em [12], mas foi verificado em todas as implementações de rede de acesso WLAN testadas durante a elaboração deste trabalho, conforme detalhado no capítulo 6.

De maneira geral, as soluções para resolver o problema do tempo despendido na alocação dinâmica de endereços IP podem ser separadas em duas linhas:
a) Manutenção da conexão WWAN ativa em paralelo com a conexão WLAN até a *interface* IP estar completamente apta a encaminhar os pacotes;
b) Identificação de outro método para alocação de endereços IP e verificação de duplicidade de endereços em redes WLAN.

Os problemas decorrentes da manutenção das duas *interfaces* aéreas ativas de forma simultânea estão descritos na introdução deste capítulo e, devido às conclusões encontradas, esta alternativa não será considerada neste trabalho.

A segunda opção para solucionar o problema pode ser, por exemplo, através de propostas similares à de Chou em [43], que sugere a utilização de agentes inteligentes sobre redes WLAN para configurar túnel VPN com endereçamento estático para contornar o tempo gasto com a alocação dinâmica de endereços IP. Apesar da alteração proposta, Chou

termina recomendando que seja realizada em conjunto com o procedimento de *soft handover*, com a manutenção em estado ativo o enlace rádio da rede antiga até o completo término da configuração da camada 3 na nova rede, procedimento que torna dispensável a introdução do novo mecanismo.

A proposta mais adequada é a adoção do protocolo IPv6 [45] na rede de acesso WLAN, incluindo a utilização de endereçamento *stateless*, conforme descrito na recomendação do IETF de autoconfiguração de endereços em [40]. No conjunto de protocolos definidos para o IPv6 o protocolo ARP foi substituído pelo IPv6 *Neighbor Discovery* (ND) conforme descrito em [39]. Para a efetiva utilização desta opção deverá ser verificado em condições reais de rede se as implementações do protocolo ND não apresentam o mesmo problema de elevado tempo de esgotamento de temporização verificado com as implementações do protocolo ARP. Uma rápida avaliação da especificação do protocolo ND [39] indica que algumas variáveis definidas, tais como RETRANS_TIMER e MAX_RTR_SOLICITATION_DELAY, necessitam ter seus valores ajustados para atender ao requisito de tempo máximo de indisponibilidade do serviço em condições de *handover*. Esta conclusão foi exposta pelo presente autor no trabalho referenciado em [74], o qual é incluído na integra no apêndice G.

Mesmo tendo sido previsto para solucionar alguns dos problemas inerentes da versão 4, principalmente com relação à disponibilidade de endereços e QoS, o protocolo IPv6 [45] ainda não está sendo utilizado de forma abrangente pelo mercado. No decorrer do tempo alguns dos recursos desenvolvidos para a versão 6 foram adaptados para o IPv4 e mesmo a demanda inicial de esgotamento dos endereços IPv4 está sendo temporariamente contornada por avanços tais como CIDR (*Classless Inter-Domain Routing*) definido em [44] e o uso exaustivo de NAT [46] nas redes de dados atuais. Desta forma, apesar da utilização ubíqua de IPv6 ser uma solução aderente aos padrões atuais da indústria, ela ainda não se materializou em implementações comerciais de larga escala.

Apesar disso, a proposta de adoção do IPv6 se mostra a mais adequada por permitir os ganhos já desenvolvidos e por possibilitar uma base tecnológica para futuros desenvolvimentos e evoluções.

7.2 – ARQUITETURA PROPOSTA PARA PROCEDIMENTO DE AUTENTICAÇÃO E AVALIAÇÃO DE SEU DESEMPENHO

7.2.1 – Descrição da Arquitetura Proposta

A arquitetura de *roaming* WLAN [19], em conjunto com o processo de autenticação proposto pelo padrão IEEE 802.11i [32], combinada com o protocolo EAP-SIM [10], foi testada no presente trabalho e apresentou valores de atraso incompatíveis com o recomendado para o *handover* de chamadas de voz [36]. O teste realizado se concentrou no procedimento de autenticação completa definido para o protocolo EAP-SIM. O padrão EAP-SIM descreve também a possibilidade de realização de autenticação rápida em casos de retorno do terminal móvel à rede WLAN em algumas condições específicas definidas em [10]. Devido à arquitetura de servidores AAA utilizada, com interconexão via a Internet e os atrasos inerentes a esta conexão, mesmo a utilização da opção de autenticação rápida não oferece solução para o problema verificado, conforme demonstrado também no capítulo 6 deste documento.

Além do padrão EAP-SIM, o padrão IEEE 802.11i [32] permite a utilização de qualquer outro método EAP, e o IETF define também o método EAP-AKA [28] como outra possibilidade de autenticação utilizando dados armazenados nos cartões USIM utilizados nos terminais móveis em redes 3G/UMTS e vetores de autenticação gerados pela rede WWAN. Apesar dos ganhos em relação à segurança, o EAP-AKA apresenta os mesmos problemas de atraso verificados para o EAP-SIM, pois também necessita de servidores AAA realizando função de *proxy*, de autenticador e de consulta à base de dados (HLR/AuC) da rede WWAN. O método EAP-AKA é descrito no capítulo 5 deste trabalho.

Outros autores também já propuseram soluções alternativas para autenticação em redes WLAN no cenário de *handover* vertical. Alguns exemplos mais significativos são listados na sequência.

Chou propôs em [43] a utilização de agentes inteligentes (IA – *Intelligent Agent*) que seriam enviados para a rede para executar os procedimentos de conexão e autenticação com antecedência. UIAs (*User Intelligent Agents*) poderiam ser configurados para se autenticarem em nome do usuário e SIA (*Server Intelligent Agent*) poderia ser configurado

para autenticar localmente os usuários. Para esta proposta ser viabilizada a chave *Ki* armazenada no SIM e no HLR/AuC deve ser compartilhada pelos agentes inteligentes, gerando uma vulnerabilidade no sistema e violando o princípio básico de segurança das redes GSM, que é a proteção da chave de autenticação individual *Ki* de acesso ou leitura por qualquer aplicação não definida pelo 3GPP [47].

Huang desenvolve em [48] um protocolo de autenticação chamado de SAP (*Seamless Authentication Protocol*) em que dois servidores de autenticação compartilham uma chave privativa comum secreta utilizada para gerar chave temporária de *handover*. A rede de acesso WLAN armazena esta chave temporária e a utiliza para admitir o terminal móvel por um curto período de tempo, evitando os atrasos associados à consulta e geração de vetores pela rede WWAN. O tempo de validade da autenticação temporária deve ser o suficiente para permitir que a associação completa seja efetuada em paralelo à sessão ativa. Esta proposta possui qualidades que podem ser exploradas, como a autenticação transparente, mas também cria uma vulnerabilidade adicional ao permitir a autenticação de vários terminais móveis com um mecanismo que utiliza uma única chave comum.

Shidhani e Leung [75] propuseram um esquema de pré-autenticação que deriva novas chaves durante o processo de autenticação completa via utilização de EAP-AKA modificado. Neste esquema proposto, novos *handovers* horizontais na rede WLAN podem utilizar um esquema de pré-autenticação sem a troca de mensagens com o HLR da rede caseira do usuário. Esta proposta significa a alteração de diversos padrões da indústria, incluindo IEEE 802.11, IEEE 802.1x e IETF EAP-AKA, com o consequente impacto nas redes comerciais instaladas. Adicionalmente, a proposta é aplicável somente para os cenários de *handover* horizontal intra/inter-WLAN.

Lim [76] criou uma proposta de autenticação entre redes WiBro (*Wireless Broadband*) e WLAN que depende de relação de confiança entre a rede visitada e a rede alvo, de forma que, a rede visitada gera a informação de identificação temporária para o terminal móvel e a rede alvo, em conjunto com as chaves de autenticação a serem utilizadas pela rede alvo. Após o *handover*, a autenticação completa deve ser realizada pelo terminal móvel para completar a segurança. Esta proposta pressupõe o conhecimento prévio do *handover* pela rede visitada. O trabalho não mostrou nenhuma análise quantitativa de ganho.

Outros trabalhos [77][78] também propõem métodos alternativos de autenticação durante o *handover* em ambientes heterogêneos, mas falham em mostrar resultados quantitativos de melhoria na qualidade em relação aos procedimentos padrões.

Considerando os resultados obtidos, os padrões existentes e as propostas de alteração publicadas até o momento, podemos definir algumas premissas básicas que devem ser seguidas por uma arquitetura de autenticação transparente em rede WLAN de forma a tornar a mesma aplicável nos cenários de *handover* vertical de terminais móveis executando aplicações multimídia *on-line* em tempo real:

a) Manter, no mínimo, o mesmo nível de segurança existente na rede WWAN caseira do usuário;

b) Não impactar negativamente a qualidade da sessão durante o *handover*, isso é, ter duração máxima de interrupção no *handover* de 40ms [36], em conjunto com o procedimento de conexão;

c) Poder realizar autenticação inicial na rede WLAN de forma independente do tempo de espera pelos vetores de autenticação retornados pela rede WWAN;

d) Não comprometimento das chaves compartilhadas utilizadas pela rede WWAN (p. ex.: chave *Ki*).

Com base nas premissas acima e também com foco no fator interoperabilidade com os sistemas atuais é também recomendado que a arquitetura proposta tenha compatibilidade com o padrão IEEE 802.11i [32]. Do ponto de vista do procedimento de autenticação, o suporte ao padrão 802.11i significa que a autenticação deve ser realizada com o uso de mensagens EAP [9], independentemente do método ou mecanismo específico.

Os desafios desta nova arquitetura são: a definição de um método seguro de troca de chaves entre os elementos da arquitetura; a definição de um segredo específico para cada terminal móvel e a rede de acesso WLAN; e, definição de uma forma de compartilhamento segura deste segredo. Adicionalmente, os requisitos anteriores devem ser agrupados em uma arquitetura descentralizada de servidores de autenticação de forma a permitir rápida troca de mensagens de autenticação entre o terminal móvel e o servidor de autenticação.

A arquitetura nova proposta como resultado do trabalho atual se baseia na introdução de um novo elemento funcional na rede WWAN e em cada rede WLAN passível de ser

visitada pelo terminal, a este elemento é dado o nome de Servidor de Distribuição de Chaves (SDC). A figura 7.1 ilustra a arquitetura geral proposta.

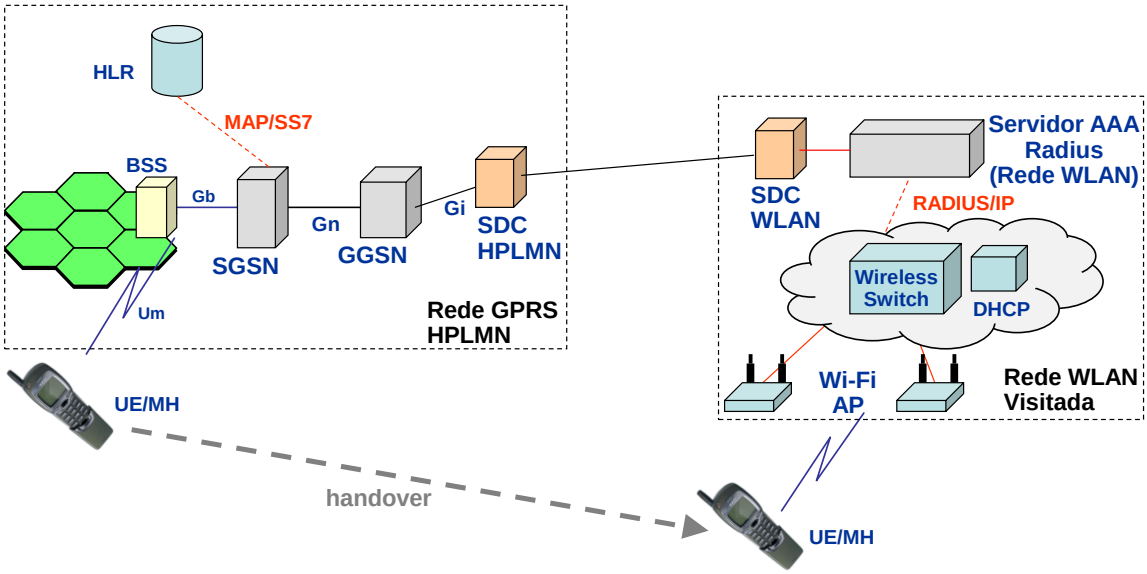


Figura 7.1 – Nova Arquitetura de Autenticação Proposta

Na rede WWAN caseira do terminal o Servidor de Distribuição de Chaves (SDC HPLMN) é colocado na *interface Gi* após o elemento GGSN [21] e possui, para fins de confidencialidade na transmissão de informação, algum mecanismo padrão, como por exemplo, através de túnel IPSec [73]. Na rede GPRS/GSM/UMTS o terminal é autenticado segundo os métodos padrões definido para redes 3GPP, pois nestas redes há mecanismos nativos para garantir a segurança na troca de dados entre o terminal e os elementos de rede, incluindo o GGSN [61]. O novo elemento da arquitetura na rede WWAN caseira do usuário, o SDC HPLMN, pode ser considerado também como tendo conexão segura com o terminal registrado na rede de acesso WWAN, pois o mesmo pode ser colocado internamente na rede local onde se encontra a *interface Gi* e possui relação de confiança com a rede WWAN via o elemento GGSN.

Na rede WLAN visitada o novo elemento Servidor de Distribuição de Chaves (SDC WLAN) é colocado na mesma rede do servidor AAA e deve possuir, para fins de confidencialidade na transmissão de informações, algum mecanismo padrão, como por exemplo, através de túnel IPSec [73].

Entre o SDC HPLMN e os diversos SDC WLAN é considerado haver também algum mecanismo de troca segura de dados, através de métodos padrões de criptografia, que não são escopo desta discussão. Desta forma é assumida a existência de uma relação de confiança de longa duração entre os elementos SDC.

O SDC WLAN tem as funções de:
a) Criar, sob requisição, novos pares de chaves de autenticação, aqui designadas como *Ka*, específicas e vinculadas a uma identificação específica do terminal móvel, como por exemplo: IMSI registrado no cartão SIM/USIM;
b) Enviar as chaves criadas para o SDC HPLMN e para o servidor AAA da rede WLAN através de conexão segura estática, ou seja, previamente configurada.

O SDC HPLMN tem as funções de:
a) Requisitar chave de autenticação específica para o SDC WLAN em nome do terminal móvel da rede WWAN, esta requisição é realizada baseada nas informações enviadas pelo terminal móvel: identificação; localização de célula; e, no SSID da rede WLAN alvo;
b) Manter base de endereços de SDC WLAN associados aos específicos SSID da rede WLAN e a localização geográfica da rede WLAN. Estas informações são fundamentais para garantir a identificação unívoca da rede WLAN e do SDC WLAN associado;
c) Retornar para o terminal móvel a chave *Ka* criada pelo SDC WLAN.

O protocolo de troca de informação entre o novo elemento SDC HPLMN e os terminais móveis ainda registrados na rede WWAN pode ser baseado em protocolo HTTP padrão. Entre os elementos SDC as informações podem ser trocadas via arquivos XML e entre o SDC WLAN e o servidor AAA a informação pode ser trocada via qualquer protocolo de troca de dados seguro suportado pelo servidor AAA.

O procedimento de operação da nova arquitetura se baseia na troca antecipada de chaves temporárias de autenticação através do auxílio da rede WWAN. As chaves trocadas e armazenadas no terminal móvel e no servidor AAA são utilizadas para a autenticação do terminal móvel na rede WLAN, seguindo os princípios definidos no padrão IEEE 802.11i [32].

As funções executadas pelo terminal móvel nesta nova arquitetura são:

a) Enquanto o terminal móvel ainda está registrado na rede WWAN, solicitar que o SBC HPLMN requisite chaves de autenticação para serem enviadas às redes WLAN próximas. As redes WLAN podem ser localizadas através de mecanismo padrão de *scanning* da rede 802.11 [32];
b) Informar ao SDC a identificação do terminal móvel, o SSID da rede WLAN alvo e a célula da rede WWAN em que se encontra;
c) Receber as chaves *Ka* retornadas pelo SDC HPLMN através da rede GPRS e armazená-las em área segura enquanto permanecer no raio de alcance da possível rede WLAN alvo;
d) Ao tomar a decisão de conectar na rede WLAN alvo, utilizar a chave *Ka* recebida na autenticação EAP-SIM no lugar da chave *Ki* armazenada no cartão SIM para validação e geração do material utilizado na autenticação mútua. Esta primeira autenticação é temporária e deve ser feita através do envio de endereço de identificação (NAI) [63] com domínio específico, de forma a informar a natureza temporária desta autenticação para o servidor AAA;
e) Após a autenticação temporária bem sucedida, do registro das aplicações na rede IMS e do completo restabelecimento da sessão, iniciar o procedimento de autenticação completa utilizando os dados padrões originais armazenados no cartão SIM.

O servidor AAA de autenticação da rede WLAN deve ser preparado para suportar as seguintes funções:
a) Realizar a autenticação temporária do terminal móvel com base no endereço NAI retornado e na chave *Ka* específica recebida do SDC WLAN;
b) Para realizar a autenticação temporária o servidor AAA deve implementar o algoritmo A3/A8 [69], ou qualquer outro algoritmo que também seja suportado pelo cartão SIM, para poder gerar os vetores de autenticação de forma autônoma do HLR da rede WWAN, mas baseado no NAI do terminal e na chave *Ka* recebida. Os vetores de autenticação podem ser gerados ao ser recebido a chave *Ka*, com o objetivo de reduzir o atraso durante a autenticação temporária;
c) Controlar o tempo de associação do terminal móvel após a realização da autenticação temporária e desconectar terminais móveis incapazes de realizar autenticação completa após um período pré-definido de tempo;
d) Enviar mensagens RADIUS *accounting* para o servidor AAA intermediário, para registro das atividades no assinante em *roaming*, para fins de tarifação.

Adicionalmente à nova arquitetura de autenticação proposta, a rede WLAN pode possuir uma topologia de servidores AAA descentralizados, rodando com menos carga e mais próximos às redes de acesso, com o objetivo de diminuir o tempo de processamento de autenticação verificado nas medidas realizadas neste trabalho.

7.2.2 – Avaliação de Desempenho da Arquitetura Proposta

Com a nova arquitetura de autenticação proposta se espera que o tempo de indisponibilidade do serviço durante o processo de *handover* vertical seja reduzido para valores menores que os recomendados pelos padrões [36]. Como a troca de chaves *Ka* ocorre antes do procedimento de *handover*, não afeta o tempo do mesmo. O tempo de autenticação durante o *handover* deve ser grandemente reduzido, por não necessitar de consulta à rede WWAN caseira e por não utilizar servidores AAA centralizados de alta capacidade e com enlaces IP via a rede Internet e sobre longas distâncias. Com base na modelagem analítica desenvolvida no capítulo 6 deste trabalho, podemos afirmar que o atraso de autenticação para a nova arquitetura proposta pode ser calculada como:

$$D'_{AUT} = D_{MH} + D_{EAP} + D_{AP} + D'_{AAA\_WLAN} \qquad \text{Eq. 7.1}$$

O valor de atraso para o servidor AAA da rede WLAN para a nova arquitetura proposta pode ser calculado como:

$$D'_{AAA\_WLAN} = \frac{n}{\mu_{AAA} - \lambda_{AAA\_WLAN}} \qquad \text{Eq. 7.2}$$

Onde *n* é o número de pares de mensagens de requisição e resposta RADIUS para a arquitetura descrita, ou seja, três para o cenário de autenticação completa EAP-SIM e os demais parâmetros estão descritos na tabela 6.1.

Os demais componentes da equação 7.1 são calculados conforme as equações 6.3, 6.6 e 6.7. Utilizando os valores listados na tabela 6.2 e FER de 10%, obtemos os seguintes valores de atraso de autenticação para a arquitetura nova proposta, mostrados de forma comparativa com os resultados obtidos para os mecanismos de autenticação padrão:

Tabela 7.1 – Atrasos de autenticação previstos para a arquitetura com SDC proposta

Atraso de Autenticação	**11Mbps (802.11b)**	**54Mbps (802.11g)**
Autenticação Completa Padrão	1,16145 s	1,15966 s
Autenticação Rápida Padrão	0,68098 s	0,67963 s
Atraso de Autenticação (SDC)	86,58 ms	84,79 ms

Os valores calculados de atraso indicam uma melhora considerável no tempo de autenticação, com uma redução no atraso maior que 92% em ambos os casos. Mas este atraso ainda não está dentro do recomendado para interrupção de serviço durante o *handover* [36], mas o valor alcançado já se encontra na mesma ordem de grandeza do recomendado. Analisando os resultados com mais cuidado, verificamos que, somente o tempo de processamento do servidor AAA contribui com 83,6ms do tempo de atraso da tabela 7.1, isso é devido ao fato de termos utilizado os valores de taxa de processamento e de taxa de chegada obtidos a partir de medições em servidor AAA centralizado e de grande porte, conforme detalhado no Apêndice D.

Caso seja seguida a premissa definida para a nova arquitetura proposta, com servidores AAA descentralizados em servidores menores, pode se esperar uma melhora no tempo de atendimento dos mesmos. Esta condição deve ser futuramente modelada e/ou simulada para verificar o grau de melhora que pode trazer além do obtido na redução do tempo de autenticação com a nova arquitetura proposta.

A arquitetura proposta neste capítulo pode também ser utilizada em conjunto com a arquitetura de *roaming* de WLAN [19]. Para isso o servidor AAA intermediário não deve ser mais utilizado como *proxy* para as mensagens de autenticação temporária inicial, mas somente para a autenticação completa realizada em paralelo com a sessão WLAN ativa do terminal móvel e para tratamento de mensagens de RADIUS *accounting*.

Ao lado dos aspectos de melhoria de desempenho caracterizados anteriormente, algumas outras vantagens desta nova arquitetura de autenticação proposta são:
a) Troca antecipada de chaves de autenticação específicas para cada terminal móvel, sem consumo do tempo de autenticação;
b) Utilização de arquitetura de autenticação temporária sem a necessidade de realização de consulta em servidores AAA e bases HLR externas à rede WLAN durante o *handover*;

c) Utilização de chaves individuais específicas e exclusivas para cada terminal móvel durante a autenticação temporária, aumentando o nível geral de segurança na rede WLAN em relação à proposta de Huang [48].

8 – CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho apresentou a avaliação do impacto dos procedimentos de conexão e autenticação em redes WLAN na manutenção de sessões multimídias de tempo real controladas via protocolo SIP [14] durante o *handover* vertical no sentido WWAN para WLAN. Foco principal foi dado na avaliação da introdução de procedimento de autenticação baseado nos padrões IEEE 802.11i [32] e IEEE 802.1x [7] em conjunto com a utilização de protocolo EAP-SIM [10]. O trabalho consistiu de três etapas distintas:

a) Desenvolvimento da modelagem analítica da arquitetura de acesso WLAN e da arquitetura de autenticação apresentada na seção 6.1 deste documento;

b) Medidas realizadas em elementos implantados em rede comercial da operadora de telefonia Brasil Telecom visando extrair valores estatísticos para popular as equações modeladas;

c) Medidas realizadas em laboratório com a finalidade de verificar a conformidade das soluções utilizadas aos protocolos e arquiteturas padronizadas.

Com base nas medidas e nas modelagens analíticas realizadas foi verificado que os tempos gastos com os procedimentos padrões propostos para conexão e autenticação à rede WLAN não são compatíveis com o tempo máximo de interrupção no serviço de voz durante o *handover* conforme recomendado por ETSI em [36]. O relatório técnico do ETSI recomenda o máximo de 40ms de interrupção do serviço de voz e os resultados obtidos neste trabalho mostram que os tempos de conexão e de autenticação em redes WLAN podem atingir, em alguns casos, valores maiores que dois segundos, conforme mostrado no seção 6.3 deste documento. De uma maneira geral, esta interrupção do serviço tem duração suficiente para provocar a perda de informação durante a sessão multimídia de comunicação em tempo real estabelecida pelo usuário. Isto significa que o tempo de interrupção do serviço observado torna o procedimento de *handover* perceptível pelo usuário final que esteja utilizando um serviço de comunicação multimídia em tempo real.

Foi avaliada também a alternativa de autenticação rápida descrita no padrão IETF para o protocolo EAP-SIM, a mesma apresentou uma melhora nos tempos de autenticação de aproximadamente 40%, mas ainda insuficiente para atender a recomendação de interrupção máxima estabelecida pelo ETSI. O procedimento de autenticação rápida é opcional pelo

padrão e válido somente para cenários de re-autenticação de usuários retornando à rede WLAN. Para garantir a segurança, a autenticação rápida deve ser utilizada um número limitado de vezes consecutivas, após o qual deve ser seguida de uma autenticação completa [10]. Devido a estes fatos, o uso de autenticação rápida também não se mostrou viável como alternativa para os cenários testados.

O elevado tempo de conexão do terminal móvel à rede WLAN verificado durante os testes, devido a um procedimento associado à alocação de dados de configuração da camada IP, foi um resultado não esperado do trabalho. A causa deste comportamento se deve ao fato de que após o recebimento dos dados de configuração da *interface* IP, via o protocolo DHCP [29], o terminal móvel utiliza o protocolo ARP [30] para verificar se o endereço IP recebido não está em uso pela rede local. Este procedimento, válido para as redes baseadas em IPv4, introduz um atraso considerável no processo de ativação da *interface* do terminal móvel, pois a confirmação é dada de forma indireta, através da expiração da temporização de mensagem de retorno do protocolo. O valor desta temporização varia de acordo com a implementação realizada no terminal e de acordo com o fabricante, podendo variar de 0,5s a 1,5s, no caso extremo verificado, conforme detalhado no capítulo 6 deste trabalho. Este resultado levou ao estudo de uma proposta de solução específica para o procedimento de conexão à rede, em adição ao trabalho realizado com o procedimento de autenticação.

A solução proposta neste trabalho para solucionar o atraso no procedimento de conexão é baseada na utilização efetiva dos padrões existentes para a evolução da rede IP para a versão 6 (IPv6) [45]. Estes padrões foram desenvolvidos para atender a demanda crescente de soluções técnicas para os problemas decorrentes da utilização massiva crescente da versão 4 do protocolo IP para serviços avançados, com avanços focados em questões específicas, tais como, aumento da disponibilidade de endereços, melhora na priorização de tráfego e na qualidade de serviço, entre outros. Apesar de estar desenvolvido há alguns anos, a adoção do IPv6 e dos novos procedimentos e protocolos advindos desta evolução não tem ocorrido com a velocidade aguardada, devido às razões discutidas no seção 7.1 deste trabalho.

Para a diminuição do atraso evidenciado durante o procedimento de autenticação foi realizado o estudo e desenvolvimento de uma arquitetura nova alternativa à preconizada pelo IETF e 3GPP. A arquitetura nova proposta visa atacar as causas principais de atraso

evidenciados pela modelagem realizada, a saber: o tempo de espera para receber as chaves da rede caseira do assinante e a utilização de enlaces sobre a Internet para encaminhar as mensagens de autenticação até o servidor AAA da rede caseira, para verificar o resultado retornado pelo terminal móvel.

A nova arquitetura proposta introduz um novo elemento Servidor de Distribuição de Chaves (SDC) responsável por realizar a distribuição antecipada das chaves de autenticação temporárias das redes WLAN elegíveis para receber o terminal móvel no próximo *handover*. Com a introdução deste elemento e a alteração de alguns dos procedimentos de autenticação entre o terminal móvel e o servidor AAA da rede WLAN visitada se obteve uma redução significativa no resultado modelado da interrupção do serviço devido à autenticação durante o *handover* vertical. Resultado obtido pela modelagem analítica da nova solução mostrou tempos de interrupção inferiores a 90ms, valores que estão na mesma ordem de grandeza do recomendado pelo ETSI em [36]. Valores ainda menores podem ser obtidos com a utilização de servidores AAA descentralizados e distribuídos na rede WLAN visitada, conforme indicado na seção 7.2.

A nova arquitetura proposta continua a permitir a utilização de arquitetura voltada para o suporte às necessidades de *roaming* de assinantes WLAN, conforme recomendado em [19], e mantém as premissas de segurança definidas pelos padrões atuais, inclusive com a possibilidade de manutenção do algoritmo de autenticação em uso.

8.1 – SUGESTÕES DE TRABALHOS FUTUROS

Este trabalho não pretendeu ser exaustivo na sua abrangência, e devido a isso possui vários desdobramentos possíveis de serem estudados.

Com relação aos tópicos de gerência de localização não contemplados, incluindo os padrões previstos para evolução do processo de autenticação e das arquiteturas de redes os seguintes pontos podem ser explorados:

a) Avaliação da arquitetura de autenticação proposta baseada em Servidores de Distribuição de Chaves através de simulações e medidas em protótipos;

b) Avaliar a utilização de protocolo DIAMETER [41] no lugar do protocolo RADIUS no servidor AAA, como proposta de evolução da arquitetura em estudo;

c) Avaliar a evolução da arquitetura definida para o domínio 3GPP IMS [3] com a utilização do protocolo DIAMETER [41] no lugar do protocolo MAP para consulta à base de dados no elemento HSS, em substituição ao HLR atual;
d) Avaliar a utilização de protocolo EAP-AKA [28] e dos algoritmos de autenticação das redes UMTS como proposta de evolução do protocolo EAP-SIM na arquitetura em estudo;
e) Avaliar o eventual ganho no tempo de autenticação da rede WLAN para *handover* subsequente ao se utilizar o procedimento definido para o protocolo EAP-SIM de re-autenticação rápida, conforme descrito em [10];
f) Avaliar os requisitos de segurança, confidencialidade e criptografia de dados fim a fim necessários entre os terminais móveis e a rede IMS para a utilização de serviços de voz e vídeo-telefonia, os padrões 3GPP IWLAN [4], 3GPP IMS [3] e IEEE 802.11i [32] preveem alguns métodos para isso.

Com relação aos tópicos não cobertos relativos ao *handover* vertical entre redes heterogêneas WWAN e WLAN, os seguintes pontos podem ser explorados:
a) Desenvolvimento de modelo de mobilidade para usuários de serviços multimídia em tempo real em redes WLAN, Pollini em [42] menciona alguns modelos de mobilidade que podem ser utilizados como base;
b) Avaliação de mecanismos preditivos de seleção de rede para *handover*, podendo ser utilizado como base o padrão IEEE 802.21[82];
c) Avaliação de mecanismos de gerência de conexão, em forma de APIs, que poderiam ser incluídos nos terminais móveis para permitir que aplicações obtenham informação e possam participar na tomada de decisões relativas à disponibilidade de redes de acesso heterogêneas e da possibilidade de *handover*.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] 3rd Generation Partnership Project, "3GPP TS 23.003 V7.2.0: "Numbering, addressing and identification (Release 7)"", disponível em: http://www.3gpp.org, Dezembro 2006.

[2] 3rd Generation Partnership Project, "3GPP TS 23.206 V7.5.0: "Voice Call Continuity between Circuit Switched (CS) and IP Multimedia Subsystem (IMS) (Release 7)"", disponível em: http://www.3gpp.org, Dezembro 2007.

[3] 3rd Generation Partnership Project, "3GPP TS 23.228 V7.10.0: "IP Multimedia Subsystem (IMS) (Release 7)"", disponível em: http://www.3gpp.org, Dezembro 2007.

[4] 3rd Generation Partnership Project, "3GPP TS 23.234 V7.5.0: "3GPP system to Wireless Local Area Network (WLAN) interworking (Release 7)"", disponível em: http://www.3gpp.org, Março 2007.

[5] 3rd Generation Partnership Project, "3GPP TR 23.806 V7.0.0: "Voice Call Continuity between CS and IMS Study (Release 7)"", disponível em: http://www.3gpp.org, Dezembro 2005.

[6] 3rd Generation Partnership Project, "3GPP TS 33.234 V7.3.0: "Wireless Local Area Network (WLAN) interworking security (Release 7)"", disponível em: http://www.3gpp.org, Dezembro 2006.

[7] IEEE Computer Society, "IEEE Std 802.1x-2004, IEEE Standard for Local and Metropolitan Area Networks – Port Based Network Access Control", Dezembro 2004.

[8] IEEE Computer Society, "IEEE P802.21/D01.00, Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services", Março 2006.

[9] B. Aboba, et al, "Extensible Authentication Protocol (EAP)", RFC 3748, IETF, disponível em: http://www.ietf.org, Junho 2004.

[10] H. Haverinen, J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, IETF, disponível em: http://www.ietf.org, Janeiro 2006.

[11] C. Rigney, et al, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, IETF, disponível em: http://www.ietf.org, Junho 2000.

[12] N. Banerjee, W. Wu, K. Basu, S. K. Das, “Analysis of SIP-based mobility management in 4G wireless networks,” Computer Communications 27 (2004), pp. 697–707, Janeiro 2004.

[13] M. Zivkovic, et al, “Authentication Across Heterogeneous Networks”, Bell Labs Technical Journal 10(2), pp 39–56, 2005.

[14] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, “SIP: Session Initiation Protocol”, RFC 3261, IETF, disponível em: http://www.ietf.org, Junho 2002.

[15] E. Wedlund, H. Schulzrinne, “ Mobility Support using SIP”, Second ACM/IEEE International Workshop on Wireless and Mobile Multimedia (WoWMoM’99), pp. 76–82, Agosto 1999.

[16] R. Bresil, “Integração entre redes locais sem fios (WLANs) e redes dos sistemas celulares”, Trabalho final (mestrado profissional) – Universidade Estadual de Campinas, Instituto de Computação, Agosto 2004.

[17] S. K. Das, E. Lee, K. Basu, S.K. Sen, “Performance optimization of VoIP calls over wireless links using H.323 protocol”, IEEE Transactions on Computers 52 (6) (2003) pp. 742–752, Junho 2003.

[18] 3rd Generation Partnership Project, “3GPP TS 33.203 V7.4.0: “Access Security for IP-based services (Release 7)””, disponível em: http://www.3gpp.org, Dezembro 2006.

[19] R. Narjala, A. Keddy, J. Rover, A. Sampson, “Standards-based Public Wireless LAN Access and Roaming”, Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on, pp. 632–637, Fevereiro 2006.

[20] European Telecommunications Standards Institute, “ETSI TR 101 957 V1.1.1 (2001-08), “Requirements and Architectures for Interworking between HIPERLAN/2 and 3rd Generation Cellular systems””, disponível em http://www.etsi.org, Agosto 2001.

[21] 3rd Generation Partnership Project, “3GPP TS 23.002 V6.8.0: “Network architecture (Release 6)””, disponível em: http://www.3gpp.org, Junho 2005.

[22] 3rd Generation Partnership Project, “3GPP TS 23.012 V6.4.0: “Location management procedures (Release 6)””, disponível em: http://www.3gpp.org, Junho 2006.

[23] 3rd Generation Partnership Project, “3GPP TS 23.009 V6.4.0: “Handover procedures (Release 6)””, disponível em: http://www.3gpp.org, Março 2006.

[24] J. Postel, "Transmission Control Protocol", RFC 793, IETF, disponível em: http://www.ietf.org, Setembro 1981.

[25] D. Qiao, S. Choi, K. G. Shin, "Goodput Analysis and Link Adaptation for IEEE 802.11ª Wireless LANs", IEEE Transactions on Mobile Computing, vol. 1, no. 4, pp. 278–292, Outubro 2002.

[26] European Telecommunications Standards Institute, "GSM Technical Specification GSM 03.20 (ETS 300 534): "Digital cellular telecommunication system (Phase 2); Security related network functions"", disponível em http://www.etsi.org, Agosto 1997.

[27] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function", IEEE Journal on Selected Areas in Communications, vol. 18, issue: 3, pp. 535–547, Março 2000.

[28] J. Arkko, H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, IETF, disponível em: http://www.ietf.org, Janeiro 2006.

[29] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, IETF, disponível em: http://www.ietf.org, Março 1997.

[30] David C. Plummer, "An Ethernet Address Resolution Protocol", RFC 826, IETF, disponível em: http://www.ietf.org, Novembro 1982.

[31] IEEE Computer Society, "ANSI/IEEE Std 802.11, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999 Edition (R2003), Junho 2003.

[32] IEEE Computer Society, "802.11i, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements", Julho 2004.

[33] ITU, "Introduction to CCITT Signalling System No. 7," ITU-T Recommendation Q.700, ITU-T Telecommunication Standardization Sector of ITU, Março 1993.

[34] S. C. Wang, Y. M. Chen, Tsern-Huei Lee, A. Helmy, "Performance evaluations for hybrid IEEE 802.11b and 802.11g wireless networks", Performance, Computing, and

Communications Conference, IPCCC 2005 (24th IEEE International), pp. 111–118, Abril 2005.

[35] Ed. J. Sermersheim, "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, IETF, disponível em: http://www.ietf.org, Junho 2006.

[36] European Telecommunications Standards Institute, "TR 122 925 V3.1.1 (2000-02) Universal Mobile Telecommunications System (UMTS); Service aspects; Quality of Service and Network Performance (3G TR 22.925 version 3.1.1 Release 1999)", disponível em http://www.etsi.org, Abril 1999.

[37] J. M. Juran, "Juran's Quality Control handbook", 4ª edição, McGraw-Hill, 1988.

[38] William W. Dorner, "Using Microsoft Excel for Weibull Analysis ", disponível em: http://www.qualitydigest.com/jan99/html/weibull.html

[39] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, IETF, disponível em: http://www.ietf.org, Dezembro 1998.

[40] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, IETF, disponível em: http://www.ietf.org, Dezembro 1998.

[41] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", RFC 3588, IETF, disponível em: http://www.ietf.org, Setembro 2003.

[42] Gregory P. Pollini, K. S. Meier-Hellstern, D. J. Goodman, "Signaling Traffic Volume Generated by Mobile and Personal Communications", IEEE Communications Magazine, Junho 1995.

[43] Li-Der Chou, W. C. Lai, Y. C. Lin, C. M. Huang, C. H. Lin, "Intelligent Agent over WLAN with Seamless Handover and Load Balancing", Communication Technology, 2006. ICCT'06. International Conference on, pp. 1–7, Novembro 2006.

[44] Y. Rekhter, T. Li, "An Architecture for IP Address Allocation with CIDR", RFC 1518, IETF, disponível em: http://www.ietf.org, Setembro 1993.

[45] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, IETF, disponível em: http://www.ietf.org, Dezembro 1998.

[46] P. Srisuresh, K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, IETF, disponível em: http://www.ietf.org, Janeiro 2001.

[47] 3rd Generation Partnership Project, "3GPP: Technical Specification Group SA WG3; A Guide to 3rd Generation Security (3G TR 33.900 version 1.2.0)" disponível em: http://www.3gpp.org, Janeiro 2000.

[48] S C.-H. Huang, H Zhu, W. Zhang, "SAP: Seamless Authentication Protocol for Vertical Handoff in Heterogeneous Wireless Networks", Proceedings of the 3rd

international conference on Quality of service in heterogeneous wired/wireless networks, Article No. 32, 2006.

[49] A. Mishra, M. Shin, W. A. Arbaugh, “Pro-active Key Distribution using Neighbor Graphs”, IEEE Wireless Communications, vol. 11, Fevereiro 2004.

[50] B. Aboba, D. Simon, “PPP EAP TLS Authentication Protocol”, RFC 2716, IETF, disponível em: http://www.ietf.org, Outubro 1999.

[51] 3rd Generation Partnership Project, “3GPP TS 29.002 V7.8.0: “Technical Specification Group Core Network and Terminals; Mobile Application Part (MAP) specification; (Release 7)””, disponível em: http://www.3gpp.org, Junho 2007.

[52] ITU-T Recommendation Q.711 (07/1996): “Functional description of the signalling connection control part”, ITU-T Telecommunication Standardization Sector of ITU, Julho 1996.

[53] ITU-T Recommendation Q.771, Signalling System No. 7 “Functional Description of Transaction Capabilities”, ITU-T Telecommunication Standardization Sector of ITU, Março 1993.

[54] ITU-T Recommendation Q.701, “Functional Description of the Message Transfer Part (MTP) of Signalling System No. 7”, ITU-T Telecommunication Standardization Sector of ITU, Março 1993.

[55] 3rd Generation Partnership Project, “3GPP TS 23.101 V7.0.0: “Technical Specification Group Services and System Aspects General Universal Mobile Telecommunications System (UMTS) architecture (Release 7)””, disponível em: http://www.3gpp.org, Junho 2007.

[56] Isabela Barreto Duncan, "Modelagem e Análise do Protocolo IEEE 802.11", COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 2006.

[57] M. Gast, “802.11 Wireless Networks: The Definitive Guide”, O’Reilly, 2002.

[58] I. F. Akyildiz, J. McNair, J. Ho, H. Uzunalioğlu, W. Wang, “Mobility Management for Next Generation Wireless Systems,” Proc. IEEE, vol. 87, no. 8, pp. 1347–84, Agosto 1999.

[59] N. Nasser, A. Hasswa, H. Hassanein, “Handoffs in Fourth Generation Heterogeneous Networks”, IEEE Communications Magazine, pp. 96–103, Outubro 2006.

[60] J. Eberspächer, H-J Vögel, C. Bettstetter, “GSM Switching, Services and Protocols”, 2ª edição, John Willey & Sons, 1999.

[61] H. Kaaranen, A. Ahtiainen, L. Laitinen, S. Naghian, V. Niemi, “UMTS Networks - Architecture, Mobility and Services”, 2ª edição, John Willey & Sons, 2005.

[62] 3rd Generation Partnership Project, "3GPP TS 24.007 V7.0.0: "Technical Specification Group Core Network; Mobile radio *interface* signalling layer 3; General aspects (Release 7)"", disponível em: http://www.3gpp.org, Setembro 2005.

[63] B. Aboba, M. Beadles, J. Arkko, P. Eronen, "The Network Access Identifier", RFC 4282, IETF, disponível em: http://www.ietf.org, Dezembro 2005.

[64] A. M. Al Naamany, A. A. Shidhani, H. Bourdoucen, "IEEE 802.11 Wireless LAN Security Overview", IJCSNS International Journal of Computer Science and Network Security, Vol. 6 No. 5B, pp. 138–156, Maio 2006.

[65] Infocomm Development Authority of Singapore and Intel Corporation, "Public WLAN Interworking Study - Validation Report", disponível em http://www.ida.gov.sg/doc/Programmes/Programmes_Level3/Wireless%20BroadbanB%20market%20Development/WBMD_Call_for_Collaboration_Public_Document_Annex_D_-_IWS-Validation_Report_v1.0.pdf, Setembro 2004.

[66] J. Bannister, P. Mather, S. Coope, "Convergence Technologies for 3G Networks: IP, UMTS, EGPRS and ATM", John Wiley & Sons, 2004.

[67] G. Camarillo, M. A. Garcia-Martin, "The 3G IP Multimedia Subsystem (IMS)", 2ª edição, John Wiley & Sons, 2006.

[68] 3rd Generation Partnership Project, "3GPP TS 29.198-01 V6.3.1: "Open Service Access (OSA) Application Programming *Interface* (API); Part 1: Overview (Release 6)"", disponível em: http://www.3gpp.org, Dezembro 2004.

[69] 3rd Generation Partnership Project, "3GPP TS 55.205 V7.0.0: "Specification of the GSM-MILENAGE Algorithms: An example algorithm set for the GSM Authentication and Key Generation functions A3 and A8 (Release 7)"", disponível em: http://www.3gpp.org, Junho 2007.

[70] 3rd Generation Partnership Project, "3GPP TS 35.206 V7.0.0: "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 2: Algorithm Specification (Release 7)"", disponível em: http://www.3gpp.org, Junho 2007.

[71] A. de la Oliva, C. J. Bernados, T. Melia, I. Soto, A. Vidal, A. Banchs, "A Case Study: IEEE 802.21 Enabled Mobile Terminals for Optimized WLAN/3G Handovers", Mobile Computing and Communications Review, Volume 11, Number 2, pp. 29–40, Abril 2007.

[72] I. F. Akyildiz, J. Xie, S. Mohanty, “A Survey of Mobility Management in Next-Generation All-IP-Based Wireless Systems,” IEEE Wireless Communication, pp. 16–28, Agosto 2004.

[73] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, IETF, disponível em: http://www.ietf.org, Novembro 1998.

[74] Sebastião Boanerges Ribeiro Junior, Paulo R. L. Gondim, “Layer 3 Initialization Procedures Recommendation in Next Generation Heterogeneous Mobile Networks”, Communications and Networking in China, 1st International Business Conference, Chinacombiz 2008, Series: Communications in Computer and Information Science , Vol. 26, pp. 68–75, Agosto 2008.

[75] Ali Al Shidhani, Victor C. M. Leung, “Pre-Authentication Schemes for UMTS-WLAN Interworking”, EURASIP Journal on Wireless Communications and Networking, Volume 2009, Article ID 806563, Fevereiro 2009.

[76] Sun-Hee Lim, O. Yi, C.-H. Jung, K.-S. Bang, “A Fast and Efficient Authentication Protocol for a Seamless Handover between a WLAN and WiBro”, IEEE COMSWARE 2007, Janeiro 2007.

[77] J. S. Moon, J. H. Park, D. G. Lee, I.-Y. Lee, “Authentication and ID-Based Key Management Protocol in Pervasive Environment”, Wireless Personal Communications, Agosto 2009.

[78] D. Nikitopoulos, N. Papaoulakis, A. Trakos, A. Giamas, E. Sykas, M. Theologou, “Authentication platform for seamless handover in heterogeneous environments”, IEEE ICAS/ICNS 2005, Outubro 2005.

[79] IEEE Computer Society, “802.11n, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 5: Enhancements for Higher Throughput”, Outubro 2009.

[80] GSM Association, “IR.61, WLAN Roaming Guidelines 3.1.0”, Agosto 2004.

[81] ETSI, “TS 183 020 V1.1.1 (2006-03) Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment: Roaming in TISPAN NGN Network Acesses; Interface Protocol Definition”, disponível em http://www.etsi.org, 2006.

[82] IEEE Computer Society, “802.21, IEEE Standard for Local and metropolitan area networks – Part 21: Media Independent Handover Services”, Janeiro 2009.

[83] Internet Engineering Task Forcce (IETF), “Handover Keying (hokey) Charter”, disponível em http://datatracker.ietf.org/wg/hokey/charter/, acessado em Maio/2011.

[84] S. Zrelli, Y. Shinoda, “Experimental Evaluation of EAP Performance in Roaming Scenarios”, AINTEC '07 Proceedings of the 3rd Asian conference on Internet Engineering: Sustainable Internet, pp. 86-98, Novembro 2007.

APÊNDICES

APÊNDICE A – CÁLCULO DE ATRASO DE TRANSMISSÃO WLAN

O atraso de transmissão fim a fim utilizado neste trabalho foi calculado utilizando o modelo desenvolvido por Bianchi em [27] para avaliação do desempenho de redes WLAN 802.11 que utilizam DCF (*Distributed Coordination Function*). Para referências sobre DCF e redes IEEE 802.11 podem ser consultados [31], [34], [25], além do próprio trabalho em referência [27].

Em [27], Bianchi realiza uma avaliação analítica da taxa efetiva em condição de saturação, ou seja, é assumido que cada estação tem uma fila de transmissão não vazia. Com base nesta premissa é construído um modelo markoviano para obter a probabilidade de transmissão em um único *time slot* e, com base nos eventos que podem ocorrer neste *time slot*, a expressão da taxa efetiva dos métodos de acesso. Neste Apêndice é feito somente um resumo das formulações encontradas por Bianchi e dos valores calculados com base nestas e que foram utilizadas como base no trabalho presente.

Bianchi nos oferece a equação abaixo para o cálculo da taxa efetiva normalizada do sistema:

$$S = \frac{P_s P_{tr} E[P]}{(1 - P_{tr})\sigma + P_{tr} P_s T_s + P_{tr}(1 - P_s) T_c} \qquad \text{Eq. A.1}$$

Sendo que *E(P)* é o tamanho médio do pacote de *payload* e σ é a duração de um *time slot* vazio. As probabilidades listadas na equação A.1 são definidas como:

$$P_{tr} = 1 - (1 - \tau)^n \qquad \text{Eq. A.2}$$

Onde P_{tr} é a probabilidade de que há pelo menos uma transmissão no *time slot* considerado, sendo *n* o número de estações utilizando o canal e τ a probabilidade de cada estação transmitir. P_s é a probabilidade da transmissão no canal ser bem sucedida e é definido por Bianchi como:

$$P_s = \frac{n\tau(1 - \tau)^{n-1}}{P_{tr}} = \frac{n\tau(1 - \tau)^{n-1}}{1 - (1 - \tau)^n} \qquad \text{Eq. A.3}$$

T_s é o tempo médio em que o canal é escutado como ocupado por uma transmissão bem sucedida e T_c é o tempo médio em que o canal é escutado como ocupado durante condição de colisão. Estes tempos são descritos por Bianchi, para o mecanismo de acesso básico do DCF, como:

$$\begin{cases} T_s^{bas} = & H + E[P] + \text{SIFS} + \delta + \text{ACK} + \text{DIFS} + \delta \\ T_c^{bas} = & H + E[P^*] + \text{DIFS} + \delta \end{cases} \qquad \text{Eq. A.4}$$

Onde, *H* é o tempo de transmissão do cabeçalho do pacote, ACK é o tempo de transmissão do pacote de reconhecimento, SIFS (*Short InterFrame Space*) e DIFS (*Distributed InterFrame Space*) são tempos definidos para os procedimentos do DCF, *E[P*]* é o tempo médio do maior pacote de *payload* envolvido em uma colisão e δ é o atraso de propagação.

Por fim, Bianchi calculou a probabilidade de cada estação transmitir como sendo:

$$\tau(p) = \frac{2}{1 + W + pW \sum_{i=0}^{m-1} (2p)^i} \qquad \text{Eq. A.5}$$

Onde, $W = CW_{min}$ e *CW* é o *Contention Window* adotado pelo esquema de *backoff* exponencial do DCF, *m* é "*maximum backoff stage*" tal que $CW_{max} = 2^m W$ e *p* é a probabilidade de colisão condicional.

Os valores utilizados para o para o cálculo do resultado de *S* (equação A.1) foram retirados do próprio trabalho de Bianchi e atualizados com dados fornecidos por Wang em [34] e com o padrão definido pelo IEEE [31]. A tabela A.1 sumariza estes dados:

Tabela A.1 – Dados utilizados no cálculo da taxa efetiva da rede WLAN [27], [34] e [31]

Parâmetros	**802.11b**	**802.11g**
H	400 *bits*	400 *bits*
ACK	240 *bits*	240 *bits*
Taxa de transmissão	11 Mbps	54 Mbps
Atraso de propagação - δ	1 μs	1 μs
Slot time - σ	20 μs	20 μs
SIFS	10 μs	10 μs
DIFS	50 μs	50 μs
W	31	15
m	5	5
n	10	10

Com base nos dados acima e na fórmula de taxa efetiva deduzida por Bianchi foram calculados os atrasos de transmissão esperados na *interface* aérea para diferentes taxas de transmissão e tamanho de pacotes (MPDU) igual a 1500 *bytes*, conforme resumido na tabela A.2.

Tabela A.2 – Cálculo do atraso de transmissão

Taxa de Transmissão	**Atraso de Transmissão**
11Mbps (802.11b)	1,445 ms
54Mbps (802.11g)	0,419 ms

APÊNDICE B – REGISTRO DOS TRAÇADOS DE SINALIZAÇÃO

Os traçados de sinalização utilizados neste trabalho foram obtidos por meio de ferramentas e equipamentos específicos. Para a obtenção das mensagens de sinalização sobre rede IP foi utilizado o programa *Wireshark* (*http://www.wireshark.org/*). Para obtenção das mensagens de sinalização sobre a rede SS7 foi utilizada ferramenta comercial de monitoração de redes de sinalização *AcceSS7* fornecida pelo fabricante *Agilent Technologies* (*http://www.home.agilent.com*) e instalada na rede da operadora Brasil Telecom GSM.

APÊNDICE C – DIAGRAMA DE REDE EM LABORATÓRIO E EXPERIMENTOS REALIZADOS

Neste Apêndice é mostrado inicialmente o diagrama de rede e conexões entre os equipamentos utilizados no cenário fim a fim montado em laboratório, bem como os resultados das medidas obtidas neste ambiente.

C.1 – DIAGRAMA DE REDE

Na figura C.1 é mostrada a topologia implementada e os elementos principais utilizados.

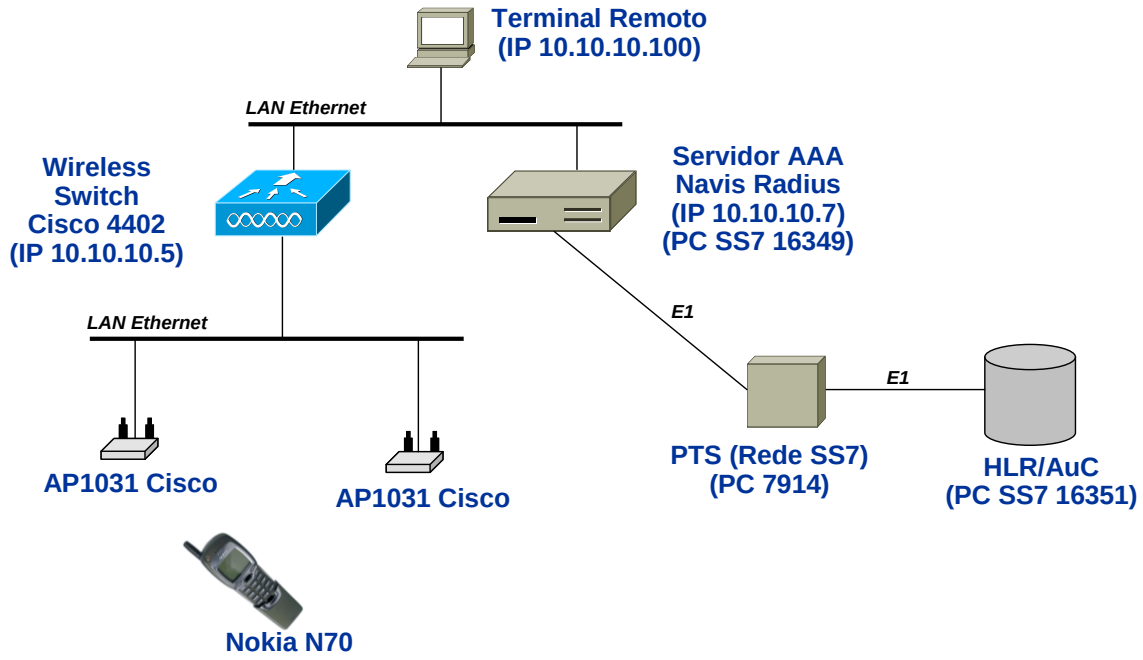


Figura C.1 – Topologia de teste montada em laboratório

Para a rede de acesso WLAN foi utilizado um *Wireless Controller* e dois AP do fabricante *Cisco*, para o servidor de autenticação foi utilizado o produto *Navis RADIUS* do fabricante *Alcatel-Lucent*, para a rede de sinalização foi utilizado o elemento PTS existente na rede STFC do operador Brasil Telecom e para o HLR/AuC foi utilizado uma base de teste do fabricante *UTStarcom*. Os dados de configuração de cada um dos elementos na sua respectiva rede estão indicados na figura C.1.

Na rede local entre o *Wireless Controller* e o servidor AAA foram capturados os pacotes de autenticação com a utilização da ferramenta *Wireshark* referenciada no Apêndice B.

C.2 – EXPERIMENTOS REALIZADOS NA REDE LOCAL EM LABORATÓRIO

Abaixo é listado um exemplo de uma sequência de troca de sinalização RADIUS entre a rede WLAN e o servidor AAA capturada com a ferramenta *Wireshark*, pode ser verificado que os pacotes EAP estão encapsulados dentro de parâmetros AVP RADIUS e que os campos do protocolo trocados seguem o especificado, como definido pelos padrões IETF [10][11].

```
No.     Time        Source                Destination           Protocol
Info
     13 14.270846   30.30.30.5            30.30.30.7            RADIUS
Access-Request(1) (id=76, l=226)

Frame 13 (268 bytes on wire, 268 bytes captured)
    Arrival Time: Oct 29, 2007 16:32:07.930784000
    [Time delta from previous packet: 14.270846000 seconds]
    [Time since reference or first frame: 14.270846000 seconds]
    Frame Number: 13
    Packet Length: 268 bytes
    Capture Length: 268 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:udp:radius:eap]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: Airespac_43:60:40 (00:0b:85:43:60:40), Dst:
SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
    Destination: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        Address: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Source: Airespac_43:60:40 (00:0b:85:43:60:40)
        Address: Airespac_43:60:40 (00:0b:85:43:60:40)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Type: IP (0x0800)
Internet Protocol, Src: 30.30.30.5 (30.30.30.5), Dst: 30.30.30.7
(30.30.30.7)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 254
    Identification: 0x0000 (0)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
```

```
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0xc1a7 [correct]
        [Good: True]
        [Bad : False]
    Source: 30.30.30.5 (30.30.30.5)
    Destination: 30.30.30.7 (30.30.30.7)
User Datagram Protocol, Src Port: 32769 (32769), Dst Port: radius (1812)
    Source port: 32769 (32769)
    Destination port: radius (1812)
    Length: 234
    Checksum: 0x8bd3 [correct]
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x4c (76)
    Length: 226
    Authenticator: 4752698855D204177A70224AD103CED1
    Attribute Value Pairs
        AVP: l=45  t=User-Name(1): 3SvCYCT5O+kNYnGj4AQ3pOq7U@sim-
operator1.com
            User-Name: 3SvCYCT5O+kNYnGj4AQ3pOq7U@sim-operator1.com
        AVP: l=19  t=Calling-Station-Id(31): 00-15-A0-FE-CF-8A
            Calling-Station-Id: 00-15-A0-FE-CF-8A
        AVP: l=26  t=Called-Station-Id(30): 00-0B-85-23-DA-D0:EAPSIM
            Called-Station-Id: 00-0B-85-23-DA-D0:EAPSIM
        AVP: l=6  t=NAS-Port(5): 29
            NAS-Port: 29
        AVP: l=6  t=NAS-IP-Address(4): 30.30.30.5
            NAS-IP-Address: 30.30.30.5 (30.30.30.5)
        AVP: l=6  t=NAS-Identifier(32): 4400
            NAS-Identifier: 4400
        AVP: l=12  t=Vendor-Specific(26) v=Airespace, Inc (formerly Black
Storm Networks)(14179)
            VSA: l=6 t=Unknown-Attribute(1): 00000001
                Unknown-Attribute: 00000001
        AVP: l=6  t=Service-Type(6): Framed-User(2)
            Service-Type: Framed-User (2)
        AVP: l=6  t=Framed-MTU(12): 1300
            Framed-MTU: 1300
        AVP: l=6  t=NAS-Port-Type(61): Wireless-802.11(19)
            NAS-Port-Type: Wireless-802.11 (19)
        AVP: l=50  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Response (2)
                Id: 1
                Length: 48
                Type: Identity [RFC3748] (1)
                Identity (43 bytes): 3SvCYCT5O+kNYnGj4AQ3pOq7U@sim-
operator1.com
        AVP: l=18  t=Message-Authenticator(80):
A62DC2CEDD02AF54E439AA5850961358
            Message-Authenticator: A62DC2CEDD02AF54E439AA5850961358
```

```
No.     Time        Source                Destination           Protocol
Info
     14 14.275214   30.30.30.7            30.30.30.5            RADIUS
Access-challenge(11) (id=76, l=67)

Frame 14 (109 bytes on wire, 109 bytes captured)
    Arrival Time: Oct 29, 2007 16:32:07.935152000
    [Time delta from previous packet: 0.004368000 seconds]
    [Time since reference or first frame: 14.275214000 seconds]
    Frame Number: 14
    Packet Length: 109 bytes
    Capture Length: 109 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:udp:radius:eap]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3), Dst:
Airespac_43:60:40 (00:0b:85:43:60:40)
    Destination: Airespac_43:60:40 (00:0b:85:43:60:40)
        Address: Airespac_43:60:40 (00:0b:85:43:60:40)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Source: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        Address: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Type: IP (0x0800)
Internet Protocol, Src: 30.30.30.7 (30.30.30.7), Dst: 30.30.30.5
(30.30.30.5)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 95
    Identification: 0xcd1e (52510)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (0x11)
    Header checksum: 0x3627 [correct]
        [Good: True]
        [Bad : False]
    Source: 30.30.30.7 (30.30.30.7)
    Destination: 30.30.30.5 (30.30.30.5)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 32769 (32769)
    Source port: radius (1812)
    Destination port: 32769 (32769)
    Length: 75
    Checksum: 0x3f23 [correct]
Radius Protocol
    Code: Access-challenge (11)
    Packet identifier: 0x4c (76)
```

```
    Length: 67
    Authenticator: 0294F976D0DE800C8F9441EDDF4AC9AB
    Attribute Value Pairs
        AVP: l=18  t=Message-Authenticator(80):
22AE1C384B2B78A90E50FE6F7D61655E
            Message-Authenticator: 22AE1C384B2B78A90E50FE6F7D61655E
        AVP: l=18  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Request (1)
                Id: 2
                Length: 16
                Type: EAP-SIM Nokia IP smart card authentication
[Haverinen] (18)
                subtype: 10 (Start)
                Reserved: 0
                Attribute: AT_VERSION_LIST
                    Type: 15
                    Length: 2 (8 bytes)
                    Value: 000200010000
        AVP: l=5  t=State(24): 353833
            State: 353833
        AVP: l=6  t=Session-Timeout(27): 180
            Session-Timeout: 180
```

```
No.     Time        Source                Destination           Protocol
Info
     15 14.296434   30.30.30.5            30.30.30.7            RADIUS
Access-Request(1) (id=77, l=215)

Frame 15 (257 bytes on wire, 257 bytes captured)
    Arrival Time: Oct 29, 2007 16:32:07.956372000
    [Time delta from previous packet: 0.021220000 seconds]
    [Time since reference or first frame: 14.296434000 seconds]
    Frame Number: 15
    Packet Length: 257 bytes
    Capture Length: 257 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:udp:radius:eap]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: Airespac_43:60:40 (00:0b:85:43:60:40), Dst:
SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
    Destination: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        Address: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Source: Airespac_43:60:40 (00:0b:85:43:60:40)
        Address: Airespac_43:60:40 (00:0b:85:43:60:40)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Type: IP (0x0800)
Internet Protocol, Src: 30.30.30.5 (30.30.30.5), Dst: 30.30.30.7
(30.30.30.7)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 243
    Identification: 0x0000 (0)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0xc1b2 [correct]
        [Good: True]
        [Bad : False]
    Source: 30.30.30.5 (30.30.30.5)
    Destination: 30.30.30.7 (30.30.30.7)
User Datagram Protocol, Src Port: 32769 (32769), Dst Port: radius (1812)
    Source port: 32769 (32769)
    Destination port: radius (1812)
    Length: 223
    Checksum: 0x3af4 [correct]
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x4d (77)
```

```
    Length: 215
    Authenticator: 96A068334BFC7D7D33AFBA337D18FBCF
    Attribute Value Pairs
        AVP: l=45  t=User-Name(1): 3SvCYCT5O+kNYnGj4AQ3pOq7U@sim-
operator1.com
            User-Name: 3SvCYCT5O+kNYnGj4AQ3pOq7U@sim-operator1.com
        AVP: l=19  t=Calling-Station-Id(31): 00-15-A0-FE-CF-8A
            Calling-Station-Id: 00-15-A0-FE-CF-8A
        AVP: l=26  t=Called-Station-Id(30): 00-0B-85-23-DA-D0:EAPSIM
            Called-Station-Id: 00-0B-85-23-DA-D0:EAPSIM
        AVP: l=6  t=NAS-Port(5): 29
            NAS-Port: 29
        AVP: l=6  t=NAS-IP-Address(4): 30.30.30.5
            NAS-IP-Address: 30.30.30.5 (30.30.30.5)
        AVP: l=6  t=NAS-Identifier(32): 4400
            NAS-Identifier: 4400
        AVP: l=12  t=Vendor-Specific(26) v=Airespace, Inc (formerly Black
Storm Networks)(14179)
            VSA: l=6 t=Unknown-Attribute(1): 00000001
                Unknown-Attribute: 00000001
        AVP: l=6  t=Service-Type(6): Framed-User(2)
            Service-Type: Framed-User (2)
        AVP: l=6  t=Framed-MTU(12): 1300
            Framed-MTU: 1300
        AVP: l=6  t=NAS-Port-Type(61): Wireless-802.11(19)
            NAS-Port-Type: Wireless-802.11 (19)
        AVP: l=34  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Response (2)
                Id: 2
                Length: 32
                Type: EAP-SIM Nokia IP smart card authentication
[Haverinen] (18)
                subtype: 10 (Start)
                Reserved: 0
                Attribute: AT_NONCE_MT
                    Type: 7
                    Length: 5 (20 bytes)
                    Value: 0000B15CB7AC77FEF611DD735437C3A4A925
                Attribute: AT_SELECTED_VERSION
                    Type: 16
                    Length: 1 (4 bytes)
                    Value: 0001
        AVP: l=5  t=State(24): 353833
            State: 353833
        AVP: l=18  t=Message-Authenticator(80):
E233DB85414DD971AF7CAE1F75DA5D1D
            Message-Authenticator: E233DB85414DD971AF7CAE1F75DA5D1D
```

```
No.     Time        Source                Destination           Protocol
Info
     16 14.304731   30.30.30.7            30.30.30.5            RADIUS
Access-challenge(11) (id=77, l=219)

Frame 16 (261 bytes on wire, 261 bytes captured)
    Arrival Time: Oct 29, 2007 16:32:07.964669000
    [Time delta from previous packet: 0.008297000 seconds]
    [Time since reference or first frame: 14.304731000 seconds]
    Frame Number: 16
    Packet Length: 261 bytes
    Capture Length: 261 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:udp:radius:eap]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3), Dst:
Airespac_43:60:40 (00:0b:85:43:60:40)
    Destination: Airespac_43:60:40 (00:0b:85:43:60:40)
        Address: Airespac_43:60:40 (00:0b:85:43:60:40)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Source: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        Address: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Type: IP (0x0800)
Internet Protocol, Src: 30.30.30.7 (30.30.30.7), Dst: 30.30.30.5
(30.30.30.5)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 247
    Identification: 0xcd1f (52511)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (0x11)
    Header checksum: 0x358e [correct]
        [Good: True]
        [Bad : False]
    Source: 30.30.30.7 (30.30.30.7)
    Destination: 30.30.30.5 (30.30.30.5)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 32769 (32769)
    Source port: radius (1812)
    Destination port: 32769 (32769)
    Length: 227
    Checksum: 0xfd99 [correct]
Radius Protocol
    Code: Access-challenge (11)
    Packet identifier: 0x4d (77)
```

```
    Length: 219
    Authenticator: 4BB568C3D83FEBD1B82CC241C7FD6A51
    Attribute Value Pairs
        AVP: l=18  t=Message-Authenticator(80):
777E0500B1DCF39322F6674D885AA71D
            Message-Authenticator: 777E0500B1DCF39322F6674D885AA71D
        AVP: l=170  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Request (1)
                Id: 3
                Length: 168
                Type: EAP-SIM Nokia IP smart card authentication
[Haverinen] (18)
                subtype: 11 (Challenge)
                Reserved: 0
                Attribute: AT_RAND
                    Type: 1
                    Length: 9 (36 bytes)
                    Value:
000064779228E6DF79D453408817B47FAA485EAEA8EF317F...
                Attribute: AT_MAC
                    Type: 11
                    Length: 5 (20 bytes)
                    Value: 00001D8AED5ECE2145DF9B3454AA3A2BCBDB
                Attribute: AT_IV
                    Type: 129
                    Length: 5 (20 bytes)
                    Value: 0000846DFBF9AFEBFE4C451A6A8CE262DA4E
                Attribute: AT_ENCR_DATA
                    Type: 130
                    Length: 21 (84 bytes)
                    Value:
0000578352D6402870DA887AA9F998DA39FD1B6614E31E3D...
        AVP: l=5  t=State(24): 353834
            State: 353834
        AVP: l=6  t=Session-Timeout(27): 180
            Session-Timeout: 180
```

```
No.     Time        Source                Destination           Protocol
Info
     17 14.777140   30.30.30.5            30.30.30.7            RADIUS
Access-Request(1) (id=78, l=211)

Frame 17 (253 bytes on wire, 253 bytes captured)
    Arrival Time: Oct 29, 2007 16:32:08.437078000
    [Time delta from previous packet: 0.472409000 seconds]
    [Time since reference or first frame: 14.777140000 seconds]
    Frame Number: 17
    Packet Length: 253 bytes
    Capture Length: 253 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:udp:radius:eap]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: Airespac_43:60:40 (00:0b:85:43:60:40), Dst:
SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
    Destination: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        Address: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Source: Airespac_43:60:40 (00:0b:85:43:60:40)
        Address: Airespac_43:60:40 (00:0b:85:43:60:40)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Type: IP (0x0800)
Internet Protocol, Src: 30.30.30.5 (30.30.30.5), Dst: 30.30.30.7
(30.30.30.7)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 239
    Identification: 0x0000 (0)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
    Header checksum: 0xc1b6 [correct]
        [Good: True]
        [Bad : False]
    Source: 30.30.30.5 (30.30.30.5)
    Destination: 30.30.30.7 (30.30.30.7)
User Datagram Protocol, Src Port: 32769 (32769), Dst Port: radius (1812)
    Source port: 32769 (32769)
    Destination port: radius (1812)
    Length: 219
    Checksum: 0xc378 [correct]
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x4e (78)
```

```
    Length: 211
    Authenticator: 12A0F9DE47CD5E2851EC11F4A4CBBA3D
    Attribute Value Pairs
        AVP: l=45  t=User-Name(1): 3SvCYCT5O+kNYnGj4AQ3pOq7U@sim-
operator1.com
            User-Name: 3SvCYCT5O+kNYnGj4AQ3pOq7U@sim-operator1.com
        AVP: l=19  t=Calling-Station-Id(31): 00-15-A0-FE-CF-8A
            Calling-Station-Id: 00-15-A0-FE-CF-8A
        AVP: l=26  t=Called-Station-Id(30): 00-0B-85-23-DA-D0:EAPSIM
            Called-Station-Id: 00-0B-85-23-DA-D0:EAPSIM
        AVP: l=6  t=NAS-Port(5): 29
            NAS-Port: 29
        AVP: l=6  t=NAS-IP-Address(4): 30.30.30.5
            NAS-IP-Address: 30.30.30.5 (30.30.30.5)
        AVP: l=6  t=NAS-Identifier(32): 4400
            NAS-Identifier: 4400
        AVP: l=12  t=Vendor-Specific(26) v=Airespace, Inc (formerly Black
Storm Networks)(14179)
            VSA: l=6 t=Unknown-Attribute(1): 00000001
                Unknown-Attribute: 00000001
        AVP: l=6  t=Service-Type(6): Framed-User(2)
            Service-Type: Framed-User (2)
        AVP: l=6  t=Framed-MTU(12): 1300
            Framed-MTU: 1300
        AVP: l=6  t=NAS-Port-Type(61): Wireless-802.11(19)
            NAS-Port-Type: Wireless-802.11 (19)
        AVP: l=30  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Response (2)
                Id: 3
                Length: 28
                Type: EAP-SIM Nokia IP smart card authentication
[Haverinen] (18)
                subtype: 11 (Challenge)
                Reserved: 0
                Attribute: AT_MAC
                    Type: 11
                    Length: 5 (20 bytes)
                    Value: 0000A12F0B733729F1788AEAF7AFD159FF11
        AVP: l=5  t=State(24): 353834
            State: 353834
        AVP: l=18  t=Message-Authenticator(80):
9C42CA6EC6B614773D536346711B4302
            Message-Authenticator: 9C42CA6EC6B614773D536346711B4302
```

```
No.     Time        Source                Destination           Protocol
Info
     18 14.787857   30.30.30.7            30.30.30.5            RADIUS
Access-Accept(2) (id=78, l=229)

Frame 18 (271 bytes on wire, 271 bytes captured)
    Arrival Time: Oct 29, 2007 16:32:08.447795000
    [Time delta from previous packet: 0.010717000 seconds]
    [Time since reference or first frame: 14.787857000 seconds]
    Frame Number: 18
    Packet Length: 271 bytes
    Capture Length: 271 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:udp:radius:eap]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3), Dst:
Airespac_43:60:40 (00:0b:85:43:60:40)
    Destination: Airespac_43:60:40 (00:0b:85:43:60:40)
        Address: Airespac_43:60:40 (00:0b:85:43:60:40)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Source: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        Address: SunMicro_12:ef:e3 (00:03:ba:12:ef:e3)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
    Type: IP (0x0800)
Internet Protocol, Src: 30.30.30.7 (30.30.30.7), Dst: 30.30.30.5
(30.30.30.5)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 257
    Identification: 0xcd20 (52512)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (0x11)
    Header checksum: 0x3583 [correct]
        [Good: True]
        [Bad : False]
    Source: 30.30.30.7 (30.30.30.7)
    Destination: 30.30.30.5 (30.30.30.5)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 32769 (32769)
    Source port: radius (1812)
    Destination port: 32769 (32769)
    Length: 237
    Checksum: 0x0628 [correct]
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x4e (78)
```

```
    Length: 229
    Authenticator: DF2CB6F9C9EEB4D04AC5634D24E9B1DD
    Attribute Value Pairs
        AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
            VSA: l=52 t=MS-MPPE-Recv-Key(17):
80AB234E8AE5CBF82FD58D7E453409F2F2EC3D0C282219B5...
                MS-MPPE-Recv-Key:
80AB234E8AE5CBF82FD58D7E453409F2F2EC3D0C282219B5...
        AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
            VSA: l=52 t=MS-MPPE-Send-Key(16):
80ACD3E69ED719C64D4ED114498774D6AB95393E2003ABD7...
                MS-MPPE-Send-Key:
80ACD3E69ED719C64D4ED114498774D6AB95393E2003ABD7...
        AVP: l=45  t=User-Name(1): 3SvCYCT5O+kNYnGj4AQ3pOq7U@sim-
operator1.com
            User-Name: 3SvCYCT5O+kNYnGj4AQ3pOq7U@sim-operator1.com
        AVP: l=18  t=Message-Authenticator(80):
B5C60F3CA6D7537E696A1E27B8C4042B
            Message-Authenticator: B5C60F3CA6D7537E696A1E27B8C4042B
        AVP: l=6  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Success (3)
                Id: 3
                Length: 4
        AVP: l=6  t=Service-Type(6): Framed-User(2)
            Service-Type: Framed-User (2)
        AVP: l=6  t=Session-Timeout(27): 90
            Session-Timeout: 90
        AVP: l=6  t=Framed-IP-Address(8): Negotiated
            Framed-IP-Address: Negotiated
        AVP: l=6  t=Termination-Action(29): RADIUS-Request(1)
            Termination-Action: RADIUS-Request (1)
```

C.3 – EXPERIMENTOS REALIZADOS NA REDE SS7 EM LABORATÓRIO

Nas medidas realizadas na rede de sinalização SS7 foi utilizada a ferramenta *AcceSS7* referenciada no Apêndice B. Os dados capturados possuem as mesmas informações verificadas em pedidos de envio de dados de autenticação realizados nos procedimentos normais de uma rede GSM, conforme traçado mostrado no Apêndice E. Abaixo são listados os pares de mensagens *Send Authentication Information* (SAI) de requisição e resposta capturadas durante os testes.

```
10:41:37.486 AM  Link: ->BSA-BSAUTSSG_0
  SI: SCCP  SSF: NN   DPC: DF-BSAUTSH1  OPC: DF-BSA4AL1  SLS: 1

   1  |           |ITU.WHITE.LAP
   1  | 0|0101100 |BIB = 0,  BSN =  44
   2  | 0|0110101 |FIB = 0,  FSN =  53
   3  | 00|111111 |Length Indicator : MSU, LI =  63 octets
   4  |           |ITU.WHITE.MTP
   4  | 1000|0011 |Service Indicator = SCCP, SSF = National Network
   5  | 1101 1111 |DPC :    16351 dec,   3FDF hex
   6  | 01|111111 |
   7  | 1111 0111 |OPC :    16349 dec,   3FDD hex
   8  | 0001|1111 |SLS :        1 dec,      1 hex
   9  |           |ITU.WHITE.SCCP
   9 F| 0000 1001 |MT = Unitdata (UDT)
  10 F| 0000 0001 |Protocol Class = class 1
  11 V| 0000 0011 |Pointer to Called Party Address Parameter = 3
  12 V| 0001 0010 |Pointer to Calling Party Address Parameter = 18
  13 V| 0001 1111 |Pointer to Data Parameter = 31
  14 V| 0000 1111 |LI of Called Party Address parameter = 15 octet(s)
  15 V| 0101 0011 |Addr Ind: Route=PC&SSN; GT=TT&NP&ES&NoA; PC=Y; SSN=Y
  16 V| 1101 1111 | Point Code : 16351 dec, 3FDF hex
  17 V| 0011 1111 | Point Code
  18 V| 0000 0110 | Subsystem Number =   6  HLR Home Location Register
  19 V| 0000 1001 | Translation Type =   9  9h
  20 V| 0001|0001 | Numbering Plan & Encoding Scheme
  21 V| 0|0000011 | Nature of Address Indicator
  22 V| 0010|0111 | Address Signal
  23 V| 0001|0100 | Address Signal
  24 V| 1001|0110 | Address Signal
  25 V| 0000|1000 | Address Signal
  26 V| 0011|0010 | Address Signal
  27 V| 1001|0110 | Address Signal
  28 V| 0111|0101 | Address Signal
  29 V| 0000|0100 | Address Signal
  30 V| 0000 1101 |LI of Calling Party Address parameter = 13 octet(s)
  31 V| 0101 0011 |Addr Ind: Route=PC&SSN; GT=TT&NP&ES&NoA; PC=Y; SSN=Y
  32 V| 1101 1101 | Point Code : 16349 dec, 3FDD hex
  33 V| 0011 1111 | Point Code
  34 V| 0000 0111 | Subsystem Number =   7  VLR Visited Location Register
  35 V| 0000 1001 | Translation Type =   9  9h
  36 V| 0001|0001 | Numbering Plan & Encoding Scheme
  37 V| 0|0000011 | Nature of Address Indicator
  38 V| 1001|0001 | Address Signal
  39 V| 0111|0000 | Address Signal
```

```
40 V| 0011|1000 | Address Signal
41 V| 1001|0001 | Address Signal
42 V| 0101|1000 | Address Signal
43 V| 0000|0001 | Address Signal
44 V| 0011 1100 |LI of Data parameter = 60 octet(s)
45  |           |IMT.2000.MAP
45 M| 0110 0010 |TCAP Message Type = Begin
46 M| 0|0111010 |Total TCAP Message length = 58 octet(s)
47 M| 0100 1000 |Originating Transaction ID tag
48 M| 0|0000100 |Originating Transaction ID length = 4 octet(s)
49 M| 0101 1100 |Transaction ID  = 5C190012 hex
50 M| 0001 1001 |Transaction ID
51 M| 0000 0000 |Transaction ID
52 M| 0001 0010 |Transaction ID
53 M| 0110 1011 |Dialogue tag
54 M| 0|0011110 |Dialogue length = 30 octet(s)
55 M| 0010 1000 |External tag
56 M| 0|0011100 |External length = 28 octet(s)
57 M| 0000 0110 |Object Identifier tag
58 M| 0|0000111 |Object Identifier length = 7 octet(s)
59 M| 0000 0000 |Dialogue-as-ID value ccitt
60 M| 0001 0001 |Dialogue-as-ID value q
61 M| 1000 0110 |Dialogue-as-ID value 773
62 M| 0000 0101 |Dialogue-as-ID value
63 M| 0000 0001 |Dialogue-as-ID value as
64 M| 0000 0001 |Dialogue-as-ID value DialoguePDU
65 M| 0000 0001 |Dialogue-as-ID value version 1
66 M| 1010 0000 |Single-ASN.1-type tag
67 M| 0|0010001 |Single-ASN.1-type length = 17 octet(s)
68 M| 0110 0000 |Dialogue Request (AARQ-apdu) tag
69 M| 0|0001111 |Dialogue Request (AARQ-apdu) length = 15 octet(s)
70 O| 1000 0000 |Protocol Version tag
71 O| 0|0000010 |Protocol Version length = 2 octet(s)
72 O| 0000 0111 |Protocol Version
73 O| 1000 0000 |Protocol Version
74 M| 1010 0001 |Application Context Name tag
75 M| 0|0001001 |Application Context Name length = 9 octet(s)
76 M| 0000 0110 |Object Identifier tag
77 M| 0|0000111 |Object Identifier length = 7 octet(s)
78 M| 0000 0100 |Application Context Name ccitt identified organisation
79 M| 0000 0000 |Application Context Name etsi
80 M| 0000 0000 |Application Context Name mobile domain
81 M| 0000 0001 |Application Context Name GSM/UMTS Network
82 M| 0000 0000 |Application Context Name AC
83 M| 0000 1110 |Application Context Name infoRetrieval
84 M| 0000 0010 |Application Context Name version 2
85 M| 0110 1100 |Component Portion tag
86 M| 0|0010010 |Component Portion length = 18 octet(s)
87 M| 1010 0001 |Component Type Tag = Invoke
88 M| 0|0010000 |Component length = 16 octet(s)
89 M| 0000 0010 |Invoke ID tag
90 M| 0|0000001 |Invoke ID length = 1 octet(s)
91 M| 0000 0001 | Invoke ID  =    1 dec, 01 hex
92 M| 0000 0010 |Local Operation Code tag
93 M| 0|0000001 |Local Operation Code length = 1 octet(s)
94 F| 0011 1000 |Operation Code = Send Authentication Information
95 M| 0000 0100 |IMSI Tag
96 M| 0000 1000 |IMSI length =     8 octet(s)
97 M| 0010|0111 | MCC2 / MCC1, MCC  = 724 (bcd)
98 M| 0001|0100 | NMSI / MCC3
99 M| 1001|0110 | NMSI,   NMSI = 169802369574
```

```
 100 M| 0000|1000 | NMSI Digits
 101 M| 0011|0010 | NMSI Digits
 102 M| 1001|0110 | NMSI Digits
 103 M| 0111|0101 | NMSI Digits
 104 M| 1111|0100 | NMSI Digits



10:41:37.924 AM  Link: ->BSA-BSA4AL1_0
  SI: SCCP  SSF: NN   DPC: DF-BSA4AL1  OPC: DF-BSAUTSH1  SLS: 4

   1  |           |ITU.WHITE.LAP
   1  | 1|0001011 |BIB = 1,  BSN =  11
   2  | 1|1000010 |FIB = 1,  FSN =  66
   3  | 00|111111 |Length Indicator : MSU, LI =  63 octets
   4  |           |ITU.WHITE.MTP
   4  | 1000|0011 |Service Indicator = SCCP, SSF = National Network
   5  | 1101 1101 |DPC :    16349 dec,   3FDD hex
   6  | 11|111111 |
   7  | 1111 0111 |OPC :    16351 dec,   3FDF hex
   8  | 0100|1111 |SLS :        4 dec,      4 hex
   9  |           |ITU.WHITE.SCCP
   9 F| 0001 0001 |MT = Extended Unitdata (XUDT)
  10 F| 1000 0001 |Protocol Class = class 1
  11 F| 0000 1111 |Hop Counter = 15 dec
  12 V| 0000 0100 |Pointer to Called Party Address Parameter = 4
  13 V| 0001 0001 |Pointer to Calling Party Address Parameter = 17
  14 V| 0010 0000 |Pointer to Data Parameter = 32
  15 V| 1111 0001 |Pointer to start of optional part = 241
  16 V| 0000 1101 |LI of Called Party Address parameter = 13 octet(s)
  17 V| 0101 0011 |Addr Ind: Route=PC&SSN; GT=TT&NP&ES&NoA; PC=Y; SSN=Y
  18 V| 1101 1101 | Point Code : 16349 dec, 3FDD hex
  19 V| 0011 1111 | Point Code
  20 V| 0000 0111 | Subsystem Number =   7  VLR Visited Location Register
  21 V| 0000 1001 | Translation Type =   9  9h
  22 V| 0001|0001 | Numbering Plan & Encoding Scheme
  23 V| 0|0000011 | Nature of Address Indicator
  24 V| 1001|0001 | Address Signal
  25 V| 0111|0000 | Address Signal
  26 V| 0011|1000 | Address Signal
  27 V| 1001|0001 | Address Signal
  28 V| 0101|1000 | Address Signal
  29 V| 0000|0001 | Address Signal
  30 V| 0000 1111 |LI of Calling Party Address parameter = 15 octet(s)
  31 V| 0101 0011 |Addr Ind: Route=PC&SSN; GT=TT&NP&ES&NoA; PC=Y; SSN=Y
  32 V| 1101 1111 | Point Code : 16351 dec, 3FDF hex
  33 V| 0011 1111 | Point Code
  34 V| 0000 0110 | Subsystem Number =   6  HLR Home Location Register
  35 V| 0000 1001 | Translation Type =   9  9h
  36 V| 0001|0001 | Numbering Plan & Encoding Scheme
  37 V| 0|0000011 | Nature of Address Indicator
  38 V| 0010|0111 | Address Signal
  39 V| 0001|0100 | Address Signal
  40 V| 1001|0110 | Address Signal
  41 V| 0000|1000 | Address Signal
  42 V| 0011|0010 | Address Signal
  43 V| 1001|0110 | Address Signal
  44 V| 0111|0101 | Address Signal
  45 V| 0000|0100 | Address Signal
  46 V| 1101 0001 |LI of Data parameter = 209 octet(s)
  47  |           |IMT.2000.MAP
```

```
 48 M| 0110 0100 |TCAP Message Type = End
 49 M| 1|0000010 |Total TCAP Message length = 259 octet(s)
 50 M| 0000 0001 | Length Of Contents
 51 M| 0000 0011 | Length Of Contents
 52 M| 0100 1001 |Destination Transaction ID tag
 53 M| 0|0000100 |Destination Transaction ID length = 4 octet(s)
 54 M| 0101 1100 |Transaction ID  = 5C190012 hex
 55 M| 0001 1001 |Transaction ID
 56 M| 0000 0000 |Transaction ID
 57 M| 0001 0010 |Transaction ID
 58 M| 0110 1011 |Dialogue tag
 59 M| 0|0101010 |Dialogue length = 42 octet(s)
 60 M| 0010 1000 |External tag
 61 M| 0|0101000 |External length = 40 octet(s)
 62 M| 0000 0110 |Object Identifier tag
 63 M| 0|0000111 |Object Identifier length = 7 octet(s)
 64 M| 0000 0000 |Dialogue-as-ID value ccitt
 65 M| 0001 0001 |Dialogue-as-ID value q
 66 M| 1000 0110 |Dialogue-as-ID value 773
 67 M| 0000 0101 |Dialogue-as-ID value
 68 M| 0000 0001 |Dialogue-as-ID value as
 69 M| 0000 0001 |Dialogue-as-ID value DialoguePDU
 70 M| 0000 0001 |Dialogue-as-ID value version 1
 71 M| 1010 0000 |Single-ASN.1-type tag
 72 M| 0|0011101 |Single-ASN.1-type length = 29 octet(s)
 73 M| 0110 0001 |Dialogue Response (AARE-apdu) tag
 74 M| 0|0011011 |Dialogue Response (AARE-apdu) length = 27 octet(s)
 75 O| 1000 0000 |Protocol Version tag
 76 O| 0|0000010 |Protocol Version length = 2 octet(s)
 77 O| 0000 0111 |Protocol Version
 78 O| 1000 0000 |Protocol Version
 79 M| 1010 0001 |Application Context Name tag
 80 M| 0|0001001 |Application Context Name length = 9 octet(s)
 81 M| 0000 0110 |Object Identifier tag
 82 M| 0|0000111 |Object Identifier length = 7 octet(s)
 83 M| 0000 0100 |Application Context Name ccitt identified organisation
 84 M| 0000 0000 |Application Context Name etsi
 85 M| 0000 0000 |Application Context Name mobile domain
 86 M| 0000 0001 |Application Context Name GSM/UMTS Network
 87 M| 0000 0000 |Application Context Name AC
 88 M| 0000 1110 |Application Context Name infoRetrieval
 89 M| 0000 0010 |Application Context Name version 2
 90 M| 1010 0010 |Result tag
 91 M| 0|0000011 |Result length = 3 octet(s)
 92 M| 0000 0010 |Integer tag
 93 M| 0|0000001 |Integer length = 1 octet(s)
 94 M| 0000 0000 | Result = Accepted
 95 M| 1010 0011 |Result Source Diagnostic tag
 96 M| 0|0000101 |Result Source Diagnostic length = 5 octet(s)
 97 M| 1010 0001 |Dialogue Service User tag
 98 M| 0|0000011 |Dialogue Service User length = 3 octet(s)
 99 O| 0000 0010 |Integer tag
100 O| 0|0000001 |Integer length = 1 octet(s)
101 O| 0000 0000 | Dialogue Service User = Null
102 M| 0110 1100 |Component Portion tag
103 M| 1|0000001 |Component Portion length = 206 octet(s)
104 M| 1100 1110 | Length Of Contents
105 M| 1010 0010 |Component Type Tag = Return Result (Last)
106 M| 1|0000001 |Component length = 203 octet(s)
107 M| 1100 1011 | Length Of Contents
108 M| 0000 0010 |Invoke ID tag
```

```
 109 M| 0|0000001 |Invoke ID length = 1 octet(s)
 110 M| 0000 0001 | Invoke ID  =    1 dec, 01 hex
 111 O| 0011 0000 |Sequence tag
 112 O| 1|0000001 |Sequence length = 197 octet(s)
 113 O| 1100 0101 | Length Of Contents
 114 O| 0000 0010 |Local Operation Code tag
 115 O| 0|0000001 |Local Operation Code length = 1 octet(s)
 116 F| 0011 1000 |Operation Code = Send Authentication Information
 117 M| 0011 0000 |Authentication Set List Tag
 118 M| 1000 0000 |Authentication Set List length indicator
 119 M| 0011 0000 |Authentication Set Tag
 120 M| 1000 0000 |Authentication Set length indicator
 121 M| 0000 0100 |Random (Rand) Tag
 122 M| 0001 0000 |Random (Rand) length =    16 octet(s)
 123 M| 1110 0101 | Random (Rand) = E58D46516232F9D313EA6C4A228E9968 hex
 124 M| 1000 1101 | Random (Rand)
 125 M| 0100 0110 | Random (Rand)
 126 M| 0101 0001 | Random (Rand)
 127 M| 0110 0010 | Random (Rand)
 128 M| 0011 0010 | Random (Rand)
 129 M| 1111 1001 | Random (Rand)
 130 M| 1101 0011 | Random (Rand)
 131 M| 0001 0011 | Random (Rand)
 132 M| 1110 1010 | Random (Rand)
 133 M| 0110 1100 | Random (Rand)
 134 M| 0100 1010 | Random (Rand)
 135 M| 0010 0010 | Random (Rand)
 136 M| 1000 1110 | Random (Rand)
 137 M| 1001 1001 | Random (Rand)
 138 M| 0110 1000 | Random (Rand)
 139 M| 0000 0100 |Authentication Request Response (Sres) Tag
 140 M| 0000 0100 |Authentication Request Response (Sres) length =     4
octet(s)
 141 M| 1010 1101 | Authentication Request Response (Sres) = ADB70002 hex
 142 M| 1011 0111 | Authentication Request Response (Sres)
 143 M| 0000 0000 | Authentication Request Response (Sres)
 144 M| 0000 0010 | Authentication Request Response (Sres)
 145 M| 0000 0100 |Ciphering Key (Kc) Tag
 146 M| 0000 1000 |Ciphering Key (Kc) length =     8 octet(s)
 147 M| 0011 1101 | Ciphering Key (Kc) = 3D9DBEBC6C862C00 hex
 148 M| 1001 1101 | Ciphering Key (Kc)
 149 M| 1011 1110 | Ciphering Key (Kc)
 150 M| 1011 1100 | Ciphering Key (Kc)
 151 M| 0110 1100 | Ciphering Key (Kc)
 152 M| 1000 0110 | Ciphering Key (Kc)
 153 M| 0010 1100 | Ciphering Key (Kc)
 154 M| 0000 0000 | Ciphering Key (Kc)
 155 M| 0000 0000 |EOC for Authentication Set
 156 M| 0000 0000 |EOC length =     0 octet(s)
 157 M| 0011 0000 |Authentication Set Tag
 158 M| 1000 0000 |Authentication Set length indicator
 159 M| 0000 0100 |Random (Rand) Tag
 160 M| 0001 0000 |Random (Rand) length =    16 octet(s)
 161 M| 1011 1101 | Random (Rand) = BD002B2C9B60B7F045A55B54B0480561 hex
 162 M| 0000 0000 | Random (Rand)
 163 M| 0010 1011 | Random (Rand)
 164 M| 0010 1100 | Random (Rand)
 165 M| 1001 1011 | Random (Rand)
 166 M| 0110 0000 | Random (Rand)
 167 M| 1011 0111 | Random (Rand)
 168 M| 1111 0000 | Random (Rand)
```

```
 169 M| 0100 0101 | Random (Rand)
 170 M| 1010 0101 | Random (Rand)
 171 M| 0101 1011 | Random (Rand)
 172 M| 0101 0100 | Random (Rand)
 173 M| 1011 0000 | Random (Rand)
 174 M| 0100 1000 | Random (Rand)
 175 M| 0000 0101 | Random (Rand)
 176 M| 0110 0001 | Random (Rand)
 177 M| 0000 0100 |Authentication Request Response (Sres) Tag
 178 M| 0000 0100 |Authentication Request Response (Sres) length =     4
octet(s)
 179 M| 0101 0110 | Authentication Request Response (Sres) = 5608C7B6 hex
 180 M| 0000 1000 | Authentication Request Response (Sres)
 181 M| 1100 0111 | Authentication Request Response (Sres)
 182 M| 1011 0110 | Authentication Request Response (Sres)
 183 M| 0000 0100 |Ciphering Key (Kc) Tag
 184 M| 0000 1000 |Ciphering Key (Kc) length =     8 octet(s)
 185 M| 1101 0001 | Ciphering Key (Kc) = D18FD16E874C9000 hex
 186 M| 1000 1111 | Ciphering Key (Kc)
 187 M| 1101 0001 | Ciphering Key (Kc)
 188 M| 0110 1110 | Ciphering Key (Kc)
 189 M| 1000 0111 | Ciphering Key (Kc)
 190 M| 0100 1100 | Ciphering Key (Kc)
 191 M| 1001 0000 | Ciphering Key (Kc)
 192 M| 0000 0000 | Ciphering Key (Kc)
 193 M| 0000 0000 |EOC for Authentication Set
 194 M| 0000 0000 |EOC length =     0 octet(s)
 195 M| 0011 0000 |Authentication Set Tag
 196 M| 1000 0000 |Authentication Set length indicator
 197 M| 0000 0100 |Random (Rand) Tag
 198 M| 0001 0000 |Random (Rand) length =    16 octet(s)
 199 M| 0101 1000 | Random (Rand) = 584750F8573E4CF89FAEF40BF957CA9F hex
 200 M| 0100 0111 | Random (Rand)
 201 M| 0101 0000 | Random (Rand)
 202 M| 1111 1000 | Random (Rand)
 203 M| 0101 0111 | Random (Rand)
 204 M| 0011 1110 | Random (Rand)
 205 M| 0100 1100 | Random (Rand)
 206 M| 1111 1000 | Random (Rand)
 207 M| 1001 1111 | Random (Rand)
 208 M| 1010 1110 | Random (Rand)
 209 M| 1111 0100 | Random (Rand)
 210 M| 0000 1011 | Random (Rand)
 211 M| 1111 1001 | Random (Rand)
 212 M| 0101 0111 | Random (Rand)
 213 M| 1100 1010 | Random (Rand)
 214 M| 1001 1111 | Random (Rand)
 215 M| 0000 0100 |Authentication Request Response (Sres) Tag
 216 M| 0000 0100 |Authentication Request Response (Sres) length =     4
octet(s)
 217 M| 1011 0011 | Authentication Request Response (Sres) = B3C0087D hex
 218 M| 1100 0000 | Authentication Request Response (Sres)
 219 M| 0000 1000 | Authentication Request Response (Sres)
 220 M| 0111 1101 | Authentication Request Response (Sres)
 221 M| 0000 0100 |Ciphering Key (Kc) Tag
 222 M| 0000 1000 |Ciphering Key (Kc) length =     8 octet(s)
 223 M| 0000 1011 | Ciphering Key (Kc) = 0BF8C82C1AE60800 hex
 224 M| 1111 1000 | Ciphering Key (Kc)
 225 M| 1100 1000 | Ciphering Key (Kc)
 226 M| 0010 1100 | Ciphering Key (Kc)
 227 M| 0001 1010 | Ciphering Key (Kc)
```

```
 228 M| 1110 0110 | Ciphering Key (Kc)
 229 M| 0000 1000 | Ciphering Key (Kc)
 230 M| 0000 0000 | Ciphering Key (Kc)
 231 M| 0000 0000 |EOC for Authentication Set
 232 M| 0000 0000 |EOC length =     0 octet(s)
 233 M| 0011 0000 |Authentication Set Tag
 234 M| 1000 0000 |Authentication Set length indicator
 235 M| 0000 0100 |Random (Rand) Tag
 236 M| 0001 0000 |Random (Rand) length =    16 octet(s)
 237 M| 1100 0110 | Random (Rand) = C6B253033264E016E6C97784DD6A2514 hex
 238 M| 1011 0010 | Random (Rand)
 239 M| 0101 0011 | Random (Rand)
 240 M| 0000 0011 | Random (Rand)
 241 M| 0011 0010 | Random (Rand)
 242 M| 0110 0100 | Random (Rand)
 243 M| 1110 0000 | Random (Rand)
 244 M| 0001 0110 | Random (Rand)
 245 M| 1110 0110 | Random (Rand)
 246 M| 1100 1001 | Random (Rand)
 247 M| 0111 0111 | Random (Rand)
 248 M| 1000 0100 | Random (Rand)
 249 M| 1101 1101 | Random (Rand)
 250 M| 0110 1010 | Random (Rand)
 251 M| 0010 0101 | Random (Rand)
 252 M| 0001 0100 | Random (Rand)
 253 M| 0000 0100 |Authentication Request Response (Sres) Tag
 254 M| 0000 0100 |Authentication Request Response (Sres) length =     4
octet(s)
 255 M| 1001 0001 | Authentication Request Response (Sres) = 91F4 hex
 256 M| 1111 0100 | Authentication Request Response (Sres)
 257 M| 0001 0000 | Illegal tag - should be Ciphering Key (Kc)
 258 M| 0000 0100 | Unexpected Parameter length =     4 octet(s)
 259 M| 1100 0001 | Illegal tag - should be EOC
 260 M| 0000 0000 |EOC for Authentication Set List
 261 M| 0110 1110 |EOC length =   110 octet(s)
 262  |           |ITU.WHITE.SCCP
 261 O| 0000 0010 |Undefined Parameter
 262 O| 0000 0000 |Undefined Parameter Length
```

C.4 – MEDIDAS DE ATRASO INDIVIDUAL EM LABORATÓRIO

Foram também medidos os valores de atrasos em cada elemento, apesar destes valores não representarem as condições existentes em redes reais operando comercialmente e não poderem ser utilizados para validar a modelagem analítica realizada. Os valores médios encontrados na montagem em laboratório estão listados na tabela C.1.

Tabela C.1 – Valores médios de atraso nas medidas de laboratório

SS7	HLR/AuC	Servidor AAA	Terminal/AP
51 ms	406 ms	7,34 ms	21,11 ms

O valor obtido de atraso para a rede SS7 se refere ao tempo de transporte da mensagem de retorno do AuC com os valores dos *triplets* para autenticar o terminal. O valor de atraso do HLR/AuC é a diferença do tempo de recepção da mensagem de requisição e o envio da mensagem de resposta com os *triplets* do terminal sendo autenticado. O atraso do servidor AAA é em referência ao tempo de tratamento da mensagem de resposta de autenticação do terminal e o envio de mensagem de autenticação bem sucedida. O tempo de atraso do terminal em conjunto com o AP da rede WLAN é o tempo gasto na seleção da versão do protocolo e envio do campo AT_NONCE.

Os valores de atraso obtidos são diferentes dos medidos nos elementos em operação na rede da Brasil Telecom GSM. O valor de atraso na rede SS7 utilizado no laboratório foi maior que o da rede comercial devido o elemento utilizado ser mais antigo e estar dimensionado para tratar o tráfego de mensagens da rede fixa STFC que são de tamanho menor que as mensagens do protocolo MAP utilizadas na autenticação de terminais. O atraso no HLR/AuC foi maior nas medidas em laboratório devido utilização de elemento de teste instalado em servidor compartilhado com outras operações. O atraso de do servidor AAA de laboratório foi muito menor que o medido em rede comercial devido ao elemento de laboratório estar funcionando sem tráfego e em servidor dedicado.

APÊNDICE D – MEDIDAS DE ATRASO EM SERVIDOR AAA EM AMBIENTE DE PRODUÇÃO

Neste Apêndice é descrita a metodologia de medição do tráfego IP adotada para o cálculo do tempo de processamento em servidores AAA implementando protocolo RADIUS [11] e são mostrados os resultados obtidos das análises realizadas.

Para a realização das medidas foram levantados os horários de maior movimento na rede objeto, com base em dados estatísticos disponibilizados pelo operador da rede. Para os dados de atraso do protocolo RADIUS foram feitas medidas do tráfego IP na *interface* de rede em um dos servidores de AAA em produção da rede da operadora de telefonia Brasil Telecom. Este servidor é responsável pela autenticação de todos os usuários do serviço de banda larga da operadora e implementa as funções de: RADIUS-*proxy* para outros servidores AAA no caso de autenticação de usuários com conta em domínios não geridos pela operadora; autenticação para usuários com conta em domínios geridos pela operadora; autorização, e; contabilização das conexões e desconexões realizadas. A autenticação de usuários com domínios da própria operadora é efetuada após a consulta a uma base de assinantes LDAP externa ao servidor. No horário de maior movimento o servidor AAA medido foi responsável por uma média de 460.000 requisições RADIUS por hora, conforme os dados capturados.

As mensagens AAA foram capturadas com a utilização do comando *tcpdump* diretamente no servidor de AAA, na *interface* de rede específica para as requisições AAA RADIUS. O servidor de AAA em observação é o produto NAVIS RADIUS do fabricante Alcatel-Lucent, utiliza sistema operacional Unix Solaris 9 em hardware do fabricante SUN Microsystems e possui *interfaces* de rede distintas para acesso remoto, gerência e acesso de requisições de AAA via protocolo RADIUS.

Os dados capturados foram filtrados de forma a separar os diferentes conjuntos de mensagens de requisições e respostas que o servidor é responsável, a saber:

a) Requisições RADIUS recebidas de, e respondidas para os acessos de usuários finais;

b) Requisições RADIUS enviadas para, e recebidas de outros servidores AAA;

c) Requisições LDAP enviadas para, e recebidas da base de dados LDAP.

As requisições RADIUS recebidas dos acessos de usuários finais foram também filtradas para separar o grupo de requisições que gerou consultas à base LDAP do conjunto de requisições que gerou requisições RADIUS a servidores AAA externos.

Os conjuntos de mensagens do protocolo RADIUS de requisições (*Access-Request*) e respostas (*Access-Accept* e *Access-Reject*) filtradas foram então casadas com base no endereço IP de origem e destino, no valor do *byte* do campo RADIUS de identificação de pacote (*identifier*) e no valor do atributo RADIUS *user-name*. A descrição dos campos e atributos do protocolo RADIUS pode ser encontrada em [11]. O conjunto de mensagens LDAP de requisição (*searchRequest*) e respostas (*searchResEntry* e *searchResDone*) foram casadas com base no valor dos três *bytes* do campo LDAP *messageId* e no valor do objeto LDAP *uid*, a descrição dos campos e objetos do protocolo LDAP podem ser encontrados em [35].

Com base nos conjuntos casados de requisição e reposta foram extraídos os valores de tempo de resposta e calculados os valores estatísticos da taxa de chegada e da taxa de processamento para o servidor AAA funcionando como *proxy* e como autenticador. A figura D.1 ilustra os dados que foram extraídos das capturas do protocolo RADIUS realizadas.

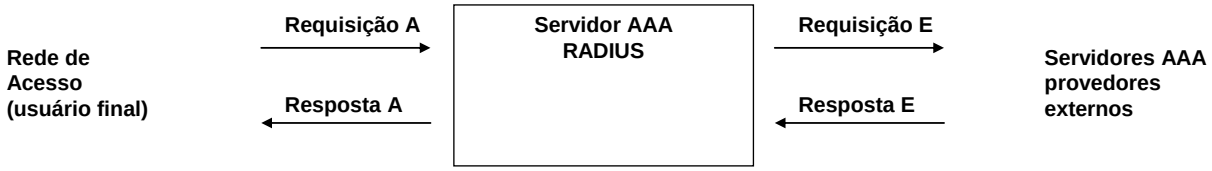


Figura D.1 – Relações de Requisição / Resposta RADIUS no servidor AAA medido

Como não foi possível realizar a correlação entre as Requisições A e as Requisições E, ilustradas na figura D.1, mas somente entre os pares Requisição A / Resposta A e Requisição E / Resposta E, teve de ser calculado os seguintes tempos de respostas:

$$\Delta t_A = t_{\mathrm{Re}\,spostaA} - t_{\mathrm{Re}\,quisiçãoA} \qquad \text{Eq. D.1}$$

$$\Delta t_E = t_{\mathrm{Re}\,spostaE} - t_{\mathrm{Re}\,quisiçãoE} \qquad \text{Eq. D.2}$$

Para os tempos calculados pelas equações D.1 e D.2 foram utilizados somente as requisições bem sucedidas, ou seja, as requisições de autenticação que retornaram resposta positiva (mensagem RADIUS *Access-Accept*). As requisições de autenticação rejeitadas (mensagem RADIUS *Access-Reject*) não foram contabilizadas devido ao servidor estar programado para inserir um atraso fixo de alguns segundos em caso de recusa da autenticação.

A diferença entre os tempos Δt_A e Δt_E é igual à soma do tempo de processamento do servidor AAA do sentido rede de acesso para os servidores AAA externos mais o tempo de processamento do servidor AAA do sentido dos servidores AAA externos para a rede de acesso. Considerando que os pacotes RADIUS considerados são pequenos, geralmente menores que 250 *bytes*, as *interfaces* de rede do servidor AAA são de alta velocidade (*Gigabit Ethernet*) e que o servidor está realizando a função de *proxy* descrita em [11], podemos considerar que os tempos de processamento são idênticos para os dois sentidos de tráfego. Sendo assim, o tempo de processamento do servidor AAA pode ser calculado como:

$$t_{AAA} = \frac{E(\Delta t_A) - E(\Delta t_E)}{2} \qquad \text{Eq. D.3}$$

Onde $E(\Delta t_A)$ e $E(\Delta t_E)$ são os valores das médias estatísticas das distribuições dos tempos Δt_A e Δt_E, calculadas com base nas amostras capturadas.

As taxas de chegada de pacotes (λ) em cada sentido foram calculadas pela contagem dos pacotes em cada amostra e em cada sentido de tráfego dividido pelo tempo da amostra. O valor final foi dado pela média das taxas de chegada em cada amostra.

Com base nos valores de tempo de processamento e de taxa de chegada é possível calcular a taxa de processamento do servidor AAA, considerando uma fila M/M/1 a taxa de processamento é dada por:

$$\mu = \frac{1 - \lambda \cdot t_{AAA}}{t_{AAA}} \qquad \text{Eq. D.4}$$

Para cada sentido de tráfego no servidor AAA foi calculado o valor referente de taxa de processamento. A figura D.2 ilustra as relações das taxas de chegadas (λ) e taxas de processamento (μ) obtidas após as analises descritas e as trocas de tráfego ilustradas na figura D.1.

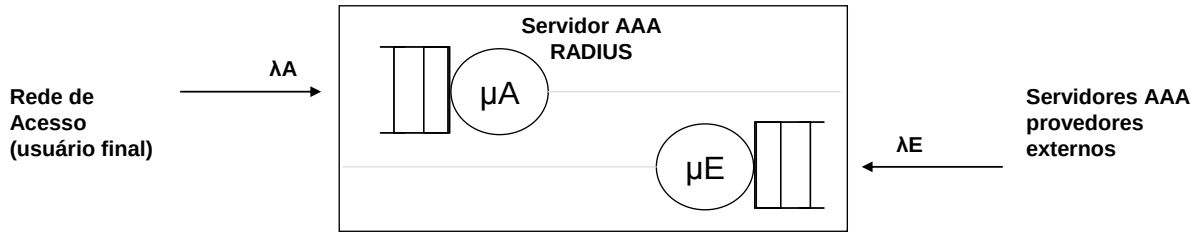


Figura D.2 – Taxas de chegadas e taxas de processamento obtidas no servidor AAA medido

As amostras de dados foram capturadas em oito medições realizadas em dias distintos, no horário de maior movimento de tráfego de autenticação (entre 18:00 e 19:00 horas). Cada medição possui no mínimo 50.000 pacotes de dados capturados na *interface* de rede específica para o tráfego de autenticação. Os dados capturados de cada amostra foram filtrados para separar os tráfegos de protocolos LDAP e RADIUS e exportados em formato texto, com o auxílio da aplicação *Wireshark*, disponível em http://www.wireshark.org. Os arquivos texto exportados foram filtrados com a utilização de aplicação específico desenvolvido em linguagem Java e importados em planilhas do aplicativo Microsoft Excel para cálculos dos parâmetros de interesse. As análises estatísticas realizadas na sequência de dados capturados foram baseadas nos métodos estatísticos descritos no capítulo 23 do *Quality Control Handbook* [37].

Com base na primeira amostra obtida, foi calculado do desvio padrão da amostra, e estimado o tamanho da amostra (*n*) necessário para obter a estimativa da média da população com 95% de nível de confiança. O erro máximo permitido foi arbitrado em 0,02s, o nível de significância (α) em 5% e o desvio padrão da população foi estimado [37]. O tamanho da amostra mínimo para o tráfego originado dos usuários finais foi estimado em 9000 pacotes e para o tráfego direcionado para os servidores AAA externo em 400 pacotes. A quantidade de dados coletados agregados acumulados foram superiores aos valores de *n* estimados.

A tabela D.1 sumariza os valores estatísticos calculados com base nos dados coletados.

Tabela D.1 – Resultado estatístico dos dados coletados

Parâmetros	**Tráfego da Rede Acesso** Δt_A	**Tráfego Servidores AAA externos** Δt_E
Média (*E*) [segundos]	0,265012	0,209465
Desvio Padrão (*s*) [segundos]	0,5412569	0,375744
Valor Mínimo [segundos]	0,004163	0,001320
Valor Máximo [segundos]	3,643283	3,076615
Tamanho amostra (*n*)	10.304	9.479
Taxa de chegada (λ) [pacotes/s]	124,27	43,89

Para o cálculo do tempo de processamento médio do servidor AAA (t_{AAA}) a diferença entre as distribuições estatísticas de Δt_A e Δt_E teve que ser calculada. Para este cálculo foi utilizado o método de estimativa do intervalo de confiança para a diferença entre duas distribuições, conforme descrito em [37], para obter o valor estatístico do limite superior de t_{AAA}, para nível de significância (α) de 5%. Desta forma, a equação D.3 foi alterada para:

$$t_{AAA} = \frac{E(\Delta t_A) - E(\Delta t_E) + t_{\alpha/2}\sqrt{\frac{s_A^2}{n_A} + \frac{s_E^2}{n_E}}}{2} \qquad \text{Eq. D.5}$$

Onde, $t_{\alpha/2}$ é a distribuição de Student para α/2 e o menor valor entre $(n_A\text{-}1)$ e $(n_E\text{-}1)$ como grau de liberdade, s_A e s_E são os desvios padrões das amostras e n_A e n_E são o tamanho das amostras.

Os valores médios finais calculados com base nos dados das amostras e nas equações descritas neste apêndice estão listados na tabela D.2.

Tabela D.2 – Valores médios finais para atraso, λ e μ

t_{AAA}	λ_A	λ_E	μ_A	μ_E
0,027876s	124,27 pacotes/s	43,89 pacotes/s	160,144 pacotes/s	79,761 pacotes/s

Os valores de λ e μ foram utilizados como dados de entrada para a modelagem analítica desenvolvida neste trabalho e estão refletidos nos parâmetros listados na tabela 6.2.

APÊNDICE E – MEDIDAS DE ATRASO NA REDE SS7 E HLR EM AMBIENTE DE PRODUÇÃO

Neste Apêndice é descrita a metodologia de medição adotada para o cálculo do tempo de processamento de mensagens de autenticação em elementos HLR/AuC e cálculo do atraso das mesmas na rede de sinalização SS7. Adicionalmente são mostrados os resultados obtidos das análises realizadas.

Para a realização das medidas foram levantados os horários de maior movimento na rede objeto, com base em dados estatísticos disponibilizados pelo operador da rede. Para os dados de atraso do HLR/AuC foram feitas medidas do tráfego do protocolo MAP na *interface* de sinalização SS7 em um dos elementos HLR/AuC em produção da rede da operadora Brasil Telecom GSM. Como o HLR/AuC realiza as funções e possui as bases de assinantes para autenticação, gerência de localização e de mobilidade, o universo de dados obtidos teve de ser filtrado para evidenciar somente as requisições de autenticação realizadas pelas mensagens MAP SAI (*Send Authentication Information*) de forma a permitir o cálculo específico do tempo de processamento de requisições de autenticação. O elemento HLR/AuC objeto das medidas trata no horário de maior movimento em média 27.000 requisições de autenticação por hora.

Para o atraso na rede SS7 foram realizadas medidas nos mesmos horários das do HLR/AuC. As medidas foram focadas nas *interfaces* de sinalização do elemento PTS responsável pela rede de sinalização da operadora de telefonia móvel Brasil Telecom GSM. Como as mensagens de autenticação possuem um tamanho maior que as mensagens de estabelecimento de chamadas, o universo de dados obtidos teve de ser filtrado para evidenciar somente as requisições de autenticação realizadas através de mensagens MAP SAI (*Send Authentication Information*) de forma a permitir o cálculo específico do tempo de atraso das mesmas na rede de sinalização.

Utilizando os dados estatísticos históricos fornecidos pela operadora Brasil Telecom GSM foi evidenciado que o horário entre 18:00 e 19:00 horas é o que apresenta o maior tráfego de requisições ao elemento HLR/AuC via a rede de sinalização SS7, independentemente do dia da semana. A figura E.1 mostra o gráfico diário de requisições médias ao HLR/Auc em uma semana.

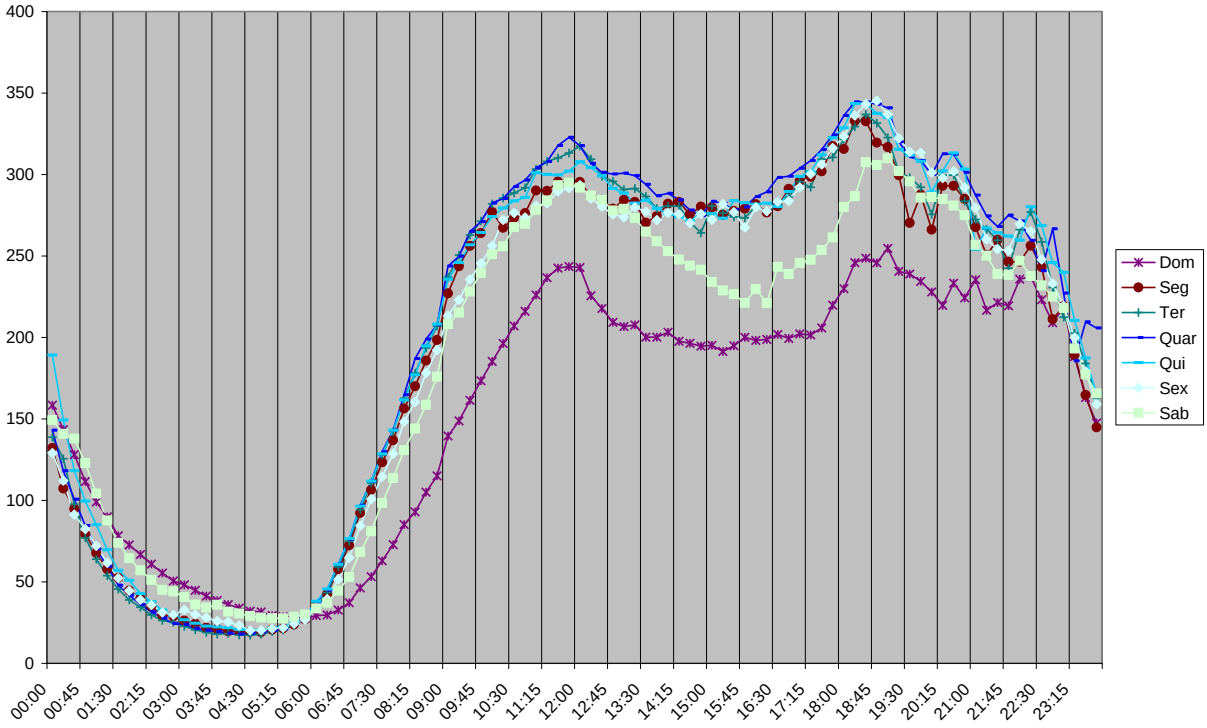


Figura E.1 – Gráfico do tráfego de sinalização do HLR/AuC

Com base no resultado acima, foi realizada coleta de dados de sinalização em dias distintos durante o período de maior movimento. Para as coletas foi utilizado o sistema de monitoração da rede de sinalização *AcceSS7* fornecido pelo fabricante *Agilent Technologies* (http://www.home.agilent.com) instalado na rede SS7 da operadora Brasil Telecom GSM. O sistema *AccceSS7* possui pontas de provas fisicamente instaladas em todos os enlaces de sinalização da operadora e para a realização de capturas de dados pode armazenar todas as mensagens de sinalização de enlaces selecionados. Para as medidas do HLR/AuC foram selecionados todos os enlaces de sinalização do elemento e para as medidas da rede SS7 foram selecionados para captura todos os enlaces de sinalização do elemento PTS primário que atende ao HLR/AuC da operadora.

Abaixo é listada a captura de uma mensagem MAP decodificada pela ferramenta *AcceSS7* de requisição de autenticação e uma de resposta da autenticação pelo HLR/AuC:

```
          |           | ITU.96.HS
1         | 1000|0011 | Service Indicator = SCCP, SSF = National Net
2         | 0010 0110 | DPC :     7974 dec,   1F26 hex
3         | 00|011111 |
```

```
 4       | 0000 1111 | OPC :     9276 dec,   243C hex
 5       | 0111|1001 | SLS :        7 dec,      7 hex
         |           | ITU.WHITE.SCCP
 6    F  | 0000 1001 | MT = Unitdata (UDT)
 7    F  | 1000 0001 | Protocol Class = class 1
 8    V  | 0000 0011 | Pointer to Called Party Address Parameter = 3
 9    V  | 0001 0000 | Pointer to Calling Party Address Parameter = 16
10    V  | 0001 1011 | Pointer to Data Parameter = 27
11    V  | 0000 1101 | LI of Called Party Add parameter = 13 octet(s)
12    V  | 0101 0010 |Addr Ind:Route=PC&SSN;GT=TT&NP&ES&NoA;PC=N;SSN=Y
13    V  | 0000 0110 |  Subsystem Number =   6  HLR Home Loc Register
14    V  | 0000 0000 |  Translation Type =   0  T Type Not Used
15    V  | 0111|0001 |  Numbering Plan & Encoding Scheme
16    V  | 0|0000100 |  Nature of Address Indicator
17    V  | 0101|0101 |  Address Signal
18    V  | 0001|0000 |  Address Signal
19    V  | 0000|0110 |  Address Signal
20    V  | 0000|0001 |  Address Signal
21    V  | 0100|0011 |  Address Signal
22    V  | 0010|0100 |  Address Signal
23    V  | 0010|0100 |  Address Signal
24    V  | 0000|0001 |  Address Signal
25    V  | 0000 1011 | LI of Calling Party Add parameter = 11 octet(s)
26    V  | 0001 0010 | Addr Ind:Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
27    V  | 0000 0111 |  Subsystem Number =   7  VLR Visited Loc Reg
28    V  | 0000 0000 |  Translation Type =   0  T Type Not Used
29    V  | 0001|0010 |  Numbering Plan & Encoding Scheme
30    V  | 0|0000100 |  Nature of Address Indicator
31    V  | 0101|0101 |  Address Signal
32    V  | 0001|0000 |  Address Signal
33    V  | 0000|0110 |  Address Signal
34    V  | 0000|0000 |  Address Signal
35    V  | 0001|0100 |  Address Signal
36    V  | 0000|0001 |  Address Signal
37    V  | 0100 0011 | LI of Data parameter = 67 octet(s)
         |           | 3GPP.MAP
38       | 0110 0010 | TCAP Message Type: Begin
39       | 0100 0001 |   Length: 65 octets
40       | 0100 1000 | Originating Trans Id Tag: 48
41       | 0000 0100 | Length: 4 octet(s)
42       | 1000 0000 |   Originating Transaction Id: 800003c2
43       | 0000 0000 |   Originating Transaction Id:
44       | 0000 0011 |   Originating Transaction Id:
45       | 1100 0010 |   Originating Transaction Id:
46       | 0110 1011 | Dialogue Portion Tag: 6b
47       | 0001 1110 |   Length: 30 octets
48       | 0010 1000 | External Tag: 28
49       | 0001 1100 |   Length: 28 octets
50       | 0000 0110 | Object Identifier Tag: 6
51       | 0000 0111 |   Length: 7 octet(s)
52       | 0000 0000 |   ccitt recommendation: 0
53       | 0001 0001 |   q: 11
54       | 1000 0110 |   773: 86
55       | 0000 0101 |   Space character: 5
56       | 0000 0001 |   as(1): 1
57       | 0000 0001 |   dialoguePDU: 1
58       | 0000 0001 |   version1(1): 1
59       | ---0 0000 | Single ASN.1 Type Tag:
         | 10-- ---- | Single ASN.1 Type Tag: 40
60       | 0001 0001 |   Length: 17 octets
61       | 0110 0000 | Dialogue PDU: Dialogue Request
```

```
 62       | 0000 1111 |   Length: 15 octets
 63       | 1000 0000 | Protocol Version Tag: 80
 64       | 0000 0010 |   Length: 2 octet(s)
 65       | 0000 0111 |   Protocol Version: 780
 66       | 1000 0000 |   Protocol Version:
 67       | 1010 0001 | Application Context Name Tag: a1
 68       | 0000 1001 |   Length: 9 octets
 69       | 0000 0110 | Object Identifier Tag: 6
 70       | 0000 0111 |   Length: 7 octet(s)
 71       | 0000 0100 |   ccitt recommendation: 4
 72       | 0000 0000 |   etsi: 0
 73       | 0000 0000 |   mobile domain: 0
 74       | 0000 0001 |   gsm Network: 1
 75       | 0000 0000 |   ac_id: 0
 76       | 0000 1110 |   dialoguePDU: InfoRetrieval
 77       | 0000 0011 |   version: 3
 78       | 0110 1100 | Component Portion Tag: 6c
 79       | 1000 0000 |   Length: Indefinite
 80       | 1010 0001 | Invoke: a1
 81       | 0001 0101 |   Length: 21 octets
 82       | 0000 0010 | Invoke Id Tag: 2
 83       | 0000 0001 |   Length: 1 octet(s)
 84       | 0000 0001 |   Invoke Id: 1
 85       | 0000 0010 | Operation Code Tag: Local Operation Code
 86       | 0000 0001 |   Length: 1 octet(s)
 87       | 0011 1000 | Operation Code (Invoke): Send Authent. Info
 88       | 0011 0000 | Sequence Tag: 30
 89       | 0000 1101 |   Length: 13 octets
 90       | 1000 0000 | IMSI Tag: 80
 91       | 0000 1000 |   Length: 8 octet(s)
 92       | 0010 0111 |   IMSI Digits: 724160103442421
 93       | 0001 0100 |   IMSI Digits:
 94       | 0000 0110 |   IMSI Digits:
 95       | 0000 0001 |   IMSI Digits:
 96       | 0100 0011 |   IMSI Digits:
 97       | 0010 0100 |   IMSI Digits:
 98       | 0010 0100 |   IMSI Digits:
 99       | ---- 0001 |   IMSI Digits:
          | 1111 ---- |   Filler: f
100       | 0000 0010 | Number Of Requested Vectors Tag: 2
101       | 0000 0001 |   Length: 1 octet(s)
102       | 0000 0101 |   Number Of Requested Vectors: 5
103       | 0000 0000 |   End of contents: 0
104       | 0000 0000 |   End of contents:
105    M  | 0000|1000 | PDU Type = SD
106    M  | 0101 1010 | N(S)
107    M  | 0111 1000 | N(S)
108    M  | 1101 1011 | N(S)


          |           | ITU.96.HS
 1        | 1000|0011 | Service Indicator = SCCP, SSF = National Net
 2        | 1111 1000 | DPC :    11000 dec,   2AF8 hex
 3        | 10|101010 |
 4        | 1100 1001 | OPC :     7974 dec,   1F26 hex
 5        | 0000|0111 | SLS :        0 dec,      0 hex
          |           | ITU.WHITE.SCCP
 6    F   | 0000 1001 | MT = Unitdata (UDT)
 7    F   | 1000 0000 | Protocol Class = class 0
 8    V   | 0000 0011 | Pointer to Called Party Address Parameter = 3
 9    V   | 0000 1110 | Pointer to Calling Party Address Parameter = 14
```

```
10    V  | 0001 1001 | Pointer to Data Parameter = 25
11    V  | 0000 1011 | LI of Called Party Add parameter = 11 octet(s)
12    V  | 0101 0010 |Addr Ind:Route=PC&SSN;GT=TT&NP&ES&NoA;PC=N;SSN=Y
13    V  | 0000 0111 |  Subsystem Number =   7  VLR Visited Loc Reg
14    V  | 0000 0000 |  Translation Type =   0  T Type Not Used
15    V  | 0001|0010 |  Numbering Plan & Encoding Scheme
16    V  | 0|0000100 |  Nature of Address Indicator
17    V  | 0101|0101 |  Address Signal
18    V  | 0001|0000 |  Address Signal
19    V  | 0000|0110 |  Address Signal
20    V  | 0000|0000 |  Address Signal
21    V  | 0001|0100 |  Address Signal
22    V  | 0000|0001 |  Address Signal
23    V  | 0000 1011 | LI of Calling Party Add parameter = 11 octet(s)
24    V  | 0001 0010 | Addr Ind:Route=GT; GT=TT&NP&ES&NoA; PC=N; SSN=Y
25    V  | 0000 0110 |  Subsystem Number =   6  HLR Home Loc Register
26    V  | 0000 0000 |  Translation Type =   0  T Type Not Used
27    V  | 0001|0010 |  Numbering Plan & Encoding Scheme
28    V  | 0|0000100 |  Nature of Address Indicator
29    V  | 0101|0101 |  Address Signal
30    V  | 0001|0000 |  Address Signal
31    V  | 0000|0110 |  Address Signal
32    V  | 0000|0000 |  Address Signal
33    V  | 0001|0110 |  Address Signal
34    V  | 0000|0000 |  Address Signal
35    V  | 1011 0111 | LI of Data parameter = 183 octet(s)
         |           | 3GPP.MAP
36       | 0110 0100 | TCAP Message Type: End
37       | 1000 0001 |   Length: 180 octets
38       | 1011 0100 |   Length:
39       | 0100 1001 | Destination Trans Id Tag: 49
40       | 0000 0100 | Length: 4 octet(s)
41       | 1000 0000 |   Destination Transaction Id: 800003c2
42       | 0000 0000 |   Destination Transaction Id:
43       | 0000 0011 |   Destination Transaction Id:
44       | 1100 0010 |   Destination Transaction Id:
45       | 0110 1011 | Dialogue Portion Tag: 6b
46       | 0010 1010 |   Length: 42 octets
47       | 0010 1000 | External Tag: 28
48       | 0010 1000 |   Length: 40 octets
49       | 0000 0110 | Object Identifier Tag: 6
50       | 0000 0111 |   Length: 7 octet(s)
51       | 0000 0000 |   ccitt recommendation: 0
52       | 0001 0001 |   q: 11
53       | 1000 0110 |   773: 86
54       | 0000 0101 |   Space character: 5
55       | 0000 0001 |   as(1): 1
56       | 0000 0001 |   dialoguePDU: 1
57       | 0000 0001 |   version1(1): 1
58       | ---0 0000 | Single ASN.1 Type Tag:
         | 10-- ---- | Single ASN.1 Type Tag: 40
59       | 0001 1101 |   Length: 29 octets
60       | 0110 0001 | Dialogue PDU: Dialogue Response
61       | 0001 1011 |   Length: 27 octets
62       | 1000 0000 | Protocol Version Tag: 80
63       | 0000 0010 |   Length: 2 octet(s)
64       | 0000 0111 |   Protocol Version: 780
65       | 1000 0000 |   Protocol Version:
66       | 1010 0001 | Application Context Name Tag: a1
67       | 0000 1001 |   Length: 9 octets
68       | 0000 0110 | Object Identifier Tag: 6
```

```
 69       | 0000 0111 |   Length: 7 octet(s)
 70       | 0000 0100 |   ccitt recommendation: 4
 71       | 0000 0000 |   etsi: 0
 72       | 0000 0000 |   mobile domain: 0
 73       | 0000 0001 |   gsm Network: 1
 74       | 0000 0000 |   ac_id: 0
 75       | 0000 1110 |   dialoguePDU: InfoRetrieval
 76       | 0000 0011 |   version: 3
 77       | 1010 0010 | Result Tag: a2
 78       | 0000 0011 |   Length: 3 octets
 79       | 0000 0010 | Integer Tag: 2
 80       | 0000 0001 |   Length: 1 octet(s)
 81       | 0000 0000 |   Result: Accepted
 82       | 1010 0011 | Result Source Diagnostic Tag: a3
 83       | 0000 0101 |   Length: 5 octets
 84       | 1010 0001 | Service User Tag: a1
 85       | 0000 0011 |   Length: 3 octets
 86       | 0000 0010 |   Integer Tag: 2
 87       | 0000 0001 |   Length: 1 octet(s)
 88       | 0000 0000 |   Service User Value: Null
 89       | 0110 1100 | Component Portion Tag: 6c
 90       | 1000 0000 |   Length: Indefinite
 91       | 1010 0010 | Return Result (Last): a2
 92       | 0111 1100 |   Length: 124 octets
 93       | 0000 0010 | Invoke Id Tag: 2
 94       | 0000 0001 |   Length: 1 octet(s)
 95       | 0000 0001 |   Invoke Id: 1
 96       | 0011 0000 | Sequence Tag: 30
 97       | 0111 0111 |   Length: 119 octets
 98       | 0000 0010 | Operation Code Tag: Local Operation Code
 99       | 0000 0001 |   Length: 1 octet(s)
100       | 0011 1000 | Operation Code (Return Res): Send Authent. Info
101       | 1010 0011 | Sequence Tag: a3
102       | 1000 0000 |   Length: Indefinite
103       | 1010 0000 | Triplet List Tag: a0
104       | 1000 0000 |   Length: Indefinite
105       | 0011 0000 | Authentication Triplet Tag: 30
106       | 0010 0010 |   Length: 34 octets
107       | 0000 0100 | RAND Tag: 4
108       | 0001 0000 | Length: 16 octet(s)
109       | 1101 1011 |   RAND 1: dbb4105b279ff09abe9430e831abcfff
110       | 1011 0100 |   RAND 1:
111       | 0001 0000 |   RAND 1:
112       | 0101 1011 |   RAND 1:
113       | 0010 0111 |   RAND 1:
114       | 1001 1111 |   RAND 1:
115       | 1111 0000 |   RAND 1:
116       | 1001 1010 |   RAND 1:
117       | 1011 1110 |   RAND 1:
118       | 1001 0100 |   RAND 1:
119       | 0011 0000 |   RAND 1:
120       | 1110 1000 |   RAND 1:
121       | 0011 0001 |   RAND 1:
122       | 1010 1011 |   RAND 1:
123       | 1100 1111 |   RAND 1:
124       | 1111 1111 |   RAND 1:
125       | 0000 0100 | SRES Tag: 4
126       | 0000 0100 | Length: 4 octet(s)
127       | 1010 0000 |   SRES 1: a004aa2e
128       | 0000 0100 |   SRES 1:
129       | 1010 1010 |   SRES 1:
```

```
130       | 0010 1110 |   SRES 1:
131       | 0000 0100 | KC Tag: 4
132       | 0000 1000 | Length: 8 octet(s)
133       | 0011 1101 |   KC 1: 3da04abf70084800
134       | 1010 0000 |   KC 1:
135       | 0100 1010 |   KC 1:
136       | 1011 1111 |   KC 1:
137       | 0111 0000 |   KC 1:
138       | 0000 1000 |   KC 1:
139       | 0100 1000 |   KC 1:
140       | 0000 0000 |   KC 1:
141       | 0011 0000 | Authentication Triplet Tag: 30
142       | 0010 0010 |   Length: 34 octets
143       | 0000 0100 | RAND Tag: 4
144       | 0001 0000 | Length: 16 octet(s)
145       | 1000 1010 |   RAND 2: 8ae26d782918bedb81930061e470ad9d
146       | 1110 0010 |   RAND 2:
147       | 0110 1101 |   RAND 2:
148       | 0111 1000 |   RAND 2:
149       | 0010 1001 |   RAND 2:
150       | 0001 1000 |   RAND 2:
151       | 1011 1110 |   RAND 2:
152       | 1101 1011 |   RAND 2:
153       | 1000 0001 |   RAND 2:
154       | 1001 0011 |   RAND 2:
155       | 0000 0000 |   RAND 2:
156       | 0110 0001 |   RAND 2:
157       | 1110 0100 |   RAND 2:
158       | 0111 0000 |   RAND 2:
159       | 1010 1101 |   RAND 2:
160       | 1001 1101 |   RAND 2:
161       | 0000 0100 | SRES Tag: 4
162       | 0000 0100 | Length: 4 octet(s)
163       | 0110 0000 |   SRES 2: 60047951
164       | 0000 0100 |   SRES 2:
165       | 0111 1001 |   SRES 2:
166       | 0101 0001 |   SRES 2:
167       | 0000 0100 | KC Tag: 4
168       | 0000 1000 | Length: 8 octet(s)
169       | 1100 1001 |   KC 2: c9656a0db4e3f000
170       | 0110 0101 |   KC 2:
171       | 0110 1010 |   KC 2:
172       | 0000 1101 |   KC 2:
173       | 1011 0100 |   KC 2:
174       | 1110 0011 |   KC 2:
175       | 1111 0000 |   KC 2:
176       | 0000 0000 |   KC 2:
177       | 0011 0000 | Authentication Triplet Tag: 30
178       | 0010 0010 |   Length: 34 octets
179       | 0000 0100 | RAND Tag: 4
180       | 0001 0000 | Length: 16 octet(s)
181       | 0110 0110 |   RAND 3: 66c7af626a2cc7a94b93fe7d2774af3c
182       | 1100 0111 |   RAND 3:
183       | 1010 1111 |   RAND 3:
184       | 0110 0010 |   RAND 3:
185       | 0110 1010 |   RAND 3:
186       | 0010 1100 |   RAND 3:
187       | 1100 0111 |   RAND 3:
188       | 1010 1001 |   RAND 3:
189       | 0100 1011 |   RAND 3:
190       | 1001 0011 |   RAND 3:
```

```
191       | 1111 1110 |   RAND 3:
192       | 0111 1101 |   RAND 3:
193       | 0010 0111 |   RAND 3:
194       | 0111 0100 |   RAND 3:
195       | 1010 1111 |   RAND 3:
196       | 0011 1100 |   RAND 3:
197       | 0000 0100 | SRES Tag: 4
198       | 0000 0100 | Length: 4 octet(s)
199       | 0101 1111 |   SRES 3: 5fe684b8
200       | 1110 0110 |   SRES 3:
201       | 1000 0100 |   SRES 3:
202       | 1011 1000 |   SRES 3:
203       | 0000 0100 | KC Tag: 4
204       | 0000 1000 | Length: 8 octet(s)
205       | 1101 0011 |   KC 3: d3769b5d37f4d800
206       | 0111 0110 |   KC 3:
207       | 1001 1011 |   KC 3:
208       | 0101 1101 |   KC 3:
209       | 0011 0111 |   KC 3:
210       | 1111 0100 |   KC 3:
211       | 1101 1000 |   KC 3:
212       | 0000 0000 |   KC 3:
213       | 0000 0000 |   End of contents: 0
214       | 0000 0000 |   End of contents:
215       | 0000 0000 |   End of contents: 0
216       | 0000 0000 |   End of contents:
217       | 0000 0000 |   End of contents: 0
218       | 0000 0000 |   End of contents:
219    M  | 0011 0000 | Padding octet
220    M  | 0001 0100 | Padding octet
221    M  | 1000|1000 | PDU Type = SD
222    M  | 0111 0110 | N(S)
223    M  | 1110 0001 | N(S)
224    M  | 0011 1110 | N(S)
```

Todas as mensagens MAP de requisição e resposta de autenticação (*Send Authentication Information*) foram filtradas e extraídas dos dados capturados da sinalização. Para avaliação do tempo de processamento, as mensagens de requisição e resposta foram separadas pelos códigos de 4 octetos de transação de origem (*Originating Transaction Id*) e de destino (*Destination Transaction Id*), para identificar um conjunto requisição e resposta o código de transação de destino da mensagem de resposta deve ser idêntico ao código de transação de origem da mensagem de requisição.

De posse das mensagens de requisição e de suas respectivas respostas é possível descobrir o tempo de processamento do HLR/Auc pela subtração das informações de data e hora (*timestamp*) das mesmas.

Para a avaliação do atraso da rede SS7 foram separadas as mesmas mensagens de sinalização capturadas nos enlaces de entrada e de saída da rede. Com base nestes dados

foram extraídas as mensagens MAP de requisição e de resposta de autenticação (*Send Authentication Information*) e comparados os valores de data e hora do enlace de entrada contra os valores de data e hora dos enlaces de saída. O atraso foi calculado somente sobre as mensagens de autenticação devido ao fato delas serem o foco do estudo e terem comprimento maior que as mensagens com maior volume de tráfego, tais como as de sinalização de chamadas. As mensagens de resposta da autenticação podem ter até 224 octetos de dados, dependendo da quantidade de vetores de autenticação requisitados ao HLR/AuC, como comparação, as mensagens de sinalização para estabelecimento de chamadas têm em torno de 38 octetos quando não transportam campos de informação adicional.

Foram coletados dados em nove dias distintos, no horário de maior movimento para o tráfego de sinalização. A quantidade de dados coletadas por em cada rodada foram limitadas somente pela capacidade do *buffer* de dados disponível pela ferramenta de monitoração da rede de sinalização. Os dados coletados foram exportados em formato texto e importados no aplicativo Microsoft Excel para o cálculo dos dados de interesse. As análises estatísticas realizadas na sequência foram baseadas nos métodos estatísticos descritos no capítulo 23 do *Quality Control Handbook* [37].

Com base na primeira amostra obtida, foi calculado o desvio padrão da amostra, e estimado o tamanho da amostra (*n*) necessário para obter a estimativa da média da população com 95% de nível de confiança. O erro máximo permitido foi arbitrado em 0,005s e o nível de significância (α) em 5%. Como o desvio padrão da população não é conhecido, o valor estimado do tamanho da amostra foi estimado com base no Gráfico S da página AII.33 de [37]. O valor de *n* para o tempo de processamento do HLR/AuC foi estimado em 45 e para o atraso da rede SS7 foi estimado em 90. A quantidade de dados coletados agregados acumulados foi superior ao valor de *n* estimado. A tabela E.1 sumariza os dados coletados.

Tabela E.1 – Resultado estatístico dos dados coletados

Parâmetros	**Tempo de Processamento HLR/AuC**	**Atraso rede SS7**	
		Envio SAI	**Resposta SAI**
Média (*E*)	0,035589s	0,019555s	0,021612s
Desvio Padrão (*s*)	0,015887s	0,010432s	0,012938s
Valor Mínimo	0,005s	0,006s	0,005s
Valor Máximo	0,069s	0,073s	0,089s
Tamanho amostra (*n*)	360	128	80

Com os valores de atraso das amostras calculados foi desenhado o gráfico de histograma para o tempo de processamento do HLR/AuC, conforme mostrado na figura E.2, e o gráfico de histograma para o tempo de atraso da rede SS7, conforme mostrado nas figuras E.3 e E.4. Com base na média (*E*) e no desvio padrão (*s*) das amostras foram calculados os valores de frequência teóricos para cada bloco de dados no histograma, considerando uma distribuição normal. Aos conjuntos de frequência teóricos e reais foi aplicado o teste estatístico de χ^2, definido em [37], para verificar as hipóteses de que as distribuições obtidas seguem uma distribuição normal, ou seja, H0:tempo atraso SS7 é normal e H0:tempo processamento HLR é normal. Estes testes requerem um número mínimo de 30 amostras, o que foi largamente superado. Os resultados dos testes demonstraram que as distribuições obtidas não podem ser consideradas normais, conforme as tabelas E.2, E.3 e E.4.

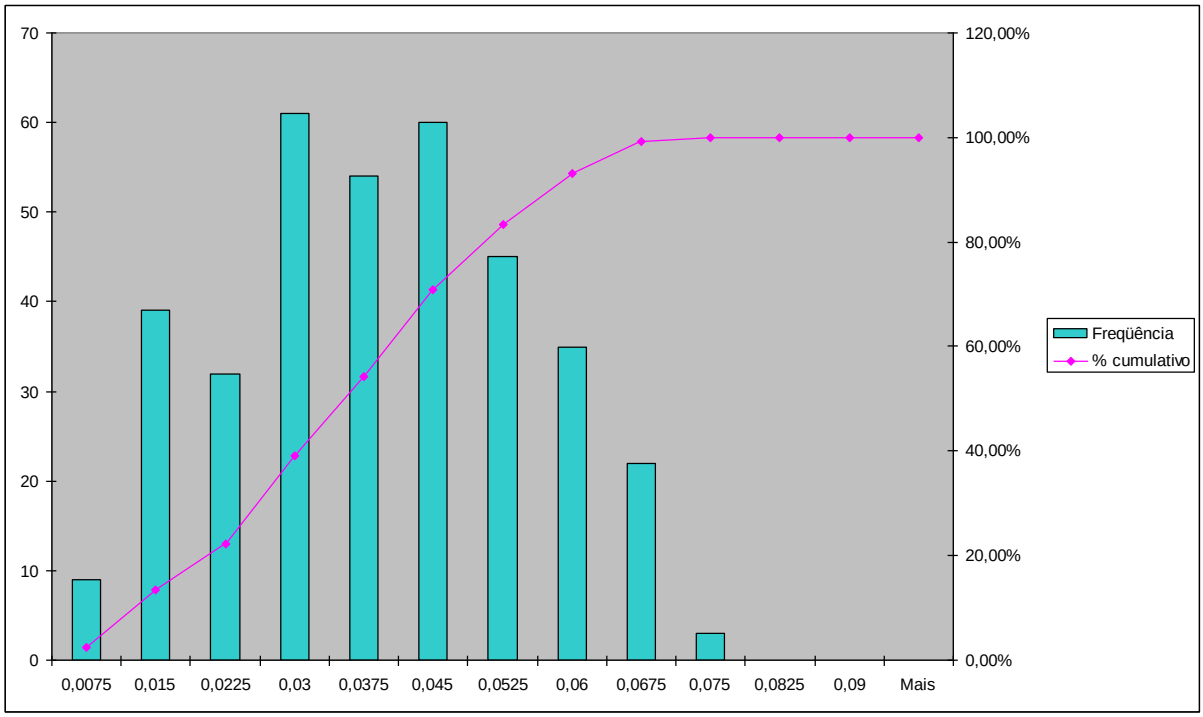


Figura E.2 – Histograma do tempo de processamento do HLR/AuC

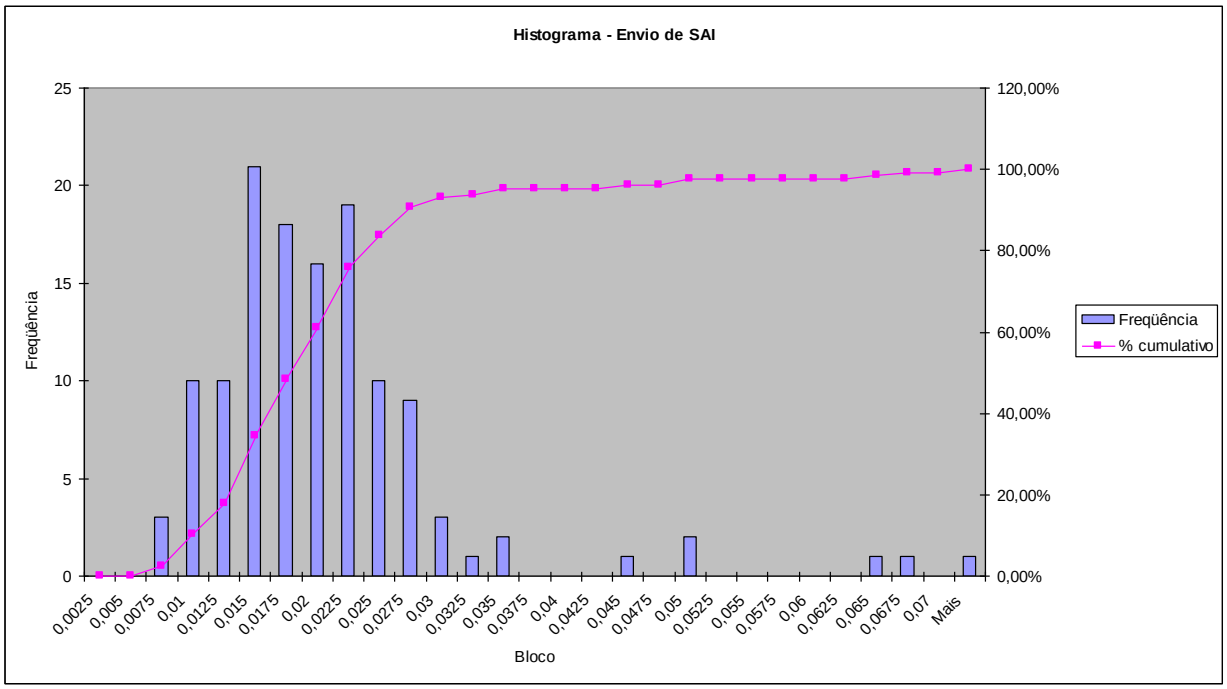


Figura E.3 – Histograma do atraso da rede SS7 – mensagens de envio de autenticação

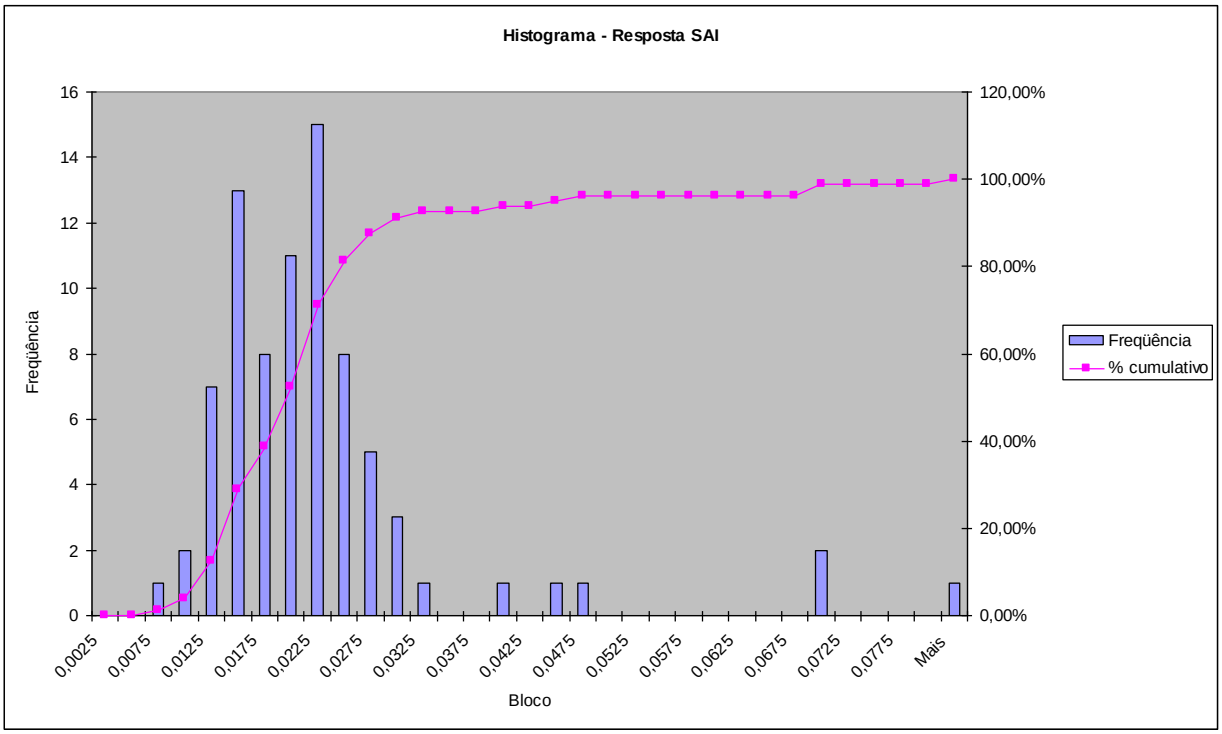


Figura E.4 – Histograma do atraso da rede SS7 – mensagens de retorno de autenticação

Tabela E.2 – Teste de χ^2 do tempo de processamento do HLR/AuC, conforme [37]

Bloco	Frequência real (*fr*)	Frequência teórica (*ft*)	$(fr - ft)^2/ft$
0,0075	9	13,87	1,70920
0,0150	39	21,23	14,87866
0,0225	32	38,70	1,16113
0,0300	61	56,70	0,32643
0,0375	54	66,74	2,43087
0,0450	60	63,12	0,15408
0,0525	45	47,97	0,18344
0,0600	35	29,29	1,11386
0,0675	22	14,37	4,05326
0,0750	3	5,66	1,25240
0,0825	0	1,79	1,79312
0,0900	0	0,46	0,45605
		Soma (χ^2_r):	29,5125
Grau de liberdade:		9	
χ^2 (tabulado):		16,91897762	
Região de aceitação: χ^2 (tabulado) > χ^2_r		Conclusão: **Hipótese rejeitada (Distribuição não normal)**	

Tabela E.3 – Teste de χ^2 do atraso da rede SS7 – envio de SAI, conforme [37]

Bloco	Frequência real (*fr*)	Frequência teórica (*ft*)	$(fr - ft)^2/ft$
0,0025	0	6,48	6,48270
0,0050	0	3,87	3,86566
0,0075	3	5,39	1,06100
0,0100	10	7,10	1,18189
0,0125	10	8,84	0,15316
0,0150	21	10,38	10,85574
0,0175	18	11,52	3,64120
0,0200	16	12,08	1,27446
0,0225	19	11,95	4,15236
0,0250	10	11,18	0,12375
0,0275	9	9,87	0,07633
0,0300	3	8,23	3,32253
0,0325	1	6,48	4,63510
0,0350	2	4,82	1,65035
0,0375	0	3,39	3,38646
0,0400	0	2,25	2,24683
0,0425	0	1,41	1,40790
0,0450	1	0,83	0,03339
0,0475	0	0,47	0,46570
0,0500	2	0,25	12,51704
0,0525	0	0,12	0,12256
0,0550	0	0,06	0,05771
0,0575	0	0,03	0,02566
0,0600	0	0,01	0,01078
0,0625	0	0,00	0,00427
0,0650	1	0,00	622,44611
0,0675	1	0,00	1762,99064
0,0700	0	0,00	0,00019
		Soma (χ^2_r):	2400,082
	Grau de liberdade:	25	
	χ^2 (tabulado):	37,65248413	
Região de aceitação: χ^2 (tabulado) > χ^2_r		Conclusão: **Hipótese rejeitada (Distribuição não normal)**	

Tabela E.4 – Teste de χ^2 do atraso da rede SS7 – resposta de SAI, conforme [37]

Bloco	Frequência real (*fr*)	Frequência teórica (*ft*)	$(fr - ft)^2/ft$
0,0025	0	5,52	5,51528
0,0050	0	2,35	2,35140
0,0075	1	3,01	1,34327
0,0100	2	3,72	0,79185
0,0125	7	4,42	1,51151
0,0150	13	5,06	12,47038
0,0175	8	5,58	1,04820
0,0200	11	5,93	4,32581
0,0225	15	6,08	13,09766
0,0250	8	6,00	0,66819
0,0275	5	5,70	0,08667
0,0300	3	5,22	0,94713
0,0325	1	4,61	2,82805
0,0350	0	3,92	3,92120
0,0375	0	3,21	3,21263
0,0400	1	2,54	0,93027
0,0425	0	1,93	1,92865
0,0450	1	1,41	0,12082
0,0475	1	1,00	0,00001
0,0500	0	0,68	0,67860
0,0525	0	0,44	0,44470
0,0550	0	0,28	0,28078
0,0575	0	0,17	0,17080
0,0600	0	0,10	0,10011
0,0625	0	0,06	0,05653
0,0650	0	0,03	0,03075
0,0675	0	0,02	0,01612
0,0700	2	0,01	487,35747
0,0725	0	0,00	0,00396
0,0750	0	0,00	0,00186
0,0775	0	0,00	0,00084
0,0800	0	0,00	0,00036
		Soma (χ^2_r):	546,242
	Grau de liberdade:	29	
	χ^2 (tabulado):	42,55696777	
Região de aceitação: χ^2 (tabulado) > χ^2_r		Conclusão: **Hipótese rejeitada (Distribuição não normal)**	

Considerando que as distribuições obtidas não podem ser consideradas normais, para a continuidade da análise foi utilizada a distribuição de probabilidade de Weibull. A

distribuição de Weibull é um grupo de muitas distribuições contínuas com cada distribuição definida unicamente pelos valores numéricos da função de probabilidade de Weibull [37]. Para obter as informações de probabilidade da população em análise, os dados amostrais são classificados em ordem crescente de valores, numerados em sequência (*i*), e tabulados com o respectivo *median rank*, dado pela expressão $(i - 0,3)/(n + 0,4)$ [37]. Os dados são plotados em gráfico específico e caso os mesmos se apresentem em uma linha reta é assumido que a distribuição de Weibull se aplica [37]. A reta obtida reflete as probabilidades da população em análise. Para os dados avaliados neste trabalho não foi utilizado o método gráfico descrito em [37], mas o aplicativo Microsoft Excel e o método descrito em [38] para a estimativa das probabilidades do tempo de processamento do HLR/AuC e do atraso da rede SS7.

Para ambas variáveis em estudo a regressão linear para os dados plotados seguindo o método descrito acima foi significativa, com a análise de variância (ANOVA) fornecendo valores calculados de *F* maiores que o dado pela tabela da distribuição de *F* [37], indicando que as probabilidades obtidas pela distribuição de Weibull se aplicam. Na tabela E.5 são listados os valores obtidos para probabilidade acumulada para o tempo de processamento do HLR/AuC e nas tabelas E.6 e E.7 são listados as probabilidades acumuladas para o atraso da rede SS7.

Tabela E.5 – Probabilidades cumulativas do tempo de processamento do HLR/AuC

Probabilidade Tempo de Processamento	**Tempo (segundos)**
0,10	0,014672
0,25	0,023055
0,50	0,034247
0,75	0,046781
0,90	0,058780
0,95	0,066169
0,99	0,080293

Tabela E.6 – Probabilidades cumulativas do atraso da rede SS7 – Envio de SAI

Probabilidade Atraso SS7	Tempo (segundos)
0,10	0,009525
0,25	0,013778
0,50	0,019035
0,75	0,024558
0,90	0,029593
0,95	0,032598
0,99	0,038179

Tabela E.7 – Probabilidades cumulativas do atraso da rede SS7 – Resposta de SAI

Probabilidade Atraso SS7	Tempo (segundos)
0,10	0,009977
0,25	0,014792
0,50	0,020882
0,75	0,027403
0,90	0,033435
0,95	0,037069
0,99	0,043876

Para a análise realizada neste documento foram utilizados valores que representam, com 95% de probabilidade, os tempos de processamento de HLR/AuC (Δ_{HLR}) e de atraso da rede SS7 (Δ_{SS7}).

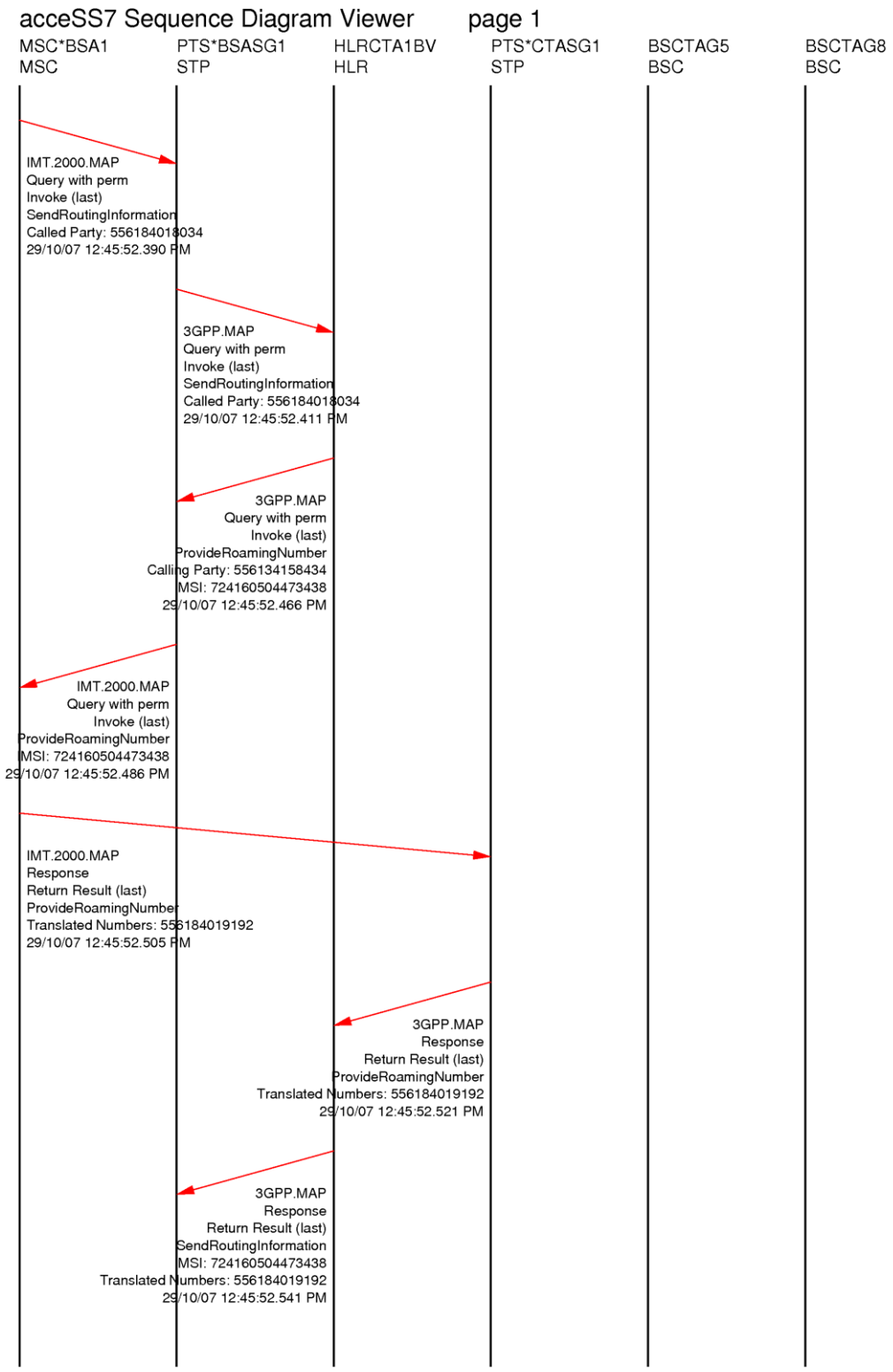
APÊNDICE F – MEDIDAS DE HANDOVER HORIZONTAL

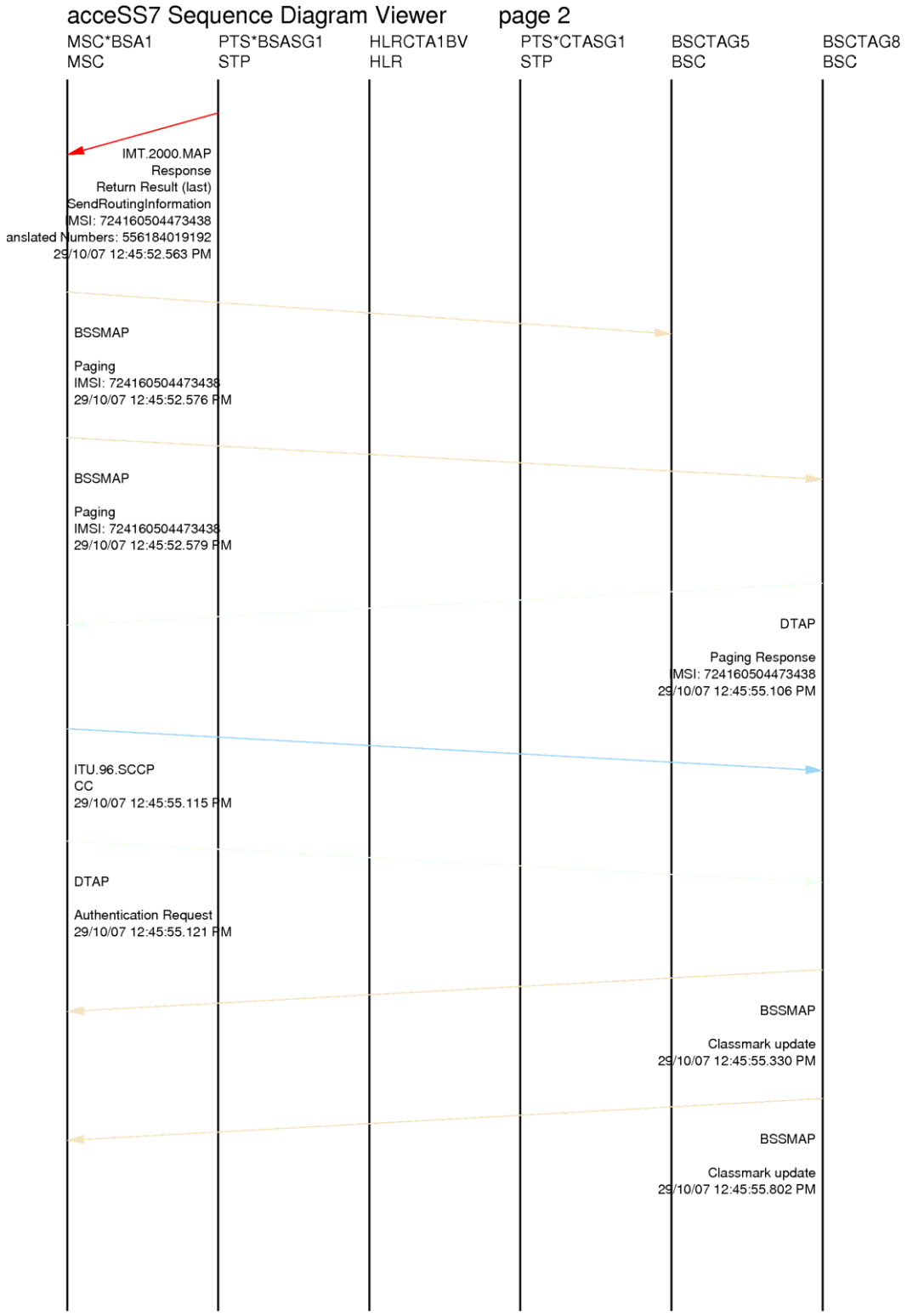
Neste Apêndice são listados os traçados de sinalização obtidos de chamadas com *handover* horizontal em rede comercial WWAN implementando tecnologia GSM. O objetivo destes traçados é tentar extrair a informação do tempo gasto na autenticação e no *handover* em redes GSM, como uma forma de comparação com o cenário de *handover* vertical avaliado no trabalho presente.

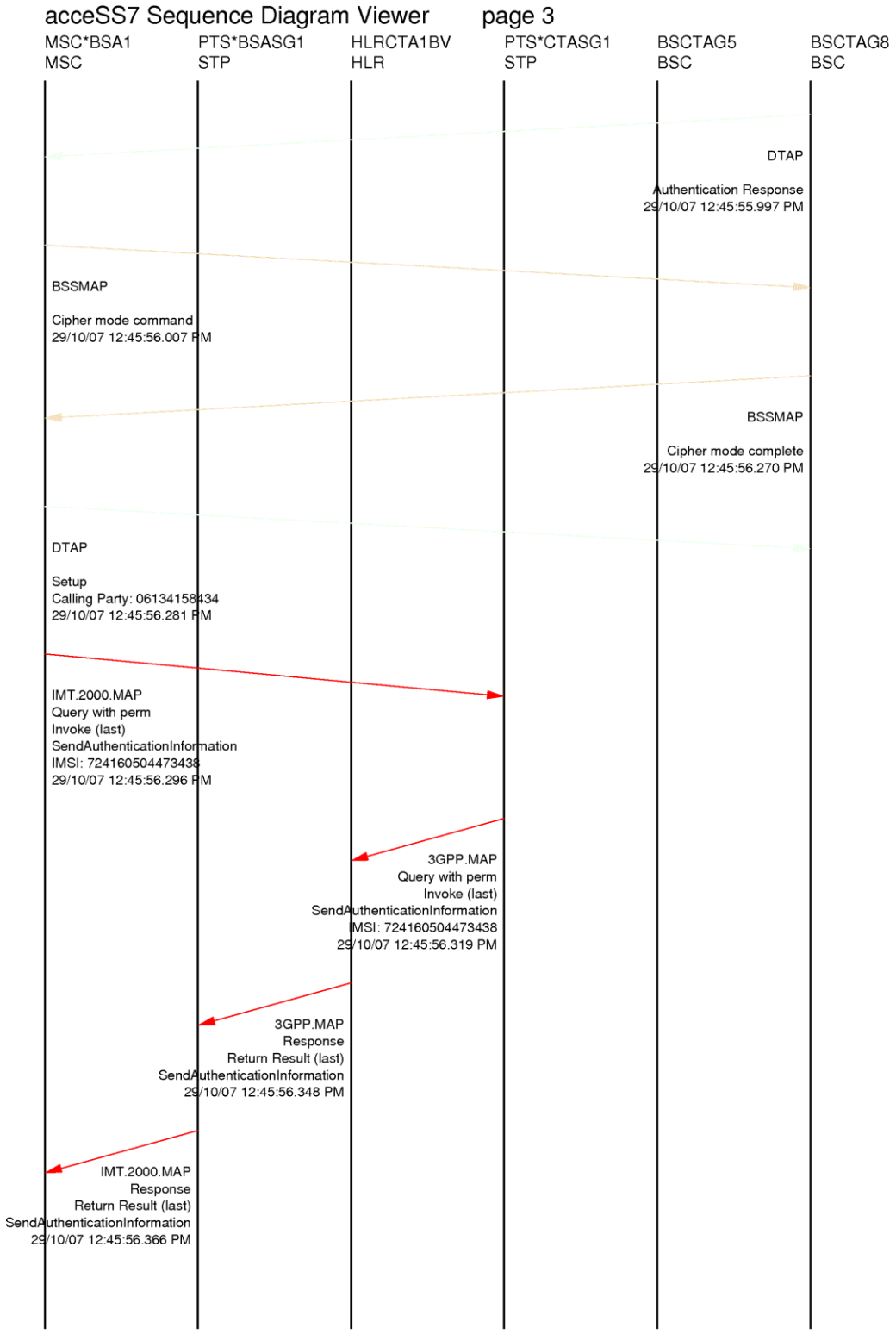
As mensagens de sinalização foram capturadas com a utilização da ferramenta *AcceSS7* referenciada no Apêndice B. Foram monitorados e capturados os enlaces de sinalização entre os elementos BSC e MSC (*interface A*) e entre os elementos MSC/VLR e HLR/AuC (*interface D*). A sinalização nas *interfaces* entre os elementos BSC e BTS (*interface Abis*) e entre o BTS e o terminal (*interface Um*) não foram capturas por falta de ferramentas disponíveis. A descrição geral da arquitetura GSM pode ser encontrada no capítulo 2 deste documento. A sinalização capturada na *interface D* é baseada no protocolo MAP (*Mobile Application Part*) da camada de aplicação da rede SS7 GSM e na *interface A* foram capturados os protocolos de aplicação SS7 DTAP (*Direct Transfer Application Part*) e BSSMAP (*Base Station System Management Part*). O protocolo MAP é responsável pelos mecanismos de gerência de localização e autenticação, o protocolo DTAP é responsável por transportar sinalização do terminal para a MSC e o protocolo BSSMAP transporta sinalização entre a MSC e BSS, maiores informações podem ser encontradas em [60].

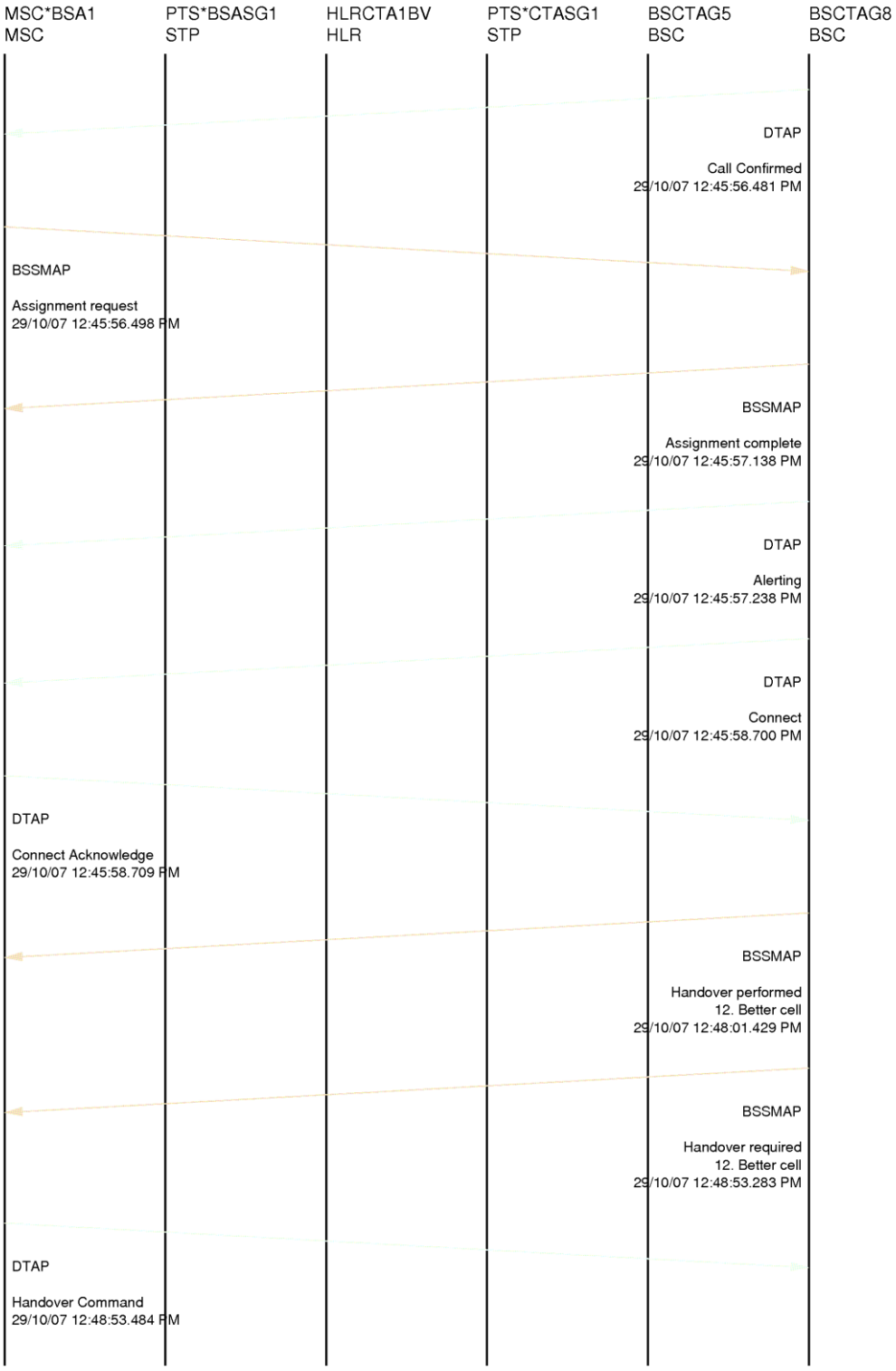
Nas redes GSM o *handover* é comandado pela rede com base nas medidas realizadas pelo terminal móvel. A autenticação do terminal ocorre antes do comando de *handover* ser enviado para o terminal e por este motivo não causa interrupção no serviço, conforme é verificado nas trocas de mensagens capturadas. O tempo verificado entre o envio do comando de *handover* e a confirmação de *handover* foi relativamente elevado, da ordem de 490 ms nas amostras capturadas, mas isso não significa que houve interrupção do serviço, pois como se trata de *handover* horizontal há mecanismos definidos nos procedimentos implementados que garantem a manutenção da comunicação durante a troca de células [60].

A figura F.1 ilustra um dos traçados de sinalização capturados, em formato de fluxo de sinalização.


acceSS7 Sequence Diagram Viewer page 1
MSC*BSA1
MSC
PTS*BSASG1
STP
HLRCTA1BV
HLR
PTS*CTASG1
STP
BSCTAG5
BSC
BSCTAG8
BSC
IMT.2000.MAP
Query with perm
Invoke (last)
SendRoutingInformation
Called Party: 556184018034
29/10/07 12:45:52.390 PM
3GPP.MAP
Query with perm
Invoke (last)
SendRoutingInformation
Called Party: 556184018034
29/10/07 12:45:52.411 PM
3GPP.MAP
Query with perm
Invoke (last)
ProvideRoamingNumber
Calling Party: 556134158434
IMSI: 724160504473438
29/10/07 12:45:52.466 PM
IMT.2000.MAP
Query with perm
Invoke (last)
ProvideRoamingNumber
IMSI: 724160504473438
29/10/07 12:45:52.486 PM
IMT.2000.MAP
Response
Return Result (last)
ProvideRoamingNumber
Translated Numbers: 556184019192
29/10/07 12:45:52.505 PM
3GPP.MAP
Response
Return Result (last)
ProvideRoamingNumber
Translated Numbers: 556184019192
29/10/07 12:45:52.521 PM
3GPP.MAP
Response
Return Result (last)
SendRoutingInformation
IMSI: 724160504473438
Translated Numbers: 556184019192
29/10/07 12:45:52.541 PM


acceSS7 Sequence Diagram Viewer page 2
MSC*BSA1
MSC
PTS*BSASG1
STP
HLRCTA1BV
HLR
PTS*CTASG1
STP
BSCTAG5
BSC
BSCTAG8
BSC
IMT.2000.MAP
Response
Return Result (last)
SendRoutingInformation
IMSI: 724160504473438
anslated Numbers: 556184019192
29/10/07 12:45:52.563 PM
BSSMAP
Paging
IMSI: 724160504473438
29/10/07 12:45:52.576 PM
BSSMAP
Paging
IMSI: 724160504473438
29/10/07 12:45:52.579 PM
DTAP
Paging Response
IMSI: 724160504473438
29/10/07 12:45:55.106 PM
ITU.96.SCCP
CC
29/10/07 12:45:55.115 PM
DTAP
Authentication Request
29/10/07 12:45:55.121 PM
BSSMAP
Classmark update
29/10/07 12:45:55.330 PM
BSSMAP
Classmark update
29/10/07 12:45:55.802 PM


acceSS7 Sequence Diagram Viewer page 3
MSC*BSA1
MSC
PTS*BSASG1
STP
HLRCTA1BV
HLR
PTS*CTASG1
STP
BSCTAG5
BSC
BSCTAG8
BSC
DTAP
Authentication Response
29/10/07 12:45:55.997 PM
BSSMAP
Cipher mode command
29/10/07 12:45:56.007 PM
BSSMAP
Cipher mode complete
29/10/07 12:45:56.270 PM
DTAP
Setup
Calling Party: 06134158434
29/10/07 12:45:56.281 PM
IMT.2000.MAP
Query with perm
Invoke (last)
SendAuthenticationInformation
IMSI: 724160504473438
29/10/07 12:45:56.296 PM
3GPP.MAP
Query with perm
Invoke (last)
SendAuthenticationInformation
IMSI: 724160504473438
29/10/07 12:45:56.319 PM
3GPP.MAP
Response
Return Result (last)
SendAuthenticationInformation
29/10/07 12:45:56.348 PM
IMT.2000.MAP
Response
Return Result (last)
SendAuthenticationInformation
29/10/07 12:45:56.366 PM


MSC*BSA1
MSC
PTS*BSASG1
STP
HLRCTA1BV
HLR
PTS*CTASG1
STP
BSCTAG5
BSC
BSCTAG8
BSC
DTAP
Call Confirmed
29/10/07 12:45:56.481 PM
BSSMAP
Assignment request
29/10/07 12:45:56.498 PM
BSSMAP
Assignment complete
29/10/07 12:45:57.138 PM
DTAP
Alerting
29/10/07 12:45:57.238 PM
DTAP
Connect
29/10/07 12:45:58.700 PM
DTAP
Connect Acknowledge
29/10/07 12:45:58.709 PM
BSSMAP
Handover performed
12. Better cell
29/10/07 12:48:01.429 PM
BSSMAP
Handover required
12. Better cell
29/10/07 12:48:53.283 PM
DTAP
Handover Command
29/10/07 12:48:53.484 PM

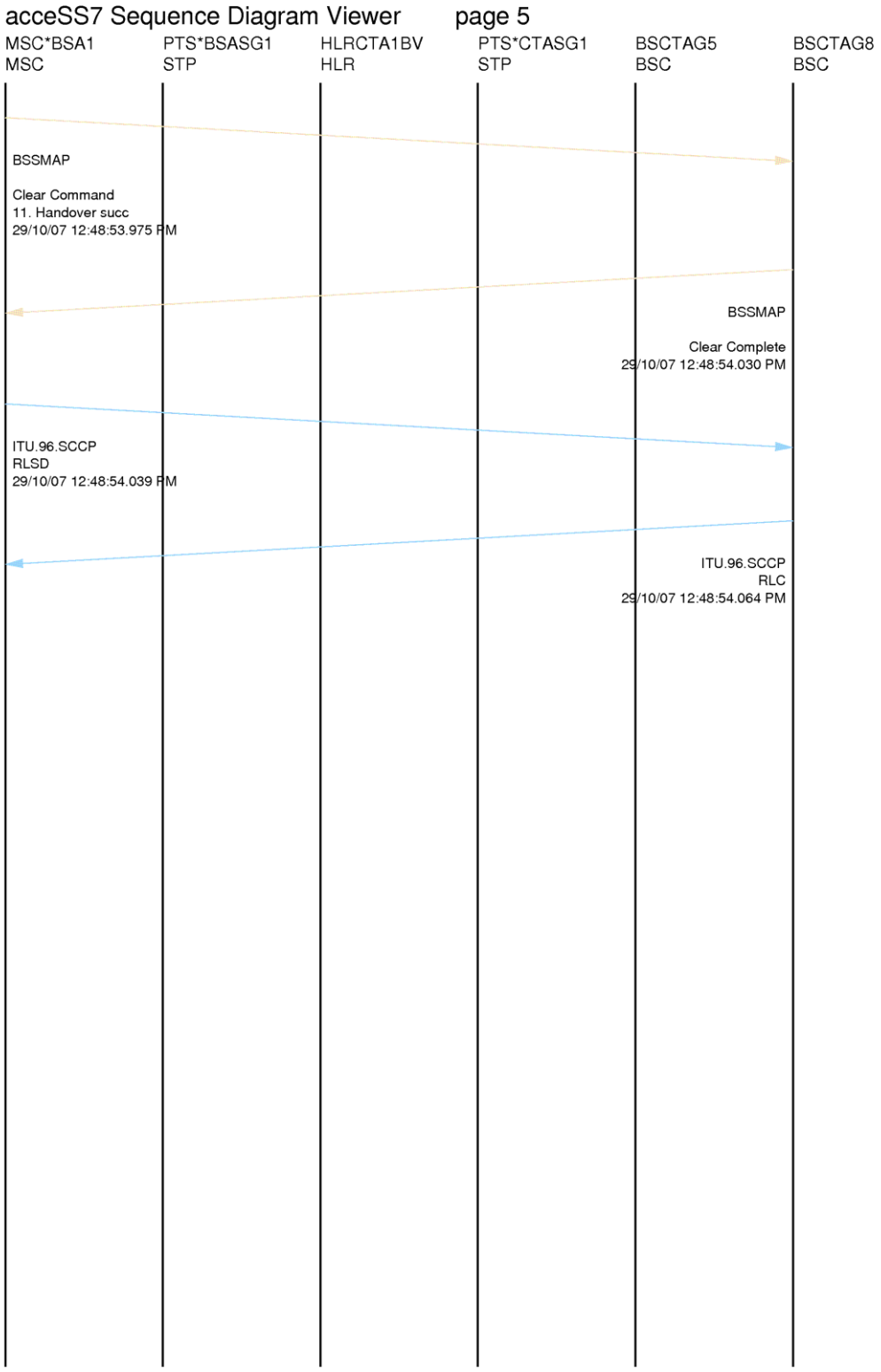


Figura F.1 – Fluxo de sinalização capturado durante *handover* horizontal WWAN

APÊNDICE G – ARTIGO PUBLICADO

Abaixo é reproduzido o artigo do autor e orientador (“Layer 3 Initialization Procedures Recommendation in Next Generation Heterogeneous Mobile Networks”) sobre parte das conclusões deste trabalho [74].

Layer 3 Initialization Procedures Recommendation in Next Generation Heterogeneous Mobile Networks

Sebastião Boanerges Ribeiro Junior, Paulo Roberto de Lira Gondim

Departamento de Engenharia Elétrica, Universidade de Brasília, Brazil
sbribeiro@brasiltelecom.com.br, pgondim@ene.unb.br

1 **Abstract.** The wireless service evolution in conjunction with widespread of WLAN and multi-mode handsets combining heterogeneous radio technologies leads to the possibility of ubiquitous service access thru the offer of vertical handovers techniques. This combined with the multimedia real time service offering unveils the need of new layer 3 initialization procedures in order to keep the end-user quality and experience. This paper presents an evaluation of the network connection procedures against the requirements of the new scenario and proposes changes to the standards.

2 **Keywords:** heterogeneous wireless networks; vertical handover; multimedia real time service; Wi-Fi association and authentication; layer 3 initialization.

1 Introduction

The technological evolution being seen in the last years lead us to the offer of distinct high speed packet data access networks suitable for real time multimedia services and to the availability of multi-mode handsets in the manner to allow the ubiquitous connection on those access networks. In conjunction with the broad acceptation of Session Initiation Protocol (SIP) [1] based service and web based services, this evolution is addressing the end user wish for seamless connection regardless the location and network being used.

The end user need of seamless connection means that the systems, which can be triggered by the network or by the handset, automatically choose the best access network based on the better balance of predefined requirements like cost, speed and quality of service (QoS). Nowadays, the most comprehensive packet data access network regarding cost and data rate are those based on IEEE 802.11 (Wi-Fi) [2]. Seamless wireless multimedia communication data service that wants to get all the advantages of the surrounding access networks must be able to execute simple, fast and effective handover procedure between different accesses networks technologies, this kind of handovers are best known on the literature as vertical handover [3].

In the case of WWAN (e.g. GSM and UMTS networks) to WLAN (e.g. IEEE 802.11) handover the traditional mechanisms based on quality connection monitoring in the physical layer cannot be applied due to the WLAN coverage is include in the WWAN coverage in most of the cases [4]. As the handset is able to scan the available WLAN networks even when the WWAN signal quality is acceptable, the handover decision to WLAN is handset based. Emerging standards like IEEE 802.21 Media Independent Handover are introducing network mechanisms to facilitate the vertical handover decision based on information services supplied from the network to the handsets [5].

Fast handover is crucial for multimedia real time services mainly when in the direction WWAN (e.g. WCDMA or GSM networks) to WLAN (e.g. IEEE 802.11g/Wi-Fi), due to the better data rate and cost per bit offered in the existing Wi-Fi networks [4]. The better end user experience in this case could be gotten as a measurement of the overall handover delay to WLAN, as this means more data rate availability and less cost using the service. In this paper, the overall handover delay is considered as the time used by the system with all the process related to the switch between the radio bearer access networks until the complete availability of the new wireless network to the service being requested by the end user.

However the process of handover can cause disruption of the service being requested due to the technology and limitations on the handset resources. The pace for the broad acceptation of seamless vertical handover services is tied with the market offer of low cost multi-mode handsets even if that means resource constrains. As example, a handset can switch off the previous radio interface before initiate attachment procedure to the new access network due to lack of resource to keep both radio interface active or as a strategy to save battery life. The different characteristics between the heterogeneous access technologies can also cause delays due to the change in the handset network interface configuration.

An important process that account for the overall handover delay and for the disruption of service is not related with the radio link itself, but with the network layer (ISO/OSI layer 3) initialization procedures. These procedures are required by the handset network interface to setup the Internet Protocol (IP) parameters for the service connection to the new access network. The procedures include the network parameters retrieving

from specific servers or from auto configuration methods and the succeeding address duplication detection method. For each version of IP (aka IPv4 and IPv6) commercially available there are different layer 3 initialization procedures and protocols defined for these procedures.

Measurements performed by the authors' unveiled delay up to 1.5 seconds during the layer 3 initialization procedures after Wi-Fi association in a handset with Windows Mobile Operational System (OS). This delay value does not guarantee the Quality of Service (QoS) during multimedia real time data services offering, including video streaming and video communication service. Literature recommendation stands that interruption of the service should not be greater of 40 ms for voice service quality during handover procedures [6].

The layer 3 initialization procedures were evaluated and the standards addressing duplication detection methods found as the main offender in the delay measurements. The standards used for address duplication detection are described in this paper and suggestions for improvements aiming the target delay are proposed.

In this paper we describe the main general procedures that will take place during the handset vertical handover to Wi-Fi networks before the service being requested to be ready to re-connect to the operator's data network. These procedures are the authentication and association to the Wi-Fi network and the layer 3 initialization and connection procedures in IPv4 and IPv6 networks. The results of the author's measurements of the layer 3 connection procedures are also described and we conclude with suggestions for standards improvement to the scenario under analysis.

2 IEEE 802.11i Authentication and Handover Delay

The original IEEE 802.11 specification defines two subtypes of authentication services: Open System and Shared Key [2]. Open System authentication can be defined as a null authentication algorithm. Shared Key authentication is based on the exchange of a shared secret key and can be used with the WEP (Wired Equivalent Privacy) privacy mechanism. Due to security weakness these security mechanisms were superseded by the IEEE 802.11i [7], published as an amendment to the IEEE 802.11 standard.

The 802.11i architecture define the use of IEEE 802.1X [8] standard for authentication and a new mechanism for confidentiality and data integrity based on RSN (Robust Security Network) together with the security protocols TKIP e CCMP [7].

Due to backward compatibility with the previous state machine the IEEE 802.11i defines that an open system authentication shall be requested before the association procedure to the selected Access Point (AP). With IEEE 802.11i, after a successful association the mobile station supplicant initiates the IEEE 802.1X authentication and the key management, in a different way, the original IEEE 802.11 standard allows the exchange of data frames just after the association state.

The IEEE 802.1X requires the use of some EAP method for the authentication procedure. Heterogeneous WWAN and WLAN services based on dual mode handsets look up to use EAP-SIM [9] or EAP-AKA [10] methods in view of the fact that they are based on the pre-existing WWAN (GSM/WCDMA) credentials stored in the SIM/USIM Card.

The use of WWAN pre-existing credentials allow seamless authentication of the handset in any supported WLANs, but may introduce some extra delay due to the authentication request being sent to the home WWAN.

After the successful IEEE 802.1X authentication, a method of security association is established for the purpose of data confidentiality. The IEEE 802.11i defines also key management procedures and protocols to provide fresh keys for the security association called 4-Way Handshake and Group Key Handshake. The Fig. 1 illustrates the IEEE 802.11 operations described.

After a successful key management procedure the handset can start the network connection, based on layer 3 procedures. As the handset IEEE 802.11 MAC management entity had issued the primitive confirming the association success and had changed the IEEE 802.11 state variable [2] (State 3: Authenticated, Associated) before the IEEE 802.1X procedures [7] the handset could also had started the disconnection from the previous access network. This means that any delay due to the network connection procedures represents an interruption on the end-user's service. Depending of the IP version supported, different procedures and different delay figures are applied, as described in the sequence.

3 Connection Procedures on IPV4 Networks

Most of the data networks deployed today is still based on the old IPv4 standards due to the lack of ubiquitous end user clients/handset supporting to new IPv6 standards. Another reason for the current scenario

is that some of address space problems aimed to be solved by IPv6 networks have been temporary postponed as result of the work done in areas as NAT (Network Address Translation) and address allocation, as the IETF Classless Inter-Domain Routing (CIDR) standard [11].

IPv4 dynamic connection procedures rely on DHCP [12] protocol. DHCP standard defines that some method should be used by the client station to check that the IP address granted is not in use by any other station or host. The industry chosen method is based on the ARP (Address Resolution Protocol) protocol. The ARP protocol is an IETF standard [13] defined to find a layer 2 address (e.g. Ethernet MAC address) based on the layer 3 information (e.g. IP address). For address duplication detection purposes a special ARP packet is send to the network with the same sender and target address, this packet is called Gratuitous ARP, and it is intended to not be replied. Most of the handsets models and mobile computer OS deployed nowadays apply three sequential Gratuitous ARP packets as its address duplication algorithm. The issue with this approach is the timer value used. For each new Gratuitous ARP packet sent the timer expiration time is multiplied by a factor (usually 2). As the success criteria (i.e. no duplicate IP address informed) means no reply to the Gratuitous ARP request, the address duplication detection means unnecessary delays due to the sequence of timer expired requests. Commercial handset with Windows Mobile OS implementations can show delays as long as 1.5 seconds as result of the sequential Gratuitous ARP timer expiration, which means an unacceptable delay in the case of seamless handover of multimedia communication applications.

The authors did performed measurements on different handsets and operational systems of the delay to execute the network connection procedures. In the worst case, which was verified with Windows Mobile 5 OS, the handset sent out three Gratuitous ARP request, the first immediately after the DHCP procedures (DHCP ACK), the second after 0.5 seconds and the third one was delivered one second after the second packet, as show in Fig. 2. This means a delay of 1.5 seconds between the first and the third Gratuitous ARP packet just to check whether IP address defined to the interface was duplicated. The best case was seamed in a GF210 handset from UTStarcom with proprietary OS and means transmit of two gratuitous ARP packets with 0.5 seconds delay between them. Even in the best case verified the delay due the ARP expiration timer is not appropriated for the offer of multimedia real time services during the vertical handover procedure.

There is no definition in the ARP standard [13] about the complete procedure for the use of gratuitous ARP to address detection. The authors believe that there is no room for modifications on this old protocol to define a new procedure for multimedia real time vertical handover services, and the best approach should be based on the introduction of the new IPv6 protocols suite.

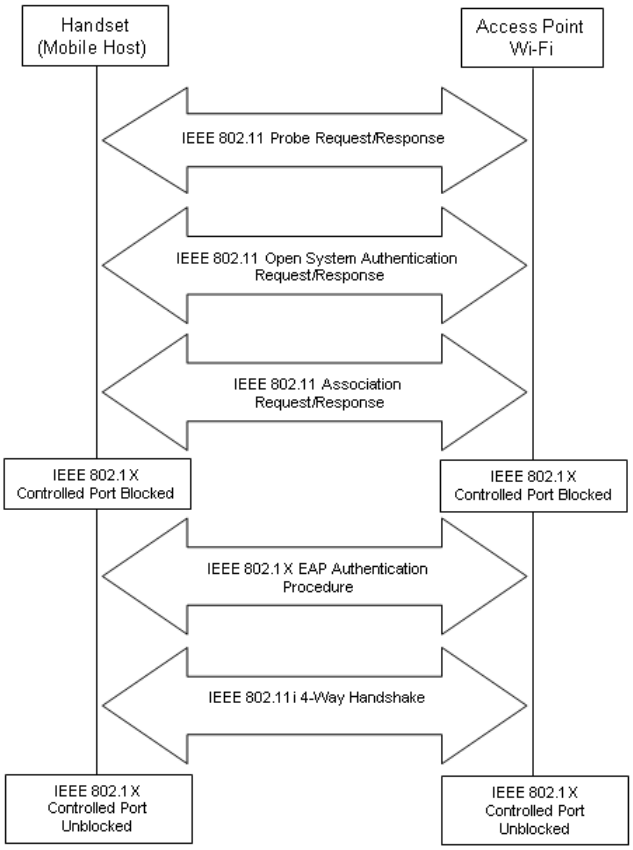


Fig. 1. IEEE 802.11 and 802.11i initial operations

4 Connection Procedures on IPV6 Networks

The IPv6 standard definition came up with a complete set of new protocols to deal with the IP address configuration issues. The IPv6 suite defines two different standard methods for network layer configuration: the autoconfiguration [14] defines a stateless IP address configuration procedure based on the subnet prefix and a local identifier [15] and the DHCPv6 [16] defines a stateful protocol and procedure for address and network configuration of host interfaces.

All IPv6 configuration methods shall use a duplicate address detection (DAD) algorithm [15], defined in [14], which is based on the use of the new ND (Neighbor Discovery) protocol [17]. In a similar way that ARP protocol implementation, the DAD algorithm defines that the station shall sends packets containing Neighbor Solicitation messages with source address as undefined address and target address as the tentative address (IP address candidate to the interface). The lack of response after a timer expiration delay means that the tentative address can be assigned to the interface.

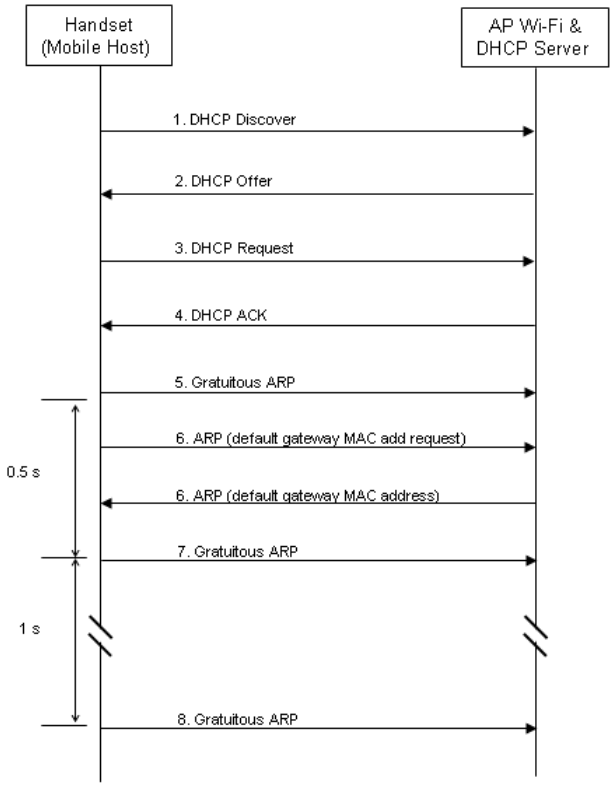


Fig. 2. IPv4 Layer 3 Initialization Procedure.

Even on this new protocol the retransmission timer proposed in the original standard (RETRANS_TIMER) is set to 1,000 milliseconds [17], an extremely long time period for multimedia real time communications. In the same standard document is recognized that the proposed timer values can be overridden by specific changes regarding the link layer being used.

Considering the proposed scenario of multimedia real time service during vertical handover procedure the authors recommend that the ND protocol timers [17] should be reviewed and updated. This review should include the retransmission timer (RETRANS_TIMER) and the maximum retransmission solicitation delay (MAX_RTR_SOLICITATION_DELAY) values, based on the expected maximum disruption time the specified service should support to keep the end user experience and quality of the service.

The MAX_RTR_SOLICITATION_DELAY is defined as the upper limit value for the random time delay selected by the node before send the first message after an interface initialization. The purpose is alleviating possible congestion problem when many interfaces are initialized at the same time, such as after a general failure. This principle could be applicable in the vertical handover scenario proposed due to the possibility of a group of handsets arrive at the same time under the coverage of the same AP or WLAN hotspot. But, the value defined in the original standard (1,000 ms) must be updated to attend the proposed scenario and because the AP coverage limits the amount of concurrent handsets associations.

For voice services the European Telecommunications Standards Institute (ETSI) recommends a maximum interruption of the service during handover of 40 ms [6]. This figure was recommended for horizontal WWAN handover scenario with switched voice service, but should be considered as indicative of the tight boundaries necessary for multimedia real time communications services.

The simple redefinition of the timer expiration time to meet the expected maximum disruption time could not be feasible for all the deployed Wi-Fi hotspots, due to the packet travel time in hotspot subnet. The adoption of smaller value for retransmission timer should lead to a re-engineering of the hotspots network to guarantee that the ND solicitations messages will be processed by all the nodes before the expiration timer.

5 Conclusion

The broad availability of different high speed wireless data access technologies covering the same region, together with the evolution of multi-mode handsets and the end user demands of multimedia real time service has lead to the development of novel seamless vertical handover methods. This paper scenario is based on vertical handover procedure from WWAN to Wi-Fi access network. The attractiveness of this scenario is due to the higher data rate and lower cost per bit provided by WLANs networks in comparison with commercial WWANs (e.g. GSM and UMTS networks).

These new vertical handover scenarios should push the review of handset authentication and layer 3 connection procedures, in the manner to address the new requirements of connection delays and quality of service while the handover is being executed. The main issue is regarding the disruption of service during a multimedia real time communication service, as per example a video conference. As the network layer 3 connection procedures are executed after the Wi-Fi association and authentication, i.e. the link layer handover, any delay on it affect directly the service quality and the end-user experience.

We have shown that the duplicate address detection mechanism is the main cause of the network connection delay, as result of its success criteria based on timer expiration request.

The IPv4 networks offer no method to avoid disruption of the service during the network connection on the proposed scenario. The methods being utilized account up to 1.5seconds delay and the authors' recommendation is to upgrade the existing access networks and handset to support IPv6 for the evaluated scenario.

With the development of IPv6 protocol suite, novel methods for IP configuration and for duplicate address detection were also developed. Even with these new methods the published standard defines a long timer limit value which is not feasible for multimedia real time service handover delay. The authors' recommendation for IPv6 Wi-Fi based networks subjected to vertical handover is the definition of new tighter timer values for the ND protocol specific variables. The use of tighter timer limits should also be accompanied with engineering guidelines for the local area networks serving the Wi-Fi hotspots, as extensive hotspots networks cannot be able to respond timely the duplicate address detection requests.

The adoption of the recommendations of this paper can assist and stimulate the development of low tier multi-mode handsets. The capacity to use the same network interfaces regardless the wireless access network, and continuing being able to offer seamless handover service can simplify the handset design and save production cost.

References

1. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, IETF, June (2002).
2. IEEE Computer Society, "ANSI/IEEE Std 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999 Edition, June (2003).
3. N. Nasser, A. Hasswa, H. Hassanein, "Handoffs in fourth generation heterogeneous networks", IEEE Communications Magazine, pp. 96–103, October (2006).
4. J. Nie, J. C. Wen, Qi Dong, Z. Zhou, "A seamless handoff in IEEE 802.16a and IEEE 802.11n hybrid networks", 2005 International Conference on Communications, Circuits and Systems, pp. 383-387, May (2005).
5. A. de la Oliva, C. J. Bernados, T. Melia, I. Soto, A. Vidal, A. Banchs, "A case study: IEEE 802.21 enabled mobile terminals for optimized WLAN/3G handovers", Mobile Computing and Communications Review, Volume 11, Number 2, pp. 29–40, April (2007).
6. European Telecommunications Standards Institute, "TR 122 925 V3.1.1 (2000-02) Universal Mobile Telecommunications System (UMTS); Service aspects; Quality of Service and Network Performance (3G TR 22.925 version 3.1.1 Release 1999)", April (1999).

7. IEEE Computer Society, “802.11i, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements”, July (2004).
8. IEEE Computer Society, “IEEE Std 802.1X-2004, IEEE Standard for Local and Metropolitan Area Networks – Port Based Network Access Control”, December (2004).
9. H. Haverinen, J. Salowey, “Extensible Authentication Protocol method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)”, RFC 4186, IETF, January (2006).
10. J. Arkko, H. Haverinen, “Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement (EAP-AKA)”, RFC 4187, IETF, January 2006.
11. Y. Rekhter, T. Li, “An architecture for IP address allocation with CIDR”, RFC 1518, IETF, September 1993.
12. R. Droms, “Dynamic Host Configuration Protocol”, RFC 2131, IETF, March 1997.
13. David C. Plummer, “An Ethernet Address Resolution Protocol”, RFC 826, IETF, (1982).
14. S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, IETF, (1998).
15. F. Donzé, “IPv6 autoconfiguration”, The Internet Protocol Journal – Volume 7, Number 2, pp. 12-16, June (2004).
16. R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, RFC 3315, IETF, July (2003).
17. T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, IETF, December (1998).