Universidade Estadual de Campinas
Faculdade de Engenharia Elétrica e de Computação
Departamento de Comunicações

ANÁLISE DO MECANISMO DE SEGURANÇA DA ARQUITETURA IMS

Autor: Francisco José Viudes Nobôa

Orientador: Prof. Dr. Yuzo Iano

Dissertação de Mestrado apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos para a obtenção do título de Mestre em Engenharia Elétrica.
Área de concentração: **Telecomunicações e Telemática.**

Banca Examinadora

Prof. Dr. Yuzo Iano (presidente)	— Decom/Feec/Unicamp
Prof. Dr. Adão Boava	— UFFS
Prof. Dr. Luiz César Martini	— Decom/Feec/Unicamp

Campinas – SP
25 de maio de 2012

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

N663a

Nobôa, Francisco José Viudes
Análise do mecanismo de segurança da arquitetura IMS / Francisco José Viudes Nobôa. --Campinas, SP: [s.n.], 2012.

Orientador: Yuzo Iano.
Dissertação de Mestrado - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Segurança. 2. Redes. 3. Redes de computação. 4. Arquitetura de redes. 5. Sistemas de segurança. I. Yuzo Iano. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Título em Inglês: Analysis of the security mechanism in the IMS architecture
Palavras-chave em Inglês: Security, Networks, Computing network, Network architecture, Security systems
Área de concentração: Telecomunicações e Telemática
Titulação: Mestre em Engenharia Elétrica
Banca examinadora: Adão Boava, Luiz César Martini
Data da defesa: 25-05-2012
Programa de Pós Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE MESTRADO

Candidato: Francisco José Viudes Nobôa

Data da Defesa: 25 de maio de 2012

Título da Tese: "Análise do Mecanismo de Segurança da Arquitetura IMS"

Prof. Dr. Yuzo Iano (Presidente): _____

Prof. Dr. Adão Boava: Adão Boava

Prof. Dr. Luiz César Martini: _____

Dedico esta dissertação de mestrado a Deus e aos meus familiares, que sempre me apoiaram e incentivaram. Especialmente à minha esposa Léa Gonçalves Nobôa, a minha filha Lívia Gonçalves Nobôa e a minha mãe, Aparecida Viudes Tineu , que apesar das dificuldades concedeu-me a oportunidade de progredir nos estudos.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, por ter me permitido cruzar mais essa etapa da vida, e por ter me alimentado na fé e perseverança e aos meus familiares.

Agradeço ao meu orientador, Prof. Dr. Yuzo Iano, por ter me aceito como um de seus orientados de mestrado e pela sua competente orientação e contribuições no desenvolvimento do trabalho apresentado.

Agradeço a minha esposa Léa pelo incentivo e por sempre ter acreditado na finalização desse trabalho, a minha querida filha Lívia que seu sorriso meigo tem me fortalecido e encorajado a continuar sempre lutando, e em especial à minha mãe Aparecida que sempre acreditou no meu potencial e foi a responsável pelo meu ingresso na Unicamp em 1995.

Agradeço ao CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico, a Capes - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, a Fapesp – Fundação de Amparo à Pesquisa do Estado de São Paulo e a Faepex – Fundo de Apoio ao Ensino, à Pesquisa e à Extensão pelo fomento à pesquisa que tanto tem ajudado o desenvolvimento e o progresso do nosso país, e em especial a Unicamp.

Agradeço também as empresas nas quais trabalhei Ericsson Telecomunicações e Motorola Industrial, que desde 2001 tem me incentivado e liberado para o estudo das disciplinas de Pós-Graduação da Unicamp.

"Sonhos não morrem, apenas adormecem na alma da gente."
(Chico Xavier)

RESUMO

Considerando-se que para controlar e possibilitar a entrega de diversos conteúdos e serviços a qualquer tipo de acesso fazia-se necessário um núcleo bem definido e estruturado, surgiu o IMS (*IP Multimedia Subsystem*) com o propósito de prover a integração completa das redes e serviços. O IMS define uma arquitetura completa e *framework* que habilita a convergência de voz, vídeo, dados e tecnologia de rede móvel através de uma infraestrutura baseada em IP, preenchendo a distância entre os dois paradigmas de comunicação mais bem sucedidos, celular e tecnologia IP. Este trabalho apresenta a arquitetura IMS como controle central de todas as redes, e uma arquitetura para o desenvolvimento de aplicações móveis que incorporem voz, vídeo e dados. A arquitetura IMS apesar de promissora apresenta inúmeras oportunidades de melhoria no seu mecanismo de segurança, muitas dessas oportunidades de melhoria estão relacionadas a falhas e até mesmo a falta de especificações de segurança quando a arquitetura foi originalmente implementada. Assim o maior desafio na implantação e globalização da arquitetura IMS são as falhas de segurança e a vulnerabilidade que a arquitetura possui a diversos tipos de ataques que podem atingir e prejudicar, tanto operadoras quanto usuários da rede. O objetivo deste projeto de pesquisa é apresentar uma análise detalhada sobre a estrutura da arquitetura IMS focando principalmente na arquitetura de segurança desenvolvida pela 3GPP, e assim prover análises e soluções para os ataques, vulnerabilidades e falhas de segurança que atingem a arquitetura tanto do ponto de vista de operadoras e provedores de serviço quanto na perspectiva do usuário.

Palavras-chaves - IMS, SIP, VoIP, segurança, redes IP.

ABSTRACT

Considering that to control and enable the delivery of diverse content and services to any type of access it should make necessary a core well-defined and structuralized, appeared the IMS (IP Multimedia Subsystem) in order to provide the complete integration of networks and services. IMS defines a complete architecture and framework that enables the convergence of voice, video, data and mobile network technology over an infrastructure based on IP, in addition to filling the gap between the two communications paradigms most successful, cellular and IP technology. This paper presents the IMS architecture as central control of all networks, and architecture for developing mobile applications that incorporate voice, video and data. The IMS architecture despite being promising presents numerous opportunities for improvement in its security mechanism, many of these opportunities for improvement are related to failures and even the lack of security specifications when creating the architecture. So the biggest challenge in the implementation of the IMS architecture and globalization are the security issues and vulnerabilities that the architecture faces being vulnerable to several types of attacks that can reach and affect carriers and network users. The objective of this research project is to present a detailed analysis on the structure of the IMS architecture focusing primarily on security architecture developed by 3GPP, and thus provide analysis and solutions about the attacks, vulnerabilities and security issues that affect the architecture from the point of view of carriers, service providers and from the network users.

Keywords *- IMS, SIP, VoIP, security, networking.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

3GPP	*Third Generation Partnership Project*
ADSL	*Asymmetric Digital Subscriber Line*
AH	*Authentication Header*
AKA	*Authentication and Key Agreement*
AIN	*Advanced Intelligent Network*
AIS	*Artificial Immune System*
AMR	*Adaptative Multi Rate*
ANSI	*American National Standards Insitute*
APN	*Access Point Name*
ARP	*Address Resolution Protocol*
AS	*Application Server*
ATM	*Asynchronous Transfer Mode*
AuC	*Authentication Center*
BGCF	*Breakout Gateway Control Function*
BS	*Billing System*
CAC	*Connection Admission Control*
CAMEL	*Customized Applications for Mobile networks using Enhanced Logic*
CAP	*CAMEL Application Part*
CCF	*Charging Collector Function*
CDMA	*Code Division Multiple Access*
CDR	*Call Detail Records*
CPU	*Central Processing Unit*
CSCF	*Call Session Control Function*
CTF	*Charging Trigger Function*

DoS	*Denial of Service*
DVR	*Digital Video Recorder*
ECUR	*Event Charging with Unit Reservation*
ECF	*Event Charging Function*
ESP	*Encapsulating Security Payload*
ETSI	*European Telecommunications Standards Institute*
FMC	*Fixed-Mobile Convergence*
GPRS	*General Packet Radio Service*
GSM	*Global System for Mobile Communication*
HLR	*Home Location Register*
HN	*Home Network*
HSDPA	*High Speed Downlink Packet Access*
HSS	*Home Subscriber System*
HSUPA	*High Speed Uplink Packet Access*
HTTP	*HyperText Transfer Protocol*
IBCF	*Interconnection Border Control Function*
I-CSCF	*Interrogating - Call Session Control Function*
IETF	*Internet Engineering Task Force*
IKE	*Internet Key Exchange*
IM	*Instant Messaging*
IMC	*IM Credentials*
IMPI	*IM Private Identity*
IMPU	*IM Public Identity*
IMS	*IP Multimedia Subsystem*
IMSI	*International Mobile Subscriber Identity*
IP	*Internet Protocol*

IPTV	*Internet Protocol Television*
ISIM	*IM Subscriber Identity Module*
ITU	*International Telecommunication Union*
ISDN	*Integrated Services Digital Network*
LBS	*Location Based Service*
MAC	*Message Authentication Code*
MGCF	*Media Gateway Controller Function*
MGCP	*Media Gateway Control Protocol*
MGW	*Media Gateway*
MIME	*Multipurpose Internet Mail Extensions*
MMS	*Multimedia Messaging Service*
MPLS	*Multiprotocol Label Switching*
MRF	*Media Resource Function*
MRFC	*Media Resource Function Controllers*
MRFP	*Media Resource Function Processors*
MSISDN	*Mobile Subscriber ISDN*
NAT	*Network Address Translation*
NGN	*Next Generation Network*
NNI	*Network-to-Network Interface*
OCF	*Online Charging Function*
OMA	*Open Mobile Alliance*
OSA	*Open Service Access*
P-CSCF	*Proxy - Call Session Control Function*
PCM	*Pulse Code Modulation*
PDF	*Policy Decision Function*
PLMN	*Public Land Mobile Network*

PoC	*Push to Talk over Cellular*
PSTN	*Public Switched Telephone Network*
PTS	*Push to Show*
PTT	*Push to Talk*
QoS	*Quality of Service*
RTCP	*Real Time control Protocol*
RTP	*Real Time Protocol*
RSVP	*Resource ReserVation Protocol*
SA	*Security Association*
SEG	*Security Gateway*
S-CSCF	*Serving – Call Session Control Function*
SCF	*Session Charging Function*
SCIM	*Service Capability Interaction Manager*
SCTP	*Stream Control Transmission Protocol*
SDP	*Session Description Protocol*
SGW	*Signaling Gateway*
SIM	*Subscriber Identity Module*
SIP	*Session Initiation Protocol*
SLF	*Subscritor Location Functions)*
SMS	*Short Message Service*
SMTP	*Simple Mail Transfer Protocol*
SPI	*Security Parameter Index*
SPIT	*Spam-over-Internet Telephony*
SQL	*Structured Query Language*
SS	*Soft Switch*
TCO	*Total Cost of Ownership*

UDP	*User Datagram Protocol*
UE	*User Equipment*
UA	*User Agent*
UAC	*User Agent Client*
UAS	*User Agent Server*
UMTS	*Universal Mobile Telecommunications System*
UNI	*User-to-Network Interface*
URI	*Uniform Resource Identifier*
USB	*Universal Serial Bus*
USIM	*Universal Subscriber Identity Module*
VoIP	*Voice over Internet Protocol*
WCDMA	*Wideband Code Division Multiple Access*
WLAN	*Wireless Local Area Network*

SUMÁRIO

xxx

CAPÍTULO 1

INTRODUÇÃO

Considerando-se que para controlar e possibilitar a entrega de diversos conteúdos e serviços a qualquer tipo de acesso fazia-se necessário um *core* bem definido e estruturado, surgiu o IMS (*IP Multimedia Subsystem*) com o propósito de prover a integração completa das redes e serviços[46].

Portanto, a Fig. 1.1 a seguir ilustra o que se proporia a ser a arquitetura IMS, como o controle central de todas as redes, como redes de acesso fixo, móvel, *broadband wirelles* e *broadband cable*.

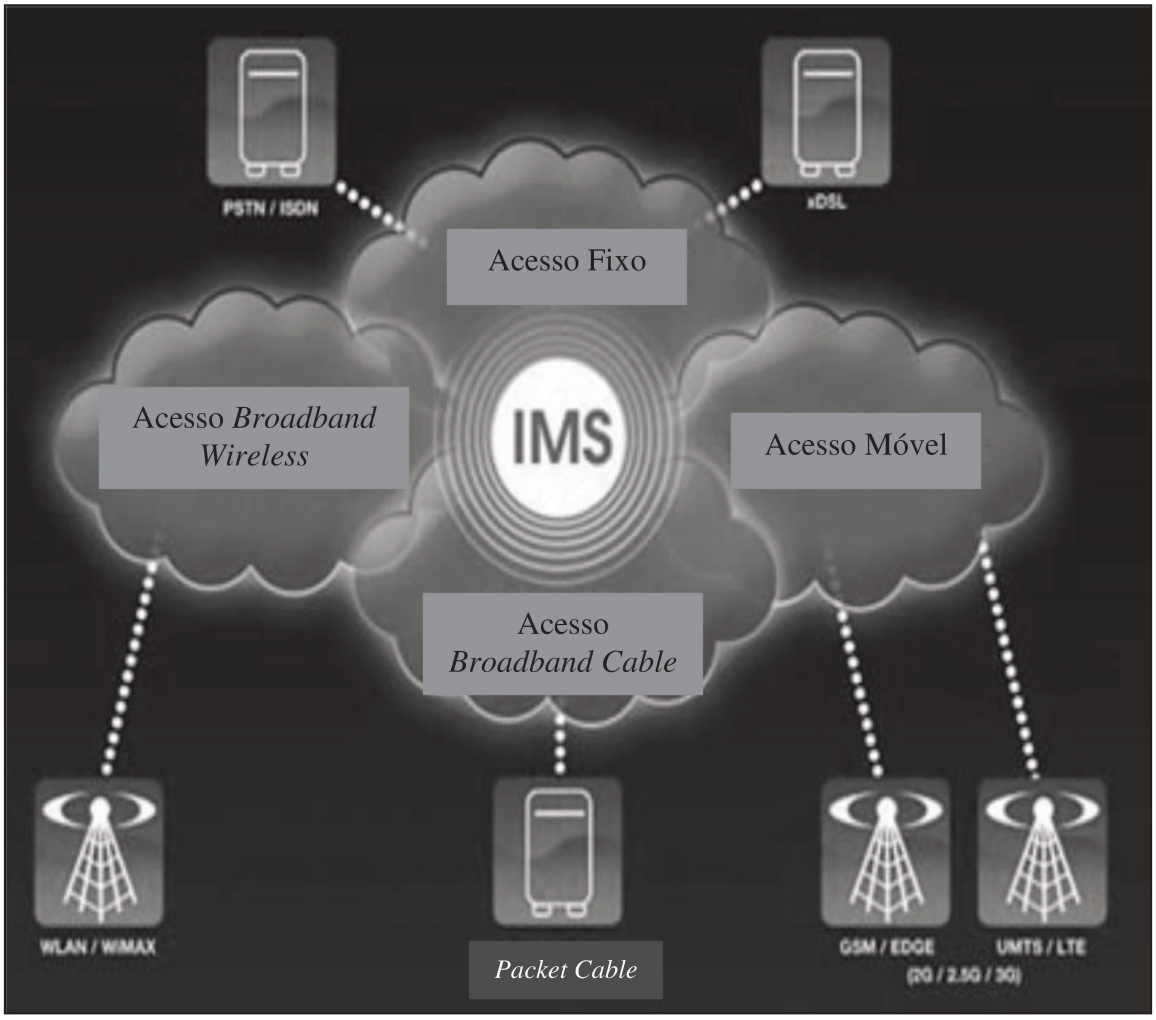

Fig. 1.1 - Arquitetura IMS como controle central de todas as redes [47].

O IMS é um conjunto de especificações que descrevem a arquitetura NGN (*Next Generation Network*) para implementação de serviços de telefonia e multimídia baseado em IP [41].

O IMS permite a integração entre diferentes tipos de redes e serviços, como por exemplo, rede celular trafegando serviço multimídia.

O IMS define uma arquitetura completa e *framework* que habilita a convergência de voz, dados, vídeo e tecnologia de rede móvel através de uma infraestrutura baseada em IP [41].

O propósito do IMS seria fornecer acesso celular para todos os serviços que dispõem de i*nternet*.

Padronizado pelo 3GPP (*Third Generation Partnership Project*), grupo responsável pela normatização das redes móveis de terceira geração.

Os protocolos utilizados na arquitetura são padronizados pelo IETF (*Internet Engineering Task Force*) e o ANSI (*American National Standards Institute*).

Enquanto o IETF padroniza os protocolos, o 3GPP especifica a integração das redes celulares com o IMS, e o ANSI permite a integração com o sistema legado através de seus protocolos.

O IMS é uma arquitetura funcional de rede que é vista como uma solução promissora, na medida em que facilita a criação e o desenvolvimento de serviços multimídia, assim como o suporte a interoperabilidade e a convergência de rede[46].

Outro ponto a salientar seria que a primeira geração da *internet* foi mais utilizada para transporte de dados não *real-time*.

Contudo com a demanda crescente por conteúdo multimídia, que tende a crescer ainda mais nos próximos anos, a *QoS* acaba sendo um requisito fundamental nas arquiteturas de rede atuais, assim a arquitetura IMS vem preencher esse requisito essencial nas arquiteturas de rede.

O cenário de pré-convergência, conforme a Fig. 1.2, mostra uma arquitetura descentralizada, ou seja, uma rede específica para cada tipo de serviço. Esse tipo de cenário possui uma rede de acesso (infraesturutra), um controle de sessão e um perfil de usuário para cada tipo de rede.

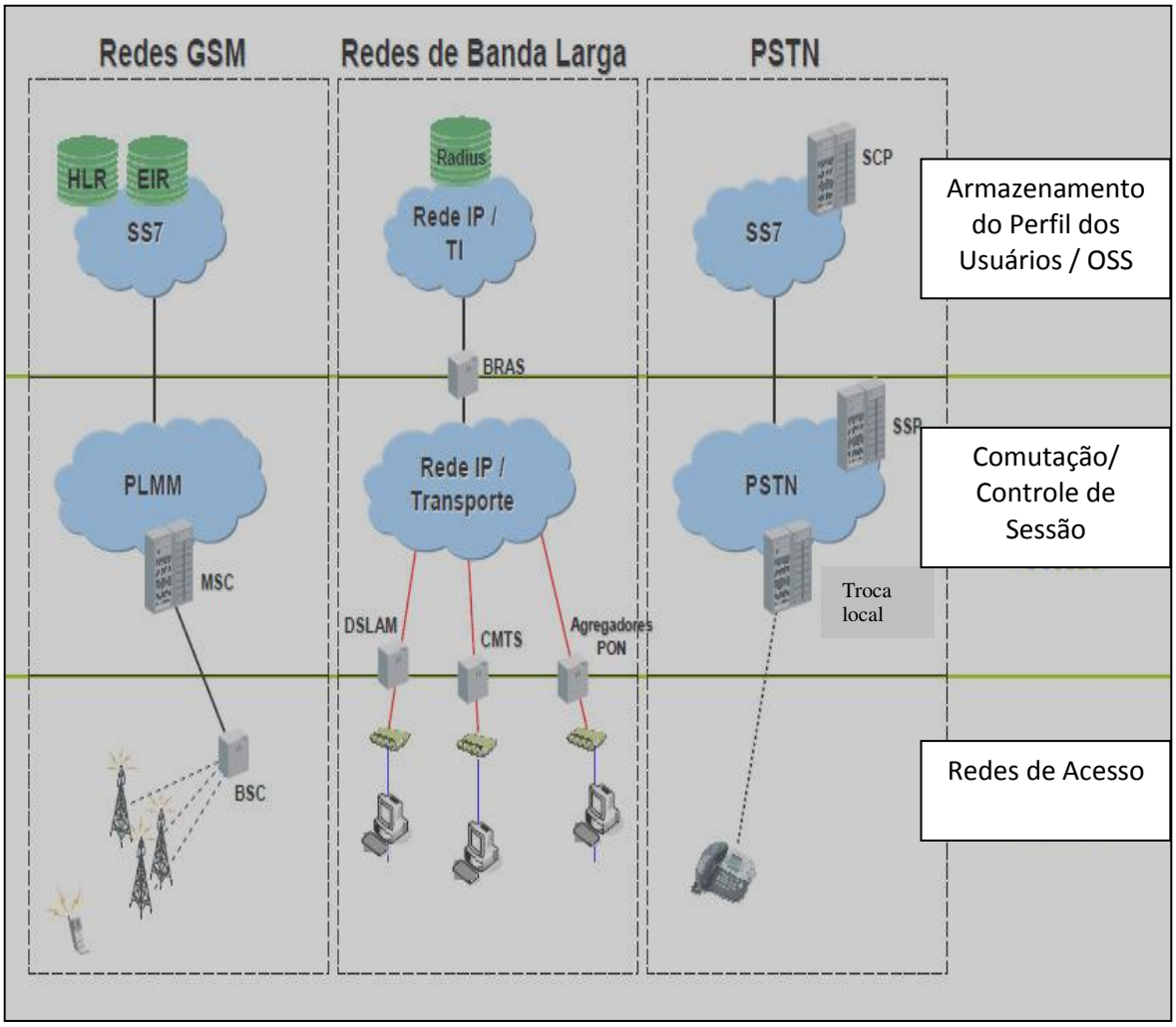

Fig. 1.2 - Cenário pré-convergência [13].

Já no cenário convergente, ou seja, arquitetura IMS, os diversos serviços prestados são tratados através de um controle de sessão único (centralizado), que faz a integração entre as diversas redes de acesso e unifica todos os perfis de usuário relacionados aos serviços, conforme ilustrado na Fig. 1.3.

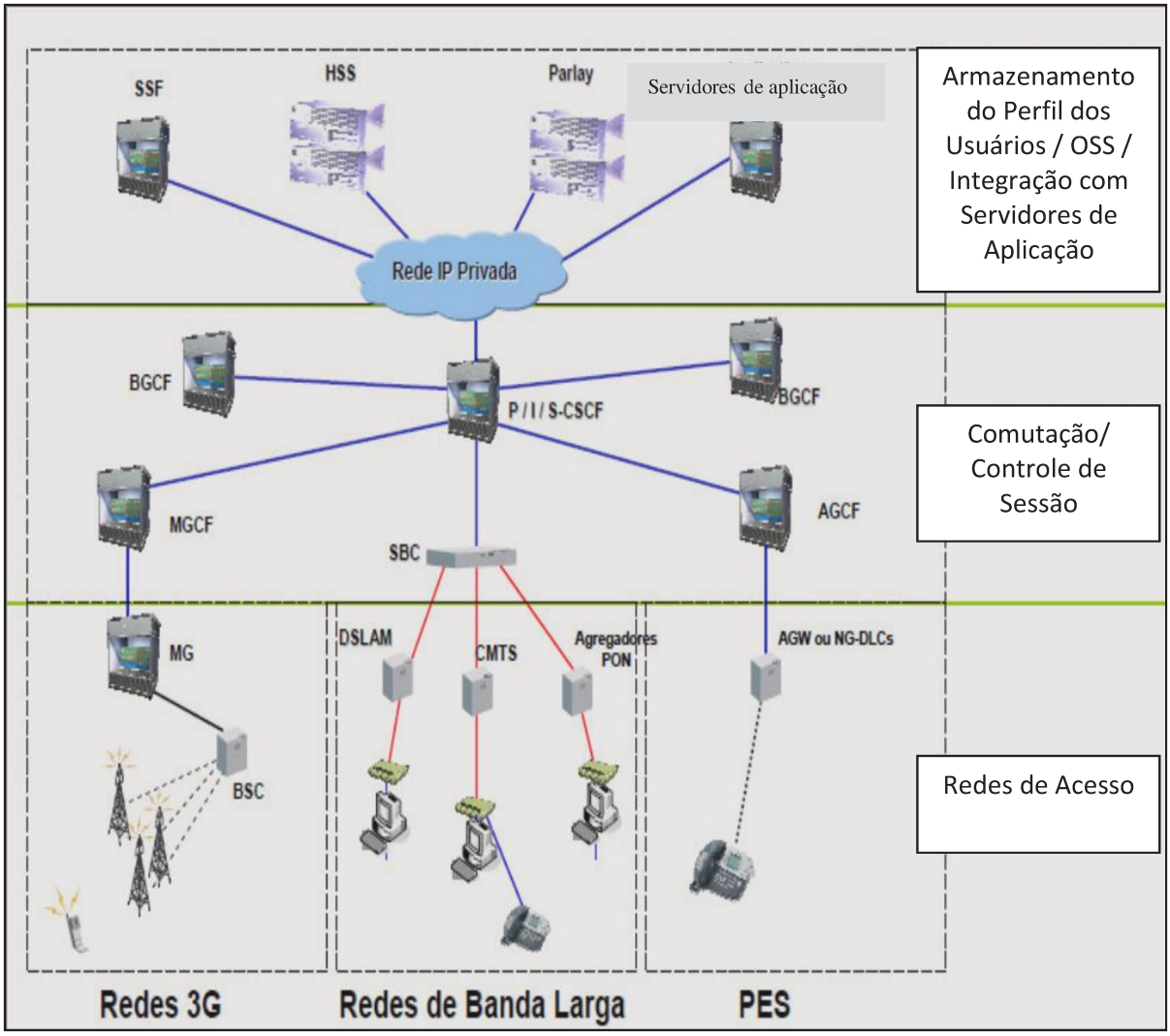

Fig. 1.3 - Cenário convergente [13].

1.1. Desafio

O maior desafio na implantação e globalização da arquitetura IMS são as falhas de segurança e a vulnerabilidade que a arquitetura possui a diversos tipos de ataques que podem atingir tanto operadoras quanto usuários da rede.

Muitos desses problemas de segurança se devem principalmente pela deficiência nos requisitos e especificações de segurança quando da implementação da arquitetura, além do que o *design* inicial da arquitetura IMS previa a utilização do IPv6 ao invés do IPv4.

Entretanto, quando a implantação da arquitetura IMS tornou-se realidade o IPv6 não estava completamente desenvolvido e implementado para utilização e a arquitetura IMS acabou tendo que mudar seu *design* original para suportar tanto o IPv4 quanto o IPv6.

Dessa forma muitas das características da arquitetura desenhadas especificamente no IPv6 tiveram que ser modificadas para se adaptar ao IPv4 também, como por exemplo, a adoção do NAT, que no caso do IPv6 não seria necessário dado a abundância de endereços IP únicos.

Além do que as características do IPSec no IPv6 também deveriam providenciar transporte de dados seguro através da rede. Ademais, como o IMS é baseado nos protocolos SIP e IP, conseqüentemente ele já herda as falhas de segurança desses protocolos.

Outro ponto a salientar seria o fato que o IMS, dada sua própria natureza de conectividade com a i*nternet*, enfrenta ameaças e exposições muito maiores que as infraestruturas de telecomunicações anteriores.

Esse fator aliado à própria evolução tecnológica que os dispositivos móveis vêm sofrendo ao longo dos anos cria um ambiente muito mais vulnerável e propício a ataques e violações de segurança.

1.2. Motivação

O tema foi escolhido para compor esse projeto de pesquisa dada a sua relevância e importância no meio acadêmico-científico.

Inúmeros pesquisadores, operadoras de telefonia e empresas de manufatura ao redor do mundo estão trabalhando nesse tema, em parceria com a 3GPP, no intuito de tornar a arquitetura segura e robusta.

Como vimos, o IMS é uma arquitetura promissora, que inclui ínúmeros benefícios e vantagens sobre as atuais arquiteturas descentralizadas.

Entretanto as inúmeras falhas de segurança apresentadas pela arquitetura impedem sua adoção e o desenvolvimento da arquitetura em escala global.

Inclusive muitas empresas abortaram seus projetos em IMS ou então partiram para a implementação de soluções próprias de segurança como é o caso da Verizon Wirelles que desenvolveu o A-IMS implementando alguns requisitos de segurança específicos.

Todavia, empresas que não possuem o porte e as condições de uma Verizon Wirelles, acabam simplesmente desistindo do IMS.

Dessa forma, o futuro dessa arquitetura depende desse trabalho de pesquisa que está sendo realizado por diversas entidades ao redor do mundo.

Trabalho esse que visa não só o mapeamento das falhas de segurança como também soluções e propostas de melhorias no mecanismo de segurança da arquitetura.

Sendo assim, quanto maior o número de pesquisadores envolvidos nesse projeto, maior serão as chances de sucesso nesse trabalho de pesquisa.

1.3. Objetivos Gerais

O objetivo geral do projeto de pesquisa é promover uma análise detalhada na arquitetura IMS, focando essa análise para as falhas de segurança apresentadas por essa arquitetura.

Dessa forma mais especificamente os objetivos da pesquisa seriam promover uma análise no mecanismo de segurança da arquitetura IMS.

Apontando assim, eventuais problemas no mecanismo de segurança da arquitetura, especificando esses problemas e dessa forma analisando e propondo potenciais soluções.

1.3.1. Objetivos Específicos

Como objetivos específicos, esse trabalho propõe a análise dos principais tipos de ataques que podem atingir as redes IMS no intuito de derrubar os serviços ou atacar os usuários da rede.

Além da análise de segurança para provedores de serviço/rede e a análise de segurança para usuários da rede, bem como uma proposta para eliminar ataques SPIT (*Spam-over-Internet Telephony*) nas redes IMS.

O trabalho finaliza apresentando um módulo de segurança para o IMS, baseado em sistemas imunológicos e agentes móvies.

Além disso, tem-se como objetivo específico o estudo da arquitetura das redes 3G e os protocolos envolvidos na arquitetura IMS.

1.4. Contribuição

O próposito deste trabalho é prover um estudo completo e detalhado na estrutura da arquitetura IMS e na implementação de segurança da arquitetura.

Mapeando e identificando falhas no mecanismo de segurança da arquitetura, e as limitações que as arquiteturas de segurança atuais apresentam.

Além de mapear e identificar os principais tipos de ataques que poderiam atingir a rede no intuito de derrubar os serviços da rede, ou mesmo prejudicar usuários e operadoras.

Uma vez mapeados e identificados os principais tipos de ataques e vulnerabilidades de segurança da arquitetura, analisar e identificar as questões de segurança para usuários da rede e provedores de serviço/rede.

Ademais, essa pesquisa tem como objetivo propor uma solução para um dos principais problemas de segurança da arquitetura que é o ataque VoIP *spam* ou SPIT (*Spam-over-Internet Telephony*).

Dessa forma, finalizando com a proposta de um módulo de segurança para o IMS. Essa proposta de segurança é baseada na arquitetura lógica de segurança do IMS, envolvendo os elementos centrais da arquitetura de segurança do IMS e a sinalização da arquitetura.

Assim, esse projeto de pesquisa não pretende realizar testes ou simulações em ambientes reais devido à limitação e a dependência de uma operadora que tenha IMS em sua rede, atualmente apenas algumas operadoras nos Estados Unidos e Europa possuem IMS em suas redes.

Além do que testes ou simulações que estejam fora do ambiente de produção real de uma operadora, e que não utilizem a tarifação, a sinalização e a base de usuários reais de uma operadora não agregariam em nada a esse projeto de pesquisa, pois seriam limitados e não representariam a realidade do que acontece em um ambiente real.

Visto que apenas um ambiente de produção real poderia enumerar e explicitar os diversos tipos de ataques que "usuários maliciosos" ou *hackers* poderiam usar para atingir a rede.

Assim, entende-se que qualquer tipo de simulação pelas limitações mencionadas acima, não agregaria valor a esse projeto.

Portanto, o real valor desse projeto de pesquisa está nas análises de segurança realizadas baseadas nos ataques que a arquitetura IMS está susceptível, e na proposta de uma arquitetura de segurança baseada em agentes imunológicos que se utilizam de agentes móveis, a introdução dessa idéia, apesar de teórica, é de total valia dado que os agentes móveis interagem com elementos reais da arquitetura de segurança do IMS proposta pelo 3GPP.

Caracterizando-se assim por ser uma proposta de segurança baseada na arquitetura lógica de segurança do 3GPP.

Algumas empresas e operadoras tem desenvolvido e implementado arquiteturas de segurança para o IMS, entretanto essas implementações são confidenciais e de uso restrito.

Como já mencionado, inúmeras pesquisas ao redor do mundo estão sendo feitas no intuito de desenvolver uma implementação segura e robusta para a aquitetura IMS.

Contribuindo dessa forma para a globalização dos problemas de segurança enfretados pela arquitetura e consequentemente difundindo o conhecimento para a descoberta e implementação de soluções.

1.5. Estrutura do Trabalho

Esta dissertação está organizada da seguinte forma:

Neste capítulo é apresentado o desafio, a motivação, o problema, os objetivos propostos e apresenta a contribuição que este trabalho acrescentará.

O capítulo 2 apresenta os conceitos da arquitetura IMS, apresentando os benefícios da arquitetura, o histórico, os principais protocolos usados e apresenta os principais componentes da arquitetura.

O capítulo 3 apresenta algumas aplicações IMS e faz a introdução dos principais serviços IMS, e apresenta o protocolo SIP, especificando as funcionalidades, formato de mensagens e fluxo de mensagens.

O capítulo 4 apresenta a arquitetura de segurança do IMS, os recursos e mecanismos de segurança da arquitetura, bem como os procedimentos para configuração de associação de segurança.

O capítulo 5 apresenta as falhas de segurança da arquitetura IMS, os principais tipos de ataques, e providencia análises de segurança para provedores e usuários da rede, bem como apresenta uma proposta de uma metodologia para eliminar o SPIT no IMS.

O capítulo 6 apresenta os sistemas imunológicos no ambiente de segurança computacional, introduzindo assim uma proposta de um módulo de segurança para o IMS utilizando AIS e agentes móveis.

O capítulo 7 apresenta as considerações finais deste trabalho, discute as conclusões observadas durante a pesquisa e sugere oportunidades de continuação deste trabalho.

Na seção final deste documento encontram-se as referências bibliográficas e as normas 3GPP e IETF, que mencionam ou estão relacionadas com o IMS.

CAPÍTULO 2

IMS – IP *MULTIMEDIA SUBSYSTEM*

O IMS é uma arquitetura funcional de rede que demanda alguns requisitos para sua implementação.

Esses requisitos foram definidos pelo 3GPP [1] com o objetivo de prover serviços de multimídia baseado em IP para os usuários finais. O primeiro, e mais óbvio, é o suporte para estabelecimento de sessões multimídia sobre IP.

Esse requisito é a base necessária para suportar o principal serviço a ser entregue pelo IMS: sessões multimídia sobre redes de comutação por pacotes, onde se entenda por multimídia a existência simultânea de vários tipos de mídia.

Como principal exemplo de serviço, e de especial importância para o usuário, tem-se a comunicação de áudio e vídeo. Nesse caso, multimídia é representada pelos tipos de mídia de áudio e de vídeo.

Outro importante requerimento, que é um componente chave para o IMS, é a negociação da qualidade de serviço – QoS (*Quality of Service*).

A QoS para uma sessão particular é determinado por uma série de fatores, como a largura máxima de banda que pode ser alocada ao usuário, que pode estar baseado no seu tipo de contrato com a operadora ou baseado no estado corrente da rede como um todo.

O IMS permite a operadora controlar a QoS do usuário. Com isso, a operadora pode diferenciar certos grupos de usuário e com isso aplicar políticas de acesso e tarifação.

Um terceiro requisito é a interoperabilidade com a i*nternet* e as redes de comutação por circuitos.

Dado que a i*nternet* possibilita acessos a conteúdo multimídia, esse se torna um requisito natural para as sessões IMS, pois a quantidade de fontes e destinos de sessões multimídia é potencialmente expandida pela i*nternet[3]*.

Já a interoperabilidade com as redes de comutação por circuito (redes de telefonia fixa, redes celulares de 1a e 2a geração) é um requisito necessário para garantir a comunicação entre a rede IMS e as redes legadas.

O suporte a um controle rígido de acesso aos serviços entregues ao usuário final, necessário às operadoras, é um requisito que pode ser dividido em duas categorias.

A primeira diz respeito a regras ou políticas genéricas, que são aplicadas a todos os usuários da rede.

Por exemplo, a operadora pode querer restringir o uso de *codecs* de áudio que utilizem uma grande largura de banda, como o G.711 [3] que utiliza 64 kbps, com o intuito de otimizar a utilização de recursos na rede de acesso.

A outra categoria diz respeito a regras ou políticas que são aplicadas a cada usuário. Nesse caso, as regras são baseadas nos serviços contratados pelo usuário.

Por exemplo, o usuário pode ter uma assinatura com acesso a serviços IMS que não incluem o uso de vídeo, embora o seu terminal tenha essa facilidade.

No caso do usuário tentar iniciar uma sessão multimídia que inclua suporte a vídeo, a operadora pode impedir que a sessão se estabelecesse baseada nessas regras.

Outro requisito definido é o suporte a implementação rápida de novos serviços, de que tem um forte impacto na definição da arquitetura do IMS[3]. Atualmente, a padronização de serviços e os testes de interoperabilidade despendem uma grande quantidade de tempo.

Como o objetivo é reduzir esse tempo para a introdução de um novo serviço, o IMS viabiliza as facilidades para a introdução de novos serviços.

Outros dois requisitos são o suporte ao *roaming* (utilização de uma rede visitada quando em viagem), requisito básico desde as redes 2G, e acesso a rede IMS a partir de outras redes que não a rede GPRS. Isso porque o 3GPP foi um projeto criado para desenvolver soluções para a evolução da rede GSM, e por isso focou no acesso GPRS para a primeira versão de IMS [4].

As futuras versões do 3GPP já estudam outros tipos de acesso a rede de pacotes, como o WLAN (*Wireless Local Area Network*).

2.1. Considerações Gerais sobre a Arquitetura IMS

O IMS é um conjunto de especificações que descrevem a arquitetura NGN (*Next Generation Network*) para implementação de serviços de telefonia e multimídia baseado em IP [41].

IMS define uma arquitetura completa e *framework* que habilita a convergência de voz, dados, vídeo e tecnologia de rede móvel através de uma infraestrutura baseada em IP.

Além do que preenche a distância entre os dois paradigmas de comunicação mais bem sucedidos, celular e tecnologia IP [41].

A visão para o IMS é que os usuários possam navegar na *web*, jogar on-line ou simplesmete entrar numa videoconferência independente do lugar onde você se encontra usando seu dispositivo 3G [41].

Portanto a visão do IMS seria fornecer acesso celular para todos os serviços que dispõem de i*nternet*.

O IMS é uma arquitetura funcional de rede que é vista como uma solução promissora, na medida em que facilita a criação e o desenvolvimento de serviços multimídia [3], assim como o suporte a interoperabilidade e a convergência de rede.

O protocolo SIP foi considerado a escolha natural de integração com o mundo IP, devido à sua evolução e sua flexibilidade. Esse protocolo foi selecionado pela 3GPP (*Third Generation Partnership Project*) como o principal componente do IMS para o *core* da rede UMTS.

O 3GPP surgiu para evoluir as especificações do GSM para a terceira geração do sistema de telefonia celular.

O 3GPP2 foi criado com o ituito de evoluir as redes celulares Norte-Americanas e Asiáticas baseadas nos padrões ANSI/TIA/EIA-41, com acesso radio CDMA2000 para o sistema de terceira geração.

Tanto o 3GPP e 3GPP2 têm suas próprias definições de IMS (tanto arquitetura quanto serviços básicos) e, no entanto, são bastante similares entre si.

Uma semelhança importante entre o IMS definido pelo 3GPP e o IMS definido pelo 3GPP2 é que ambos utilizam os protocolos de i*nternet*, tradicionalmente padronizados pelo IETF (*Internet Engineergin Task Force*), também é o IETF que define os padrões para o protocolo SIP.

O OMA (*Open Mobile Alliance*) tem a função de definir os serviços que serão disponibilizados sobre o IMS.

Enquanto o 3GPP e o 3GPP2 padronizam alguns dos serviços, como chamadas básicas de vídeo ou conferência, o foco do OMA é a padronização de habilitadores de serviços sobre a rede IMS (outros organimos de padronização podem desenvolver esse tipo de atividade para o IMS)

A arquitetura IMS inicialmente foi desenvolvida para aplicação em redes móveis 3G, a arquitetura de rede definida no 3GPP R5 e 3GPP2 [3] está gerando interesse também em operadoras de rede fixa.

Essa arquitetura é vista como o caminho para implementação de redes de nova geração NGN. Destacaremos dois elementos nessa arquitetura [17]:

• O protocolo SIP que aqui atuaria como um agente de comunicação entre os elementos principais desta rede;

• *Soft switch* (SS), com importante função de controle;

A arquitetura IMS propõe-se a fornecer uma série de vantagens [2,13], fala-se muito sobre a diminuição de custos na operação das redes, dada a convergência de voz, dados, móvel e fixo.

Entretanto aqui iremos mencionar um dos maiores benefícios da arquitetura IMS: a possibilidade de se introduzir sofisticados serviços para os assinantes.

Com certeza, as redes atuais já permitem a disponibilização de vários serviços de valor agregado para os assinantes. Todavia têm-se algumas limitações como, por exemplo:

• Baixa interação entre plataformas de serviços. Por exemplo, é conveniente que se possam criar serviços diferenciados que combinem duas ou mais capacidades da rede (um serviço que utilize simultaneamente a informação de localização do usuário e sua disponibilidade e permita ainda simultaneamente uma conversação ou troca de arquivos);

• Baixa eficiência na administração de bases de dados. Freqüentemente, cada plataforma de serviços requer sua própria base de dados de assinantes para provisionamento. Obviamente essa não é uma maneira eficiente de se implementar e operar novos serviços.

Pois cada plataforma necessita de uma gerência única para o provisionamento de serviço, ocasionando um acréscimo de custo para novos serviços.

A Fig. 2.1 abaixo mostra uma representação simplificada da implementação de serviços em uma rede IMS.

Por exemplo, o serviço A pode utilizar a informação de presença do assinante (disponível na plataforma 1) e permitir ainda que uma sessão PTT (*Push to Talk*) ou PTS (*Push to Show*) ocorra simultaneamente (disponível na plataforma 2).

A arquitetura IMS fornece uma forma eficiente de se implementar esses novos serviços sofisticados [2]. Por exemplo, o HSS (*Home Subscriber System*) contém uma base de dados centralizada dos assinantes.

Essa base de dados pode ser acessada através de protocolos abertos pelas plataformas de serviços. O serviço C, por sua vez, pode utilizar outras capacidades da rede disponíveis nas plataformas 2 e 3.

A seguir, são discutidos os elementos de uma rede IMS e suas funções:

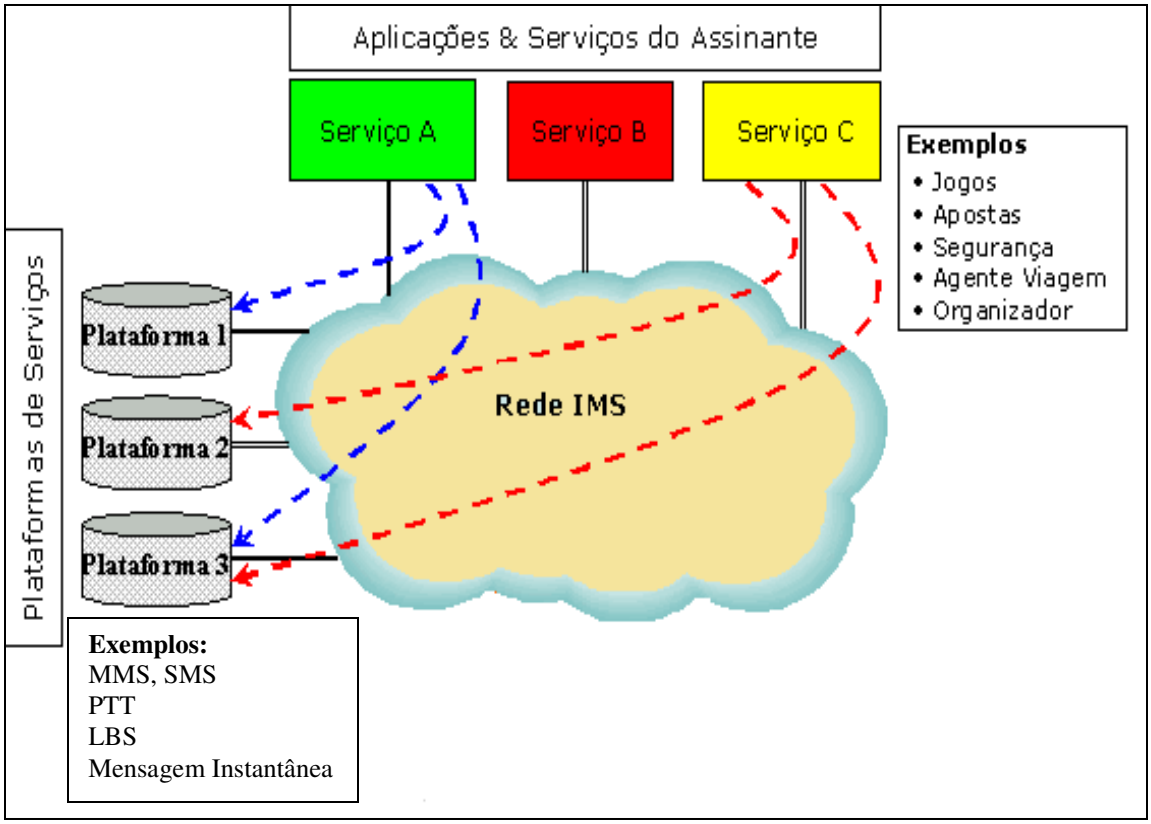

Fig. 2.1 - Implementação de serviços em uma rede IMS [3].

A arquitetura IMS se divide basicamente em três camadas:

• Camada de aplicações: contém as plataformas de serviços (PTT - *Push to Talk,* serviços de localização - LBS, serviços de mensagem curta e multimídia - SMS/MMS, plataforma de vídeo, etc.).

• Camada de controle: responsável pelo controle, incluindo estabelecimento das sessões. O *soft switch* é o elemento principal desta camada.

• Camada de acesso: meios de acesso, incluindo as interfaces *wireless* (cdma2000, UMTS/WCDMA e wifi), e interfaces cabeadas (ADSL).

Conforme mencionado, o SS (*Soft Switch*) possui um papel central na arquitetura IMS [17]. O SS contém as funções de servidor IMS, sendo responsável pelo controle da chamada/sessão provido pelo IMS na rede de origem do assinante (*home network*).

O SS gerencia as sessões IP, provê os serviços, coordena o controle da sessão com outros elementos da rede, e aloca recursos de mídia.

A seguir são descritas as funções e os componentes de um servidor IMS. Lembramos que as funções do servidor IMS são implementadas em uma *soft switch*.

Note que os elementos descritos a seguir representam entidades lógicas, podendo estar fisicamente implementados em uma mesma SS ou não. Em algumas situações, pode ser interessante a flexibilidade de implementação destas funcionalidades em SS diferentes.

Na Fig. 2.2 colocamos uma representação detalhada da arquitetura IMS, seus elementos e interfaces.

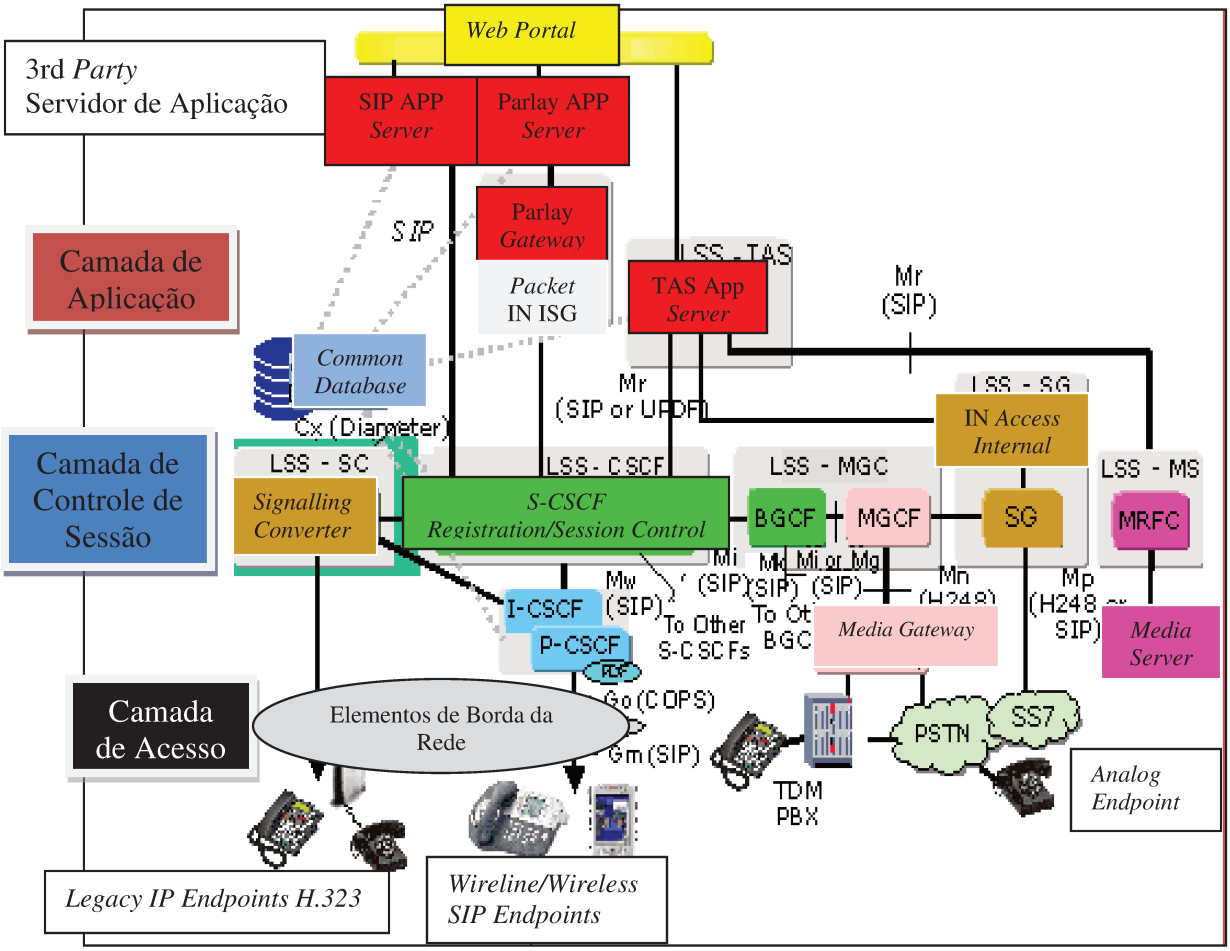

Fig. 2.2 – Componentes da rede IMS [13].

2.2. Motivadores

O IMS chegou com o intuito de revolucionar o modo como às aplicações multimídia são desenvolvidas e agora como elas vão invadir a tela dos celulares [41].

Para as operadoras, a sigla IMS significa a disponibilidade de ofertar mais serviços, para as fabricantes surge à oportunidade de vender para um setor que parecia saciado de produtos, porque embora muitos recursos multimídia já estejam disponíveis nos telefones móveis.

A arquitetura IMS permite que uma única aplicação funcione em todas as redes de acesso sem fio capacitado para IP, já que a arquitetura supera a necessidade de customizar cada aplicativo com uma tecnologia de acesso diferente.

Como o IMS é uma plataforma que controla serviços multimídia, que combina recursos *real-time*, como voz e vídeo-telefonia, com serviços *non-real time*.

Independentemente da tecnologia de rádio empregada e as aplicações construídas sobre IMS são portáveis e podem viajar com os assinantes para qualquer região.

O IMS garante a oferta de soluções convergentes de voz, dados e vídeo, com isso diversos fornecedores de conteúdo podem produzir opções variadas que se integrem às redes das operadoras.

De fato, o IMS carrega vantagens como velocidade na criação de serviços multimídia que envolvem áudio e vídeo.

Por exemplo, considerando que as operadoras de serviço móveis poderão adotar o IMS como "*hub*" e possibilitar que criadores de conteúdo e aplicativos se conectem a plataforma para acelerar o *time-to-market* de novos serviços sem fio.

Aliás, esse seria o principal atrativo da arquitetura IMS, acelerar o *time-to-market* no desenvolvimento e disponibilização de novos serviços, termo que ser torna bastante atrativo devido à acirrada competição pela qual passam as operadoras e os fabricantes.

O IMS apontava para as redes das operadoras móveis com o objetivo de disponibilizar um método rápido no desenvolvimento de novos serviços para competir com os provedores de conteúdos.

O IMS, porém, mostrou-se muito eficaz em exercer a função que ainda não estava completamente definida pelo *core*.

Apresentando um controle consistente e capaz de fazer a intermediação entre os diversos acessos e aplicações para que o propósito da convergência se tornasse uma realidade factível [2,3].

Assim, seria possível disponibilizar todos os serviços aos usuários independentemente do meio de acesso.

Consolidando a característica da horizontalização das redes aos serviços e, conseqüentemente, possibilitando/acirrando a competitividade entre as operadoras de telecomunicações fixa e móvel, e os provedores de serviços de i*nternet*.

Seriam empregados padrões da QoS, segurança e tarifação, e se disponibilizariam serviços multimídias integrados através de sua flexibilidade e rapidez para a criação e entrega de serviços.

Também seria possível abrir e compartilhar a opção de criação de serviços para terceiros, que muitas vezes são aqueles que de fato possuem os conhecimentos e a experiência no desenvolvimento.

Contudo ainda permitindo o controle sob esses desenvolvimentos e assim provendo serviços ubíquos e uniformes.

Além dos novos serviços o IMS também fornece a base de sustentação para sobreposição das redes legadas, ou seja, possibilitando o total provimento dos serviços existentes.

Assim cumprindo com todos os requisitos de qualidade exigidos pelos órgãos regulamentadores e também disponibilizando o acesso aos serviços públicos emergenciais.

Um dos princípios básicos motivadores para o uso do IMS, é que o IMS é uma arquitetura end-to-end que deve suportar vários tipos de equipamentos, a entrega do serviço deveria ser independente da tecnologia de acesso.

Assim, o uso do IP aberto é especificado no IMS para uma melhor interoperabilidade, o IMS suporta *roaming* entre diferentes redes.

O IMS é uma arquitetura horizontal: possui um conjunto de funções comuns chamadas *service enablers* [1] que podem ser usadas por diversos serviços, isso simplifica e agiliza a implementação de serviço, além do que permite a interação entre diversos serviços.

Motivações técnicas e de negócios: O desenvolvimento mais rápido de serviços na plataforma IMS deveria reduzir o *time-to-market* no desenvolvimento de aplicativos e serviços, além do que estimular a inovação.

A combinação de vários serviços numa única sessão, um único sinal e tarifação unificada são atrativos que devem atrair e despertar o interesse dos usuários.

Na arquitetura IMS a operadora está ciente do serviço atual que o cliente está usando, assim a operadora pode desenvolver um esquema de tarifação mais apropriado.

Com a arquitetura IMS disponibilizando uma platforma de desenvolvimento uniforme, reduzirá o custo das operadoras no desenvolvimento de novos serviços, permitindo uma redução substancial de custo na infraestrutura e gerenciamento da rede.

Como exemplo de alguns serviços que futuramente poderão ser disponibilizados nas redes IMS podemos citar, o PoC (*Push to Talk over Cellular*), IM (*Instant Messaging*), jogos no celular ou a combinação de alguns serviços já existentes (por exemplo IM e jogos multiplayer).

[1] *Service enablers* são definidos a fim de expor a funcionalidade de rede para prestadores de serviços externos.

2.3. Benefícios da Arquitetura IMS

A princípio surge a idéia da real necessidade do IMS, visto que já estamos familiarizados em acessar serviços da i*nternet* como *web*, *email* ou *instant messaging* via rede 2.5G ou 3G.

Contudo as vantagens do IMS sobre as atuais infraestruturas de rede celular podem ser observadas em alguns aspectos [41]:

•IMS oferece uma plataforma comum para reduzir o "*time-to-market*" para o desenvolvimento de novos serviços de multimídia: Um dos maiores desafios dos serviços de comunicações atualmente é a redução do tempo e do custo de processo para criação de novos serviços.

Os provedores de serviço estão procurando meios de reduzir o *time-to-market* para o desenvolvimento de novos serviços de multimídia, a infraestrutura IMS resolve esse problema providenciando uma plataforma padronizada e componentes reusáveis.

• IMS disponibiliza serviços multimídia com viabilização da QoS (*Quality of Service*) : Um dos grandes problemas das redes 3G é a qualidade de serviço.

As rede celulares 3G providenciam o '*best effort´* [15][2], que significa dizer que a rede fará o melhor para garantir a largura de banda requerida.

Entretanto não há garantia que permanecerá no mesmo nível, o que significa que a banda de uma particular conexão pode variar significativamente através do tempo.

Para resolver esse problema, o mecanismo da QoS foi desenvolvido no sentido de providenciar certo nível de garantia de banda de rede durante a transmissão, ao invés de apenas fazer o *´best effort´*.

O IMS especifica a viabilização da qualidade de serviço através da rede IP e a vantagem do mecanismo da QoS para melhorar e garantir a qualidade da transmissão.

• IMS permite que todos os serviços estejam disponíveis independentes da localização do usuário: um dos maiores problemas das tecnologias celulares atuais é que alguns serviços não estão disponíveis quando os usuários estão em *roaming*.

O IMS usa tecnologias e protocolos da *internet* para permitir roaming dos usuários que continuam, dessa forma, podendo executar serviços que executariam em suas redes locais.

• IMS possibilita que as operadoras tarifem as sessões multimídias mais adequadamente:

Se um usuário usa videoconferência na rede 3G, há uma taxa de transferência de dados muito alta, que consiste de áudio e vídeo, o valor desse serviço acaba saindo muito caro, visto que a operadora tarifa pela quantidade de *bytes* transferidos.

---

[2] *Best effort* significando que a rede fará o melhor esforço para garantir a largura de banda.

Contudo, se a operadora fornecer outro tipo de tarifação baseado em outro esquema com o tipo de serviço atual o beneficiado passa a ser o usuário.

A vantagem do IMS nesse caso é que ele fornece informação sobre o tipo de serviço que o usuário está usando e, portanto permite que a operadora determine como tarifar o usuário baseado no serviço que ele está realmente acessando [3].

Por exemplo, a operadora pode escolher entre tarifar o usuário pelo número de *bytes* transferidos, pela duração da sessão, ou simplesmente desenvolver algum outro tipo de tarifação.

2.4. História e Padrão

O IMS foi definido em 1999 originalmente pelo 3GPP, que é um acordo de colaboração entre alguns órgãos de padrões das telecomunicações e responsável por promover os sistemas de comunicação móvel baseados em IP.

A arquitetura IMS foi incorporada na padronização das redes UMTS (*Universal Mobile Telecommunications System*) realizada pelo 3GPP na versão 5 em 2003, quando os serviços multimídia baseados em SIP também foram incluídos.

Portanto nessa versão o SIP foi escolhido como o principal protocolo para o IMS. Nessa versão foram apresentadas as seguintes definições:

• Arquitetura IMS com as entidades de rede e os pontos de referência (interfaces) entre essas entidades.

• Identidade de usuários públicos e privados, utilizando SIP-URI e TEL-URI, ISIM, e o USIM ao invés do ISIM.

• Controle dos serviços pelo IMS que incluí a invocação e controle dos servidores de aplicação baseado em "critérios de filtros" do CSCF (*Call Session Control Function*), utilização dos serviços CAMEL (*Customized Applications for Mobile networks using Enhanced Logic*), interconexão com o OSA-GW e utilização dos serviços OSA.

• Controle de sessão do IMS que incluí registro, roteamento de sessão, modificação de sessão e compressão de sinalização SIP.

• Mecanismos de segurança através de autenticação do usuário, proteção da integridade da mensagem e segurança do domínio da rede IMS.

• Mecanismos da QoS com pré-condições e autorização da QoS de mídia baseado no PDF (*Policy Decision Function*).

O grupo 3GPP2 (3rd *Generation Partnership Project* 2) responsável pela padronização do sistema CDMA (*Code Division Multiple Access*) criou uma arquitetura baseada no IMS, chamada

MMD (*Multimedia Domain*), que também oferece suporte as redes baseadas na tecnologia CDMA 2000.

Nas versões seguintes o 3GPP fez a adaptação do IMS para o "mundo real" e incluiu o suporte as redes WLAN (*Wireless Local Area Network*) (versão 6 em 2005), sendo que as principais características são:

• Interoperabilidade com a PSTN, SIP *endpoints* da *internet* e acessos WLAN.

• Controle de sessão pelo IMS com suporte a múltiplos registros e roteamento por grupos de identidade.

• Mecanismos de segurança com proteção confidencial das mensagens SIP, utilização de chave pública de infraestrutura e interface Ut de segurança.

• Serviços de presença, mensagem instantânea, conferência e gerenciamento em grupo.

Já a versão 7 (2007) trata do suporte às redes fixas, com as seguintes características:

• Acesso por redes all-IP (DSL, WLAN, etc.).

Chamadas de emergência com funções para identificação, coleta de informações e rastreamento do usuário.

• QoS fim-a-fim provendo vários cenários e mecanismos para gerenciar e garantir a qualidade necessária.

• Evolução do controle de policiamento e bilhetagem adicionando aos perfis dos usuários as políticas de controle.

• Definição de protocolos para algumas interfaces (Mp, Go, Gx, etc.).

O IMS é uma arquitetura NGN que permite as operadoras de telefonia oferecer serviços multimídia, contudo como já foi descrito anteriormente reconhece-se que o IMS surgiu com o objetivo de integrar os serviços de telefonia celular tradicional e a tecnologia de *internet*.

Entretanto a arquitetura IMS é fundamental tanto para as operadoras de rede móvel como os operadores de rede fixa que quiserem oferecer serviços multimídia baseados nesse padrão.

Dessa forma, a arquitetura IMS é capaz de suportar os sistemas atuais de telefonia, baseados em comutação por circuito, como também os sistemas baseados em comutação de pacotes.

A arquitetura IMS utiliza um grande número de padrões e também protocolos que são especificados por diferentes grupos e órgãos como:

3GPP e 3GPP2 – Tem trabalhado em conjunto na definição do IMS/MMD.

IETF (*Internet Engineering Task Force*) – responsável pela definição de vários protocolos do IMS, entre eles os protocolos SIP e SDP.

ANSI – responsável por alguns protocolos utilizados pelo IMS para permitir a integração com o sistema legado, entre eles o T1.679 que permite a integração entre a sinalização ANSI ISUP e SIP.

ITU-T – padronizou os protocolos H.248 e Q.1912. SIP responsáveis pelo controle de mídia e pela integração entre ITU-T ISUP e SIP, respectivamente.

Parlay – promotor e especificador do "*Open Service Architecture*" (OSA), arquitetura para desenvolvimento de serviços e aplicações.

É importante ressaltar que o IMS não padroniza serviços específicos e sim *enablers* permitindo o acesso às diversas funcionalidades presentes nos AS através dos *filter criteria*.

Que disparam essas diversas funcionalidades para fazer a orquestração de um serviço de acordo com as necessidades de mercado do momento.

2.5. Protocolos Usados no IMS

A maioria dos protocolos usados no IMS é padronizada pelo IETF, a seguir a descrição dos principais:

2.5.1. Sinalização e *Media Flow*:

Os principais protocolos envolvidos na sinalização do IMS são o SS7, Sigtran e o SIP.

2.5.1.1. Pilha de Protocolos SS7

O SS7 é uma pilha de protocolos de sinalização, cuja tecnologia está completamente inserida no mundo das redes fixas de telecomunicações e continuará a ser a tecnologia predominante por muitos anos. Sua complexidade deriva de três grandes fontes:

• Trata-se de um apanhado de padrões e variações específicas por país.

Por exemplo: ITU-T (*International Telecommunication Union, Standardization Sector*), ANSI (*American National Standards Institute*), ETSI (*European Telecommunications Standards Institute*), NTT Group, JTT e Telcordia Technologies Inc. definiram as especificações SS7 e existem diferentes implementações em várias partes do mundo.

• O SS7 faz uso de subprotocolos em múltiplos níveis – essencialmente existem vários protocolos de transporte da sinalização, outros para compor e analisar essa sinalização, outros

para organizar as transações baseado nas mensagens sinalizadas e ainda outros para manipular aplicações de rede, como ISDN ou AIN (*Advanced Intelligent Network*).

Esses podem ser combinados em vários protocolos, por exemplo, INAP/TCAP/SCCP/MTP3 para AIN; ISUP/MTP3 para ISDN; BICC para infraestrutura wireless (HLR e *softswitches*); BB/NB-Networking/B-ISUP/MTP3-B para banda-larga.

• Complexidade de uma integração com o ATM[3], uma vez que o ATM foi visto como a banda larga de camada 2 quando o SS7 foi estendido na década de 80.

Isso causou mudanças adicionais no protocolo, outros foram desenvolvidos e diferentes tipos de *hardware* foram utilizados do que os em uso nas aplicações de banda estreita.

Ainda assim, as operadoras precisam aproveitar os benefícios do transporte IP enquanto mantém serviços baseados em SS7. Isso leva ao Sigtran.

2.5.1.2. SIGTRAN

O Sigtran é um conjunto de protocolos capaz de encapsular a sinalização SS7 e transportá-la sobre IP. Sua estrutura básica está representada na Fig. 2.3 e pode ser observada como o padrão quadriculado em diagonal.

Os blocos SS7 que o Sigtran transporta estão representados no padrão quadriculado vertical.

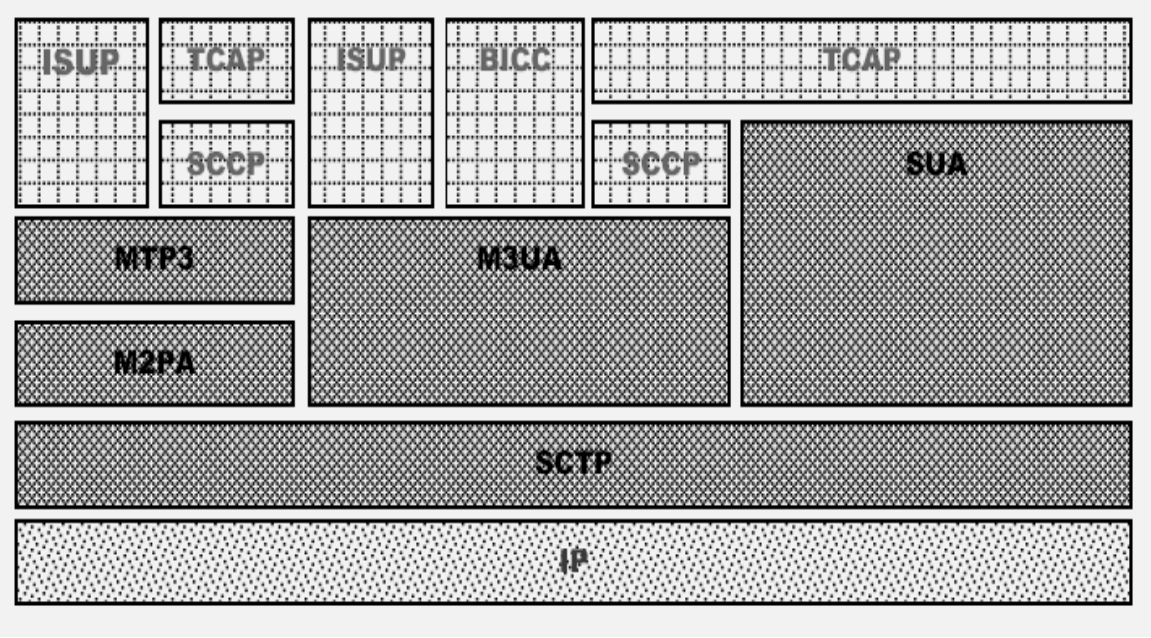

Fig. 2.3 - Protocolo SIGTRAN [13].

[3] ATM (*Asynchronous Transfer Mode*) é uma técnica de comutação padrão, concebida para unificar as redes de telecomunicações e informática.

Trabalhando sobre o protocolo da camada de transporte IP, o Sigtran atende aos seguintes protocolos:

• SCTP (*Stream Control Transmission Protocol*) – protocolo de transporte confiável operando sobre uma rede de pacotes sem conexão como IP, desenvolvido para eliminar as deficiências do TCP.

• M2PA (*MTP2-User Peer-to-Peer Adaptation Layer*) – protocolo MTP3 (protocolo de transporte de mensagens no SS7) com MTP2 (outro protocolo de transporte de mensagens do SS7) equivalente a serviços sobre IP usando serviços do SCTP.

É utilizado tipicamente na infraestrutura entre os elementos da rede e a camada de controle, como entre os STP (*Session Transfer Point*).

• M3UA (*MTP3-User Adaptation Layer*) – projetado para *gateways* de sinalização que habilitam interconexão suave entre os domínios IP e SS7.

Esse protocolo suporta o transporte de qualquer SS7 sinalização de usuário MTP3 (ISUP, SCCP) sobre IP através do uso de serviços do SCTP.

• SUA (*SCCP-User Adaptation Layer*) – suporta o transporte de sinalização do usuário SCTP. Um uso típico é o acesso ao centro de comutação móvel.

A Fig. 2.4 abaixo mostra como o SIGTAN trabalha na transição para redes baseadas em IP.

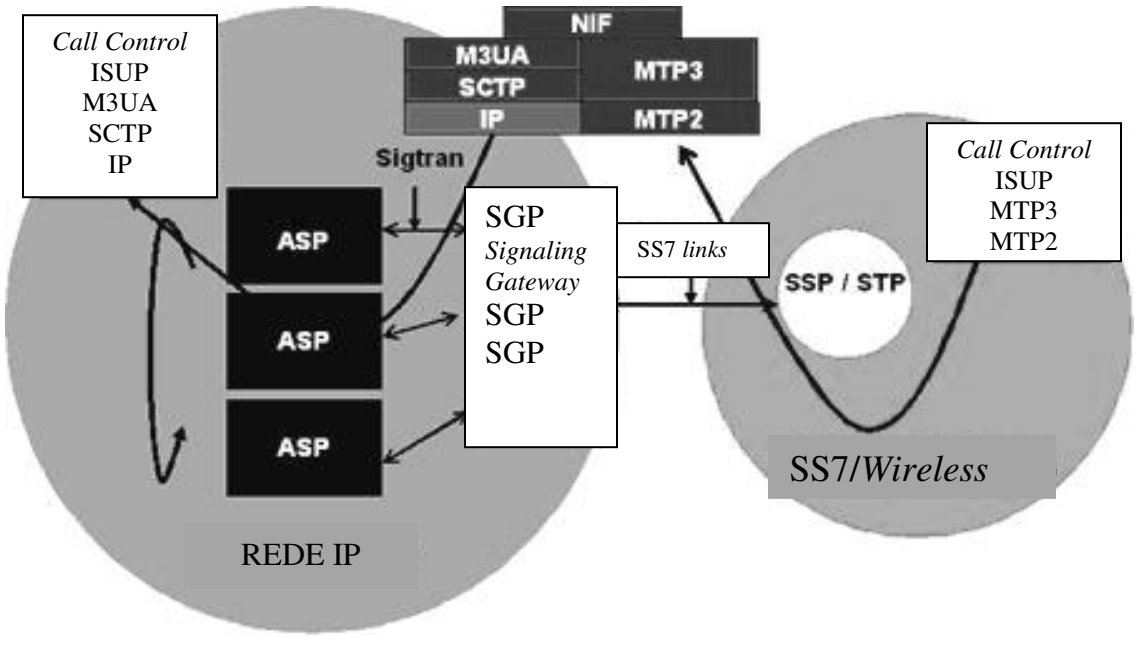

Fig. 2.4 - Como o SIGTRAN facilita a transição em redes baseadas em IP [13].

Na Fig. 2.4, o círculo SS7/*wireless* ilustra a rede tradicional de circuito comutado baseada em SS7/*wireless* PSTN, onde o controle da chamada é provido pelo padrão ISUP/MPT3/MPT2 do protocolo SS7.

A função de *gateway* de sinalização está no meio e a rede SS7-*over*-IP (SS7oIP) essa à esquerda.

O *gateway* de sinalização alimenta as informações baseadas em SS7 de um lado e usa a função de interconexão (NIF) para traduzir o SS7 no Sigtran.

Finalmente o *gateway* de sinalização se comunica com Sigtran nos processadores de servidores de aplicação (ASPs), que emulam a função do SSP/STP para uma faixa específica de chamadas, na rede IP à esquerda da Fig. 2.4.

A Fig. 2.5 mostra como uma rede completa de sinalização SS7oIP deve ser implementada. A infraestrutura IP já estará preparada para a evolução do SS7 para SIP durante a migração gradual para o IMS.

Uma vez que o M2PA está pronto no núcleo da rede de sinalização, as portadoras podem introduzir o MTP3 para links com conectividade entre os STPs e os *endpoints*.

No lado direito da figura estão representados os STPs IP que provêm função de tradução e aplicações. No lado esquerdo são exibidos os *end-points* IP, incluindo os dispositivos de próxima geração e 3G.

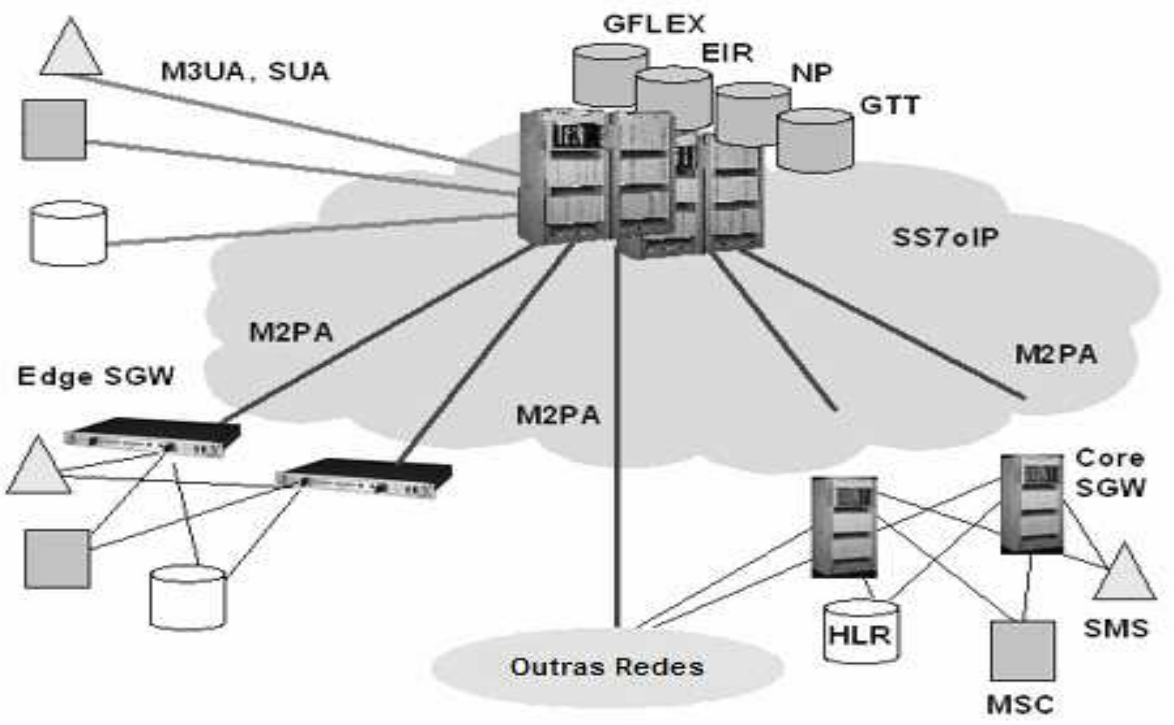

Fig. 2.5 - Rede de sinalização completa para o SS7-*Over*-IP [14].

2.5.1.3. SIP – *Session Initiation Protocol*

O principal protocolo de sinalização usado no IMS é o SIP (*Session Initiation Protocol*).

O SIP possui alguns dos princípios do HTTP e SMTP, os dois protocolos mais famosos da i*nternet*, o SIP foi selecionado no IMS principalmente porque ele atende os requisitos dessa arquitetura e é considerado um protocolo flexível e seguro.

O IMS SIP é uma versão adicionada do SIP incluindo muitas extensões como descrito no padrão 3GPP TS 24.229. O principal propósito do SIP é o estabelecimento, modificação e terminação de sessões multimídia entre dois terminais.

O corpo das mensagens SIP é descrito usando o SDP (*Session Description Protocol*), o SDP é uma sintaxe descrevendo *media flows* (*address, port, media type, encoding*, etc).

SIP acaba se tornando o protocolo chave da arquitetura IMS, além do já descrito no IMS o SIP trata o gerenciamento de subscrições, controle de serviço, autorização da QoS, tarifação, gerenciamento de recursos, etc.

2.5.2. Autenticação, Autorização e *Accounting*

O *diameter* é um protocolo recente de autenticação, autorização e *accounting* substituindo o protocolo RADIUS, ele é definido no RFC 3588.

O diameter é usado no *framework* de serviço do IMS pelo I-CSCF, S-CSCF e os servidores de aplicação nas trocas com o HSS contendo os perfis dos usuários, ele também é usado nas trocas entre o RACS e o AS e CLF.

2.5.3. Protocolos Adicionais

MeGaCo, também conhecido como H248, é o sucessor do MGCP (*Media Gateway Control Protocol*) usado para funções de controle dos *media serving* no ambiente IMS, ele é especificado no RFC 3015.

O RTP (*Real Time Protocol*) providencia funcionalidade de transporte para trasmissão de dados em tempo real, ele é especificado no RFC 3350.

Ele é usado em conjunto com um protocolo de controle chamado RTCP (*Real Time control Protocol*) para habilitar o monitoramento dos dados entregues e para providenciar o mínimo de controle e identificação das funcionalidades.

O uso do IPv6 nas redes IMS é mandatório, de acordo com a release 5 do 3GPP, mais muitos fabricantes implementam tanto o IPv4 quanto o IPv6.

2.6. Arquiterura IMS

A arquitetura IMS foi estabelecida sobre três camadas que podem evoluir independentemente, conforme representado na Fig. 2.6 abaixo, camada de aplicações e serviços, camada de controle e camada de conectividade.

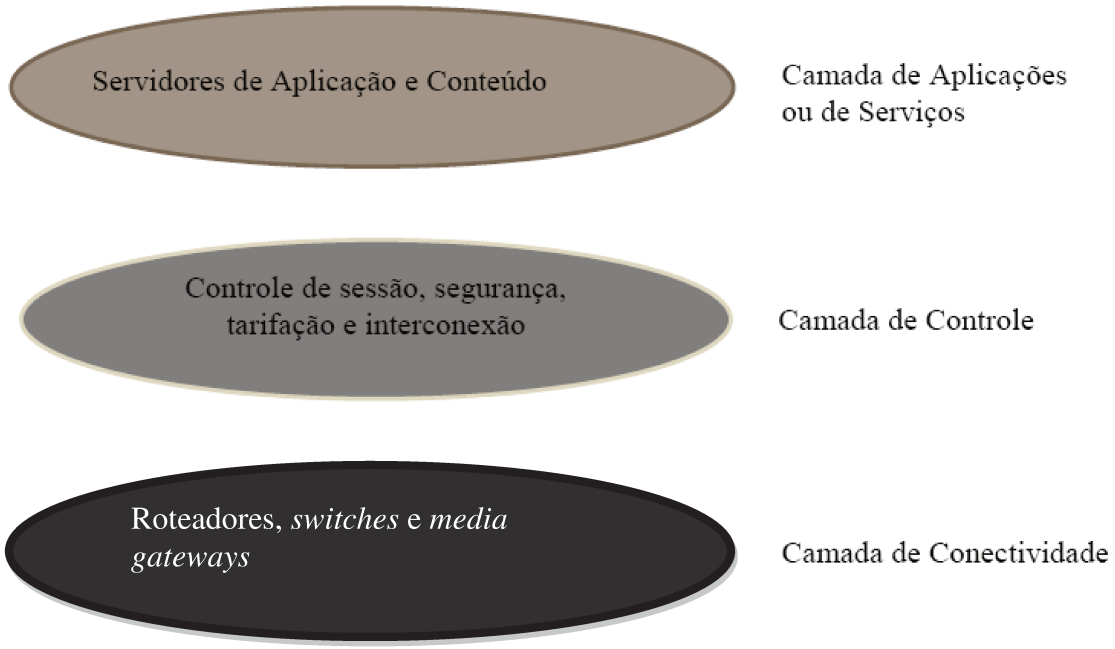

Fig. 2.6 - Arquitetura de camadas do IMS [14].

• Camada de aplicações: essa camada contém os servidores de aplicação e de conteúdo, que executam os serviços de valor adicionado para o usuário final.

• Camada de controle: essa camada contém os servidores de controle de rede, capazes de gerenciar as chamadas ou o início das sessões, as modificações e as atualizações.

Os servidores de controle podem ainda manipular funções como gerenciamento da mobilidade, sergurança, tarifação e interconexão com redes externas.

• Camada de conectividade: nessa camada estão presentes os roteadores, *switches* e outros nós que transportam os dados de usuário. Os roteadores e *switches* provêm funcionalidades de transporte tanto para a camada de controle quanto para a camada de tráfego de usuários.

O conceito de arquitetura em camadas também define uma arquitetura horizontal, onde as funções de rede comuns podem ser reutilizadas para múltiplas aplicações.

Essa arquitetura horizontal no IMS também especifica a interoperabilidade e o *roaming*, bem como provê controle de propriedade, de segurança e de tarifação, conforme ilustra a Fig. 2.7.

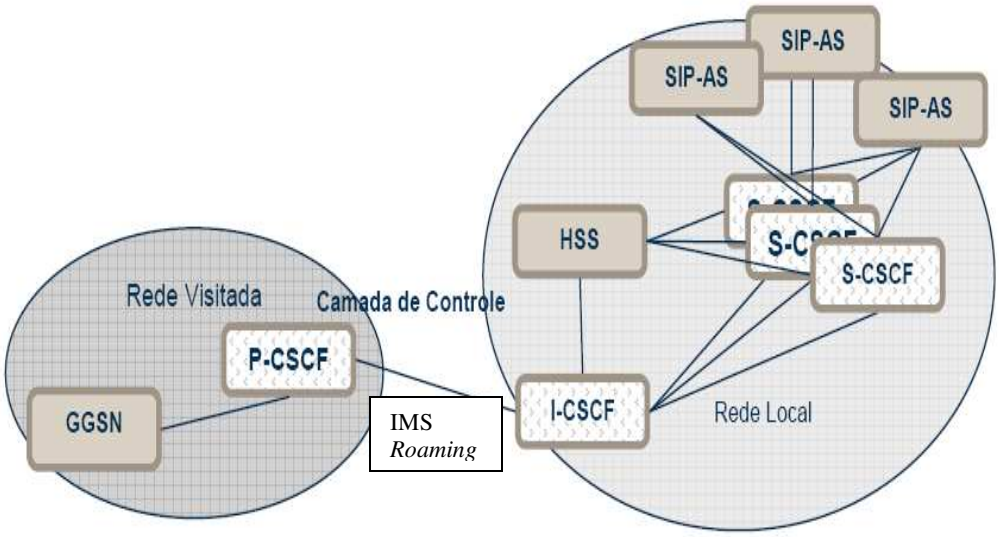

Fig. 2.7 - Camada de controle possibilita a arquitetura horizontal [14].

A Fig. 2.7 apresenta uma visão geral da camada de controle da arquitetura IMS, destacando os elementos de rede essenciais para prover serviços multimídia em tempo-real.

O IMS não depende do domínio de comutação de circuitos, uma vez que confia no domínio de comutação de pacotes para gerência de transporte e mobilidade local.

O CSCF (*Call State Control Functions*) e o HSS (*Home Subscriber Server*) são os elementos chave dessa arquitetura. Estão envolvidos essencialmente no processamento de mensagens para controle de sessões de voz e multimídia.

Adicionalmente, o CSCF ainda se envolve com tradução de endereçamento, comutação de serviços e negociação de sinal, além de gerenciar o perfil do usuário.

O CSCF pode ser categorizado de acordo com as necessidades dos cenários onde será configurado, mais detalhes sobre cada um destes elementos estão descritos nas próximas seções.

O 3GPP não padroniza os nós, mas sim funcionalidades. Isso significa que a arquitetura IMS, assim como a NGN, é uma coleção de funções interligadas por interfaces padrões.

Os fabricantes são livres para combinar duas ou mais funções em um único nó (por exemplo, em uma única caixa física), similarmente podem dividir uma única função em dois ou mais nós.

Em geral, a maioria dos fabricantes segue de perto a arquitetura IMS e implementa cada função em um único nó.

A Fig. 2.8 mostra uma visão geral da arquitetura IMS definida pelo 3GPP. Na figura não estão incluídas todas as interfaces do IMS, somente algumas mais importantes como as interfaces de sinalização.

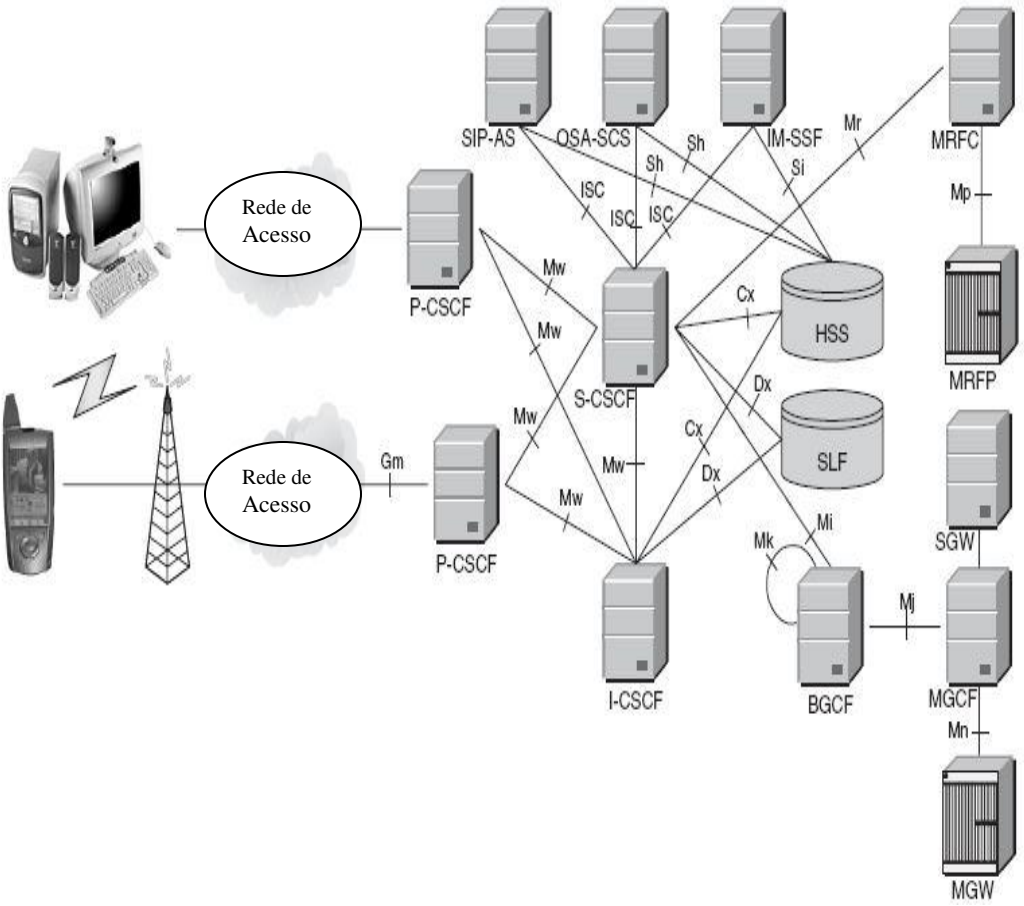

Fig. 2.8 - Visão geral da arquitetura IMS do 3GPP [14].

Além do acesso via rádio o IMS suporta outros tipos de dispositivos e de acessos. PDA's e computadores são exemplos dos dispositivos que podem conectar o IMS. Os exemplos de acessos alternativos são WLAN, ADSL, DSL ou Wimax [46].

Vemos na figura os nós incluídos no subsistema também chamado de *IP Multimedia Core Network Subsystem*. Esses nós são [46]:

• Uma ou mais bases de dados do usuário, chamadas de HSS (*Home Subscriber Servers*) e SLF (*Subscritor Location Functions*).

• Um ou mais SIP servers, conhecido coletivamente como CSCF's (*Call/Session Control Functions*).

• Um ou mais AS's (*Application Servers*).

• Um ou mais MRF's (*Media Resource Functions*), divididos entre o MRFC (*Media Resource Function Controllers*) e o MRFP (*Media Resource Function Processors*).

• Um ou mais BGCF's (*Breakout Gateway Control Functions*).

• Um ou mais *gateways* de conexão com a rede de telefonia fixa (PSTN – *Public Switched Telephone Network*) ou móvel convencional de comutação por circuitos (PLMN - *Public Land Mobile Network*), decompostos em: *gateway* de sinalização (SGW - *Signaling Gateway*), *gateway* de controle de mídia (MGCF – *Media Gateway Controller Function*) e *gateway* de mídia (MGW - *Media Gateway*);

A Fig. 2.8 também não faz referência às funções de tarifação. Esses elementos terão suas funções detalhadas a seguir.

2.6.1. Bases de Dados HSS e SLF

O HSS é um repositório central de informações de usuário. Tecnicamente, o HSS é uma evolução do nó HLR (*Home Location Register*) da rede GSM. O HSS contém todos os dados de subscrição relacionados ao usuário necessários para manipular sessões multimídia.

Esses dados incluem, entre outros itens, informações de localização, informações de segurança (incluindo ambas as informações de autenticação e autorização), informações de perfil do usuário (incluindo os serviços que o usuário tem assinado ou tem acesso) e o S-CSCF (*Serving*-CSCF) alocado ao usuário em seu registro.

O HSS também é responsável por suportar o controle de chamadas e as entidades de gerenciamento de sessão dos diferentes domínios e subsistemas (de comutação por circuitos e comutação por pacotes e IMS) de uma operadora de telecomunicações como mostra a Fig. 2.9. Além do que, o HSS armazena dados de aplicação, como por exemplo o SMS, podendo dessa forma recuperar um SMS.

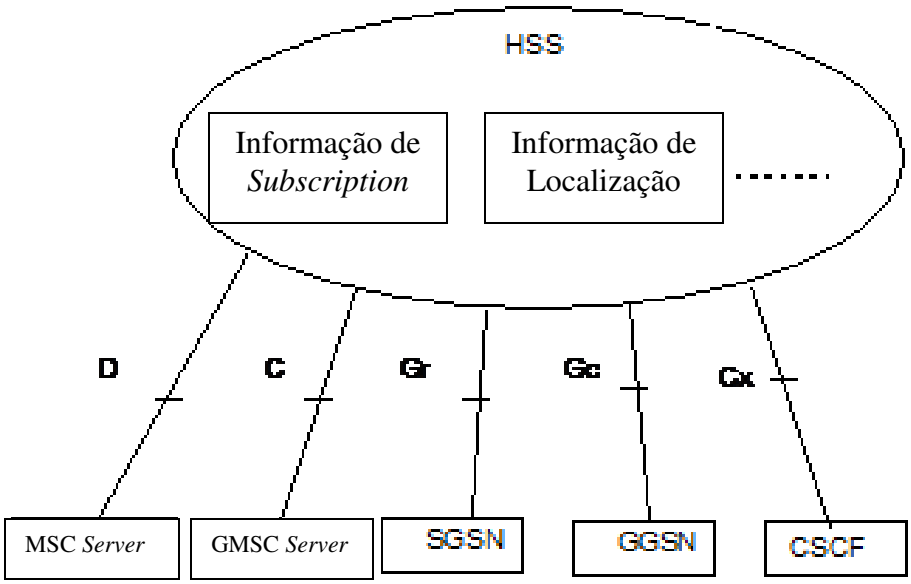

Fig. 2.9 - Exemplo de estrutura do HSS e as interfaces básicas [17].

O HSS pode combinar informações heterogêneas, e habilitar facilidades avançadas no núcleo da rede para serem oferecidas para o domínio de aplicações e serviços, ao mesmo tempo em que pode esconder essa heterogeneidade.

O HSS consiste das seguintes funcionalidades:

• Funcionalidades de multimídia IP para prover suporte para as funções de controle do subsistema Multimídia IP, como os CSCF. Isso é necessário para disponibilizar para o assinante o uso dos serviços da rede IMS. A funcionalidade de multimídia IP é independente da rede de acesso utilizada para acessar o núcleo da rede IMS;

• Funcionalidade de HLR/AuC (*Authentication Centre*) requerida pelo domínio de comutação por pacotes;

• Funcionalidade de HLR/AuC requerida pelo domínio de comutação por circuitos, se a operadora desejar habilitar o assinante para acesso ao domínio de comutação por circuitos ou para suportar assinantes visitantes da rede legada de comutação por circuitos GSM.

Uma rede IMS pode conter mais de um HSS, para o caso de haver muitos assinantes a serem gerenciados por um único HSS. De qualquer forma, todos os dados relacionados a um assinantes são armazenados em um único HSS.

As redes com somente um HSS não necessitam da função de localização de assinante (SLF). Por outro lado, redes com mais de um HSS requerem um SLF. O SLF é uma base de dados simples que mapeia endereços de usuários e seu respectivo HSS.

Assim, um nó que consulta o SLF tendo como entrada o endereço do assinante, obtém como resposta o HSS que contém todas as informações relacionadas àquele usuário.

O SLF é consultado pelo I-CSCF o processo de registro e de estabelecimento de sessão para buscar o HSS que contém os dados do assinante.

Além disso, o SLF também é consultado pelo S-CSCF no processo de registro. O SLF é acessado via interface Dx. Ambos HSS e SLF implementam o protocolo *diameter*, através de uma aplicação *diameter* especifica para o IMS.

2.6.2. Funções Lógicas do HSS

A Fig. 2.10 apresenta uma visão macro das funcionalidades de um HSS. De forma genérica pode-se descrever essas funcionalidades como:

• Gerenciamento de mobilidade: essa função suporta a mobilidade do usuário tanto no domínio de comutação por circuitos quanto a comutação por pacotes ou no domínio do subsistema IMS;

• Suporte ao estabelecimento de chamada/sessão: o HSS suporta os procedimentos de estabelecimento de chamada/sessão seja no domínio de comutação por circuitos, comutação por pacotes ou no subsistema de rede IMS. Para o tráfego terminado, o HSS provê informação sobre qual elemento de rede controla a chamada e/ou sessão;

• Geração de informação de segurança do usuário: o HSS gera autenticação de usuário, dados de integridade e cifragem para os domínios de comutação por circuitos e por pacotes e para o subsistema IMS;

• Suporte a segurança do usuário: O HSS suporta os procedimentos de autenticação para acesso aos serviços nos domínios de comutação por circuitos e por pacotes e no subsistema IMS. Através do armazenamento dos dados gerados de autenticação, integridade e cifragem e provendo essas informações para o elemento apropriado do núcleo da rede, ou seja, MSC, SGSN ou CSCF, ao qual está conectado o usuário;

• Gerenciamento de identificação do usuário: o HSS fornece o relacionamento apropriado entre todos os identificadores que unicamente determinam o usuário em cada sistema: IMSI (*International Mobile Subscriber Identity*) e MSISDN (*Mobile Subscriber ISDN - Integrated Services Digital Network*) para o domínio de comutação por circuitos, IMSI e MSISDN. E

endereço IP para o domínio de comutação por pacotes e Identidades Privada e Publicas para o subsistema de rede IMS;

• Autorização de acesso: quando os elementos de rede (MSC/VLR, SGSN ou CSCF) solicitam acesso à rede móvel, o HSS verifica se o usuário possui permissão para visitar aquela rede;

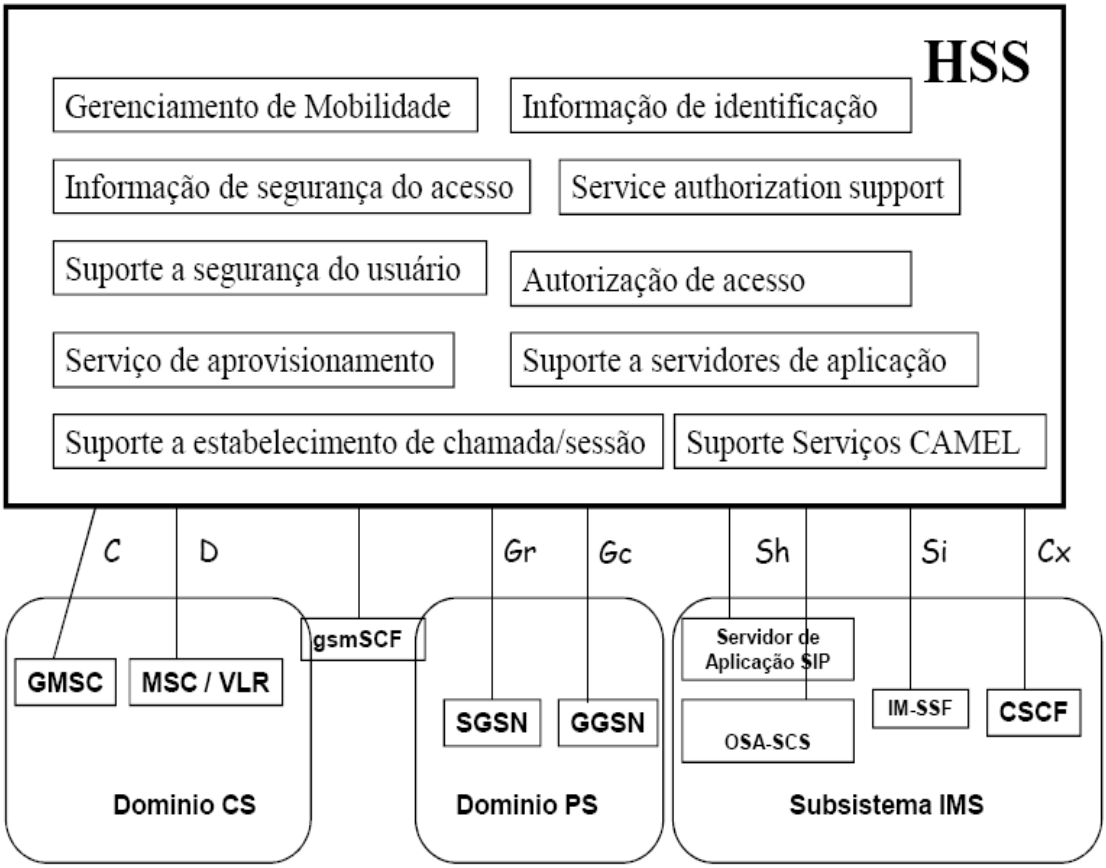

Fig. 2.10 - Funções lógicas do HSS [14].

• Suporte a autorização de serviço: o HSS fornece autorização básica para estabelecimento de chamada/sessão terminada no usuário e solicitação de serviço. Além disso, o HSS atualiza o elemento de rede no qual o usuário está registrado com informações relevantes ao serviço a ser fornecido para o usuário;

• Suporte ao aprovisionamento de serviços: o HSS fornece acesso aos dados do perfil de serviços do usuário dentro dos domínios de comutação por circuitos, comutação por pacotes e/ou do subsistema IMS;

• Suporte aos servidores de aplicação e serviços CAMEL: no subsistema IMS, o HSS comunica-se com os servidores de aplicação SIP e com o OSA-SCS para suportar as aplicações de serviços. Também se comunica com o IM-SSF para suportar os serviços baseados em CAMEL no subsistema IMS.

No caso dos domínios de comutação por circuitos e por pacotes, o HSS comunica-se com o gsmSCF para suportar os serviços CAMEL nesses domínios.

2.6.3. CSCF

O IMS CSCF (*Call Session Control Function*) provê o controle de sessão entre o acesso/transporte e camadas de aplicação do IMS e explora a infraestrutura da QoS IP.

Existem diversas funções para o CSCF – servidor, controle, *proxy* – e o desenvolvimento destes elementos está baseado em como a prestadora projeta sua rede.

Os aspectos de servidor e controle podem ser mais apropriados no núcleo da rede IMS, enquanto o *proxy* será mais apropriado na borda. O CSCF é o coração da camada de controle e precisa fornecer o mesmo desempenho que as prestadoras esperam de seus controles SS7.

A Fig. 2.11 apresenta a arquitetura IMS, onde o CSCF se comporta como elemento de controle para integração entre a rede IMS e a rede PSTN.

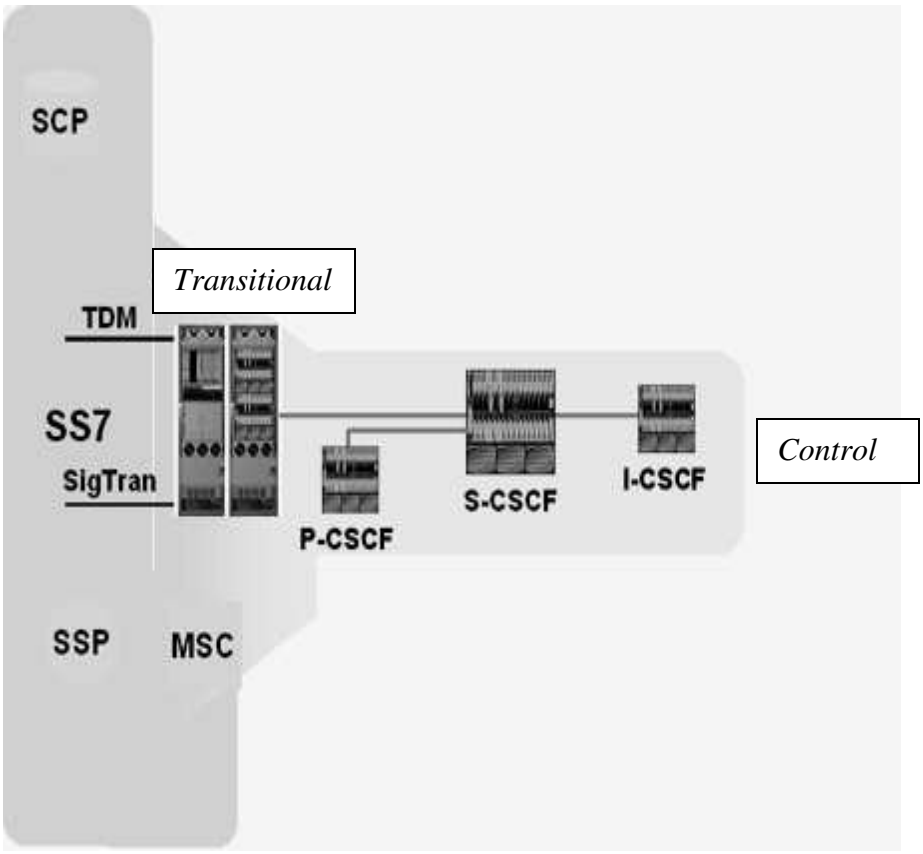

Fig. 2.11 – CSCF – Transição do PSTN para o IMS [14].

Os servidores SIP são nós essenciais na arquitetura IMS. Esses servidores são tratados conjuntamente por servidores com função de controle de chamadas e sessões, categorizados como P-CSCF (*Proxy*-CSCF), S-CSCF (*Serving*-CSCF) e I-CSCF (*Interrogating*-CSCF). O CSCF é o ponto de roteamento da sessão na rede núcleo do IMS.

Esses servidores são pontos de acesso padronizados, associados dinamicamente e independentes de serviço.

É responsável pela distribuição das chamadas entrantes para os servidores de aplicação e também por manipular a autenticação inicial de assinantes.

Cada um dos nós do núcleo IMS é detalhado nas seções subseqüentes.

2.6.3.1. P-CSCF (*Proxy* CSCF)

O P-CSCF é o primeiro ponto de contato entre o terminal e a rede IMS. Todos os pedidos iniciados ou destinados ao terminal IMS atravessam o P-CSCF. O terminal IMS se comunica apenas com um P-CSCF durante o registro.

O P-CSCF encaminha certa quantidade de associações de segurança IPSec para o terminal, a fim de oferecer proteção de integridade, como a habilidade de detectar se o conteúdo da mensagem foi modificado desde a sua criação.

O servidor autentica o usuário e valida sua identidade para o restante dos nós na rede.

O P-CSCF também é responsável por verificar a integridade do pedido SIP enviado pelo terminal IMS. Essa validação evita que o terminal crie pedidos SIP que não estejam em conformidade com as regras do protocolo.

O servidor comprime e descomprime as mensagens SIP, o que reduz o RTT[4] (*round-trip delay*) sobre *links* lentos de rádio.

O P-CSCF pode incluir um PDF (*Policy Decision Function*), que gerencia a QoS no plano de mídia. Além das funções descritas, o P-CSCF também gera informações de cobrança para os nós coletores de bilhetes de tarifação.

2.6.3.2. S-CSCF (*Serving*-CSCF)

O S-CSCF é o nó central no plano de sinalização. Trata-se essencialmente de um servidor SIP, mas, também executa funções de controle.

Está localizado na HM (*Home Network*) e usa o protocolo *diameter* Cx e Dx nas interfaces com o HSS, para *upload* e *download* de perfis de usuário, o que significa dizer que o S-CSCF não armazena informações de usuário localmente. Todas as informações necessárias são carregadas do HSS.

O S-CSCF manipula os registros SIP, o que permite conectar usuários e identificar endereços SIP. Esse servidor se localiza no caminho de todas as mensagens de sinalização e pode inspecionar todas as mensagens.

Ele atua como um SIP registrar enquanto executa funções de controle e serviços de roteamento.

---

[4] RTT é o tempo necessário para um pulso de sinal ou pacote viajar de uma específica fonte para uma destinação específica e voltar novamente.

2.6.3.3. I-CSCF (*Interrogating*-CSCF)

O I-CSCF é um *proxy* SIP localizado no limite do domínio administrativo. Esse nó é responsável por gerar solicitações ao HSS usando o protocolo *diameter* através das interfaces Cx e Dx, coletando informações de localização do usuário para propósito de roteamento.

O endereço IP do I-CSCF é publicado no DNS do domínio, a fim de ser utilizado pelo P-CSCF no domínio de rede destino, ou como um S-CSCF num domínio de rede externo, como um ponto de entrada para o todos os pacotes SIP daquele domínio.

Ele pode ainda ser utilizado para proteger do mundo externo os parâmetros internos de rede, encriptando partes das mensagens SIP (método conhecido por THIG[5]).

As três características mais críticas do CSCF são o *throughput* (o número de sessões por segundo que ele pode suportar), escalabilidade e latência.

Baixa latência é muito importante, porque afeta diretamente a experiência do usuário final, uma vez que o CSCF tem muitas responsabilidades: estabelecimento de sessões, verificação com o servidor de autenticação, acesso ao servidor de assinante por perfil de usuário, entre outros.

Todas essas funções precisam ser realizadas muito rapidamente (e independentemente da natureza do dispositivo de acesso), ou o usuário terá uma péssima impressão do serviço.

Antes que as operadoras implantem a funcionalidade de CSCF como parte de seu núcleo IMS, é necessário determinar como serão disponibilizados os serviços previamente existentes para os assinantes que serão servidos pelo CSCF.

Uma opção seria replicar toda a rede, o que obviamente torna essa opção inviável financeira e logisticamente para qualquer operadora.

A segunda opção é adicionar SIP em todos os servidores de aplicação novamente uma opção potencialmente custosa e fora da realidade.

A opção menos arriscada é o uso de tecnologias de transição (de mediação de serviço) para prover uma "ponte" entre a rede SIP IMS, a rede SS7 PSTN e a rede móvel 2G.

Essa ponte permitirá aos terminais SIP o acesso aos serviços da rede legada PSTN/2G e também permitirá aos terminais PSTN/2G o acesso a alguns serviços IMS.

A Fig. 2.12 demonstra uma ponte de transição entre a rede PSTN e o IMS. A nuvem do IMS contém uma parcela das funções do IMS que proporciona a habilidade de conduzir uma sessão do IMS para uma chamada baseada na PSTN.

---

[5] THIG é o processo de encriptar partes das mensagens SIP no intuito de proteger parâmetros internos da rede do mundo externo.

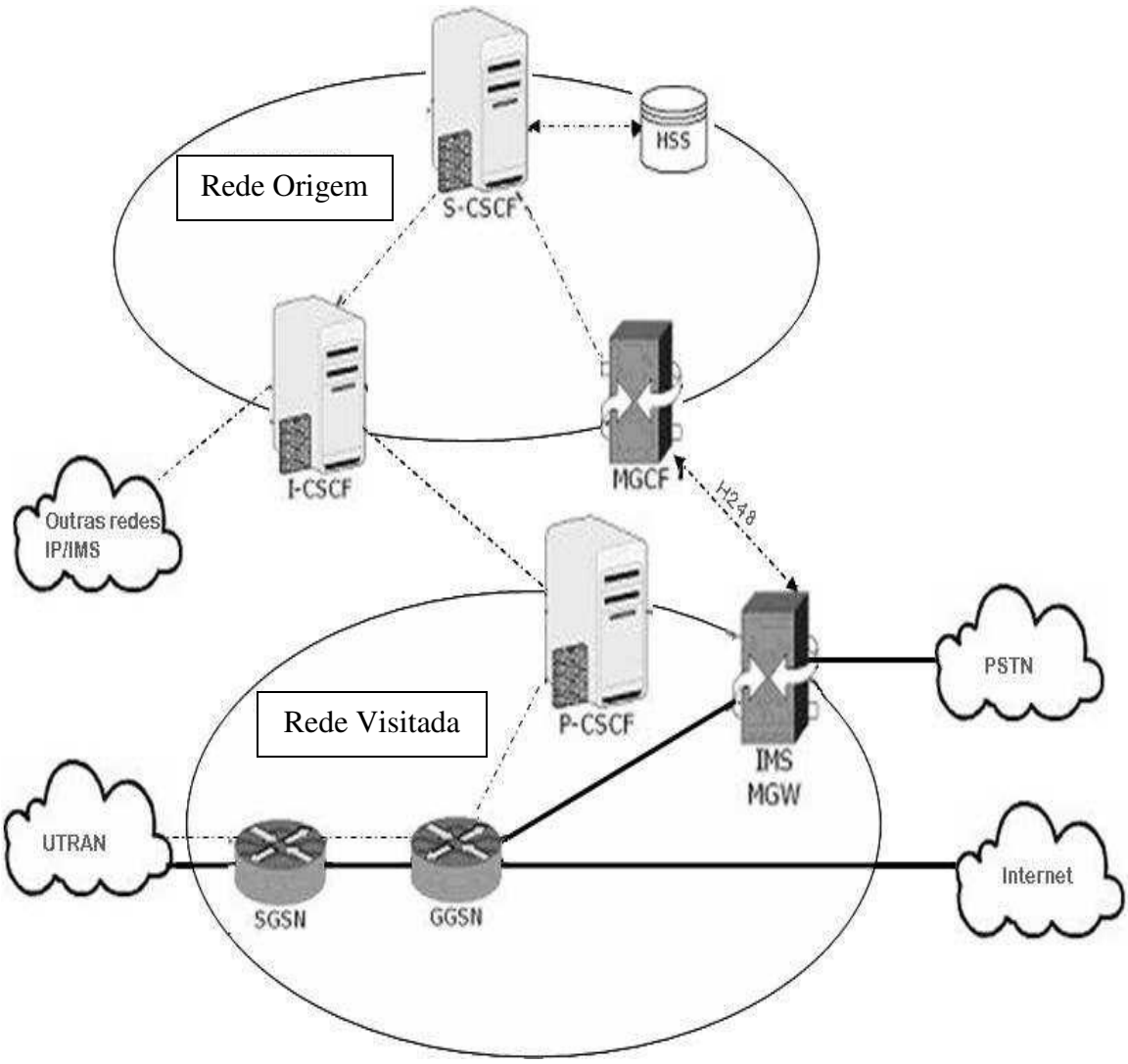

Fig. 2.12 - Tecnologias de transição para o IMS [14].

O CSCF encaminha os dados associados com a sessão do MGCF (*Media Gateway Control Function*).

Nesse ponto o caminho para sinalização e mídia se separa e o MGCF provê a informação de sinalização sobre o Sigtran para um *gateway* de sinalização, que o traduz para SS7 e o dispõe na PSTN.

Em paralelo com a transferência da informação de sinalização, o MGCF provê controle de mídia e a atualização de dados no IMS *Media Gateway* (MGW), que envia a mídia sobre TDM para a PSTN.

A arquitetura IMS ainda pode ser dividia nas seguintes seções: infraestrutura, aplicações e clientes, conforme ilustra a Fig. 2.13.

A infraestrutura é composta pelos componentes do núcleo da rede, como provedores de serviços, contendo as funções de controle de chamadas e de sessões baseadas nas especificações do IMS.

A camada de aplicações é composta pelos servidores de aplicações e serviços. A camada de clientes consiste das aplicações que suportam IMS que se encontram nos dispositivos do usuário final.

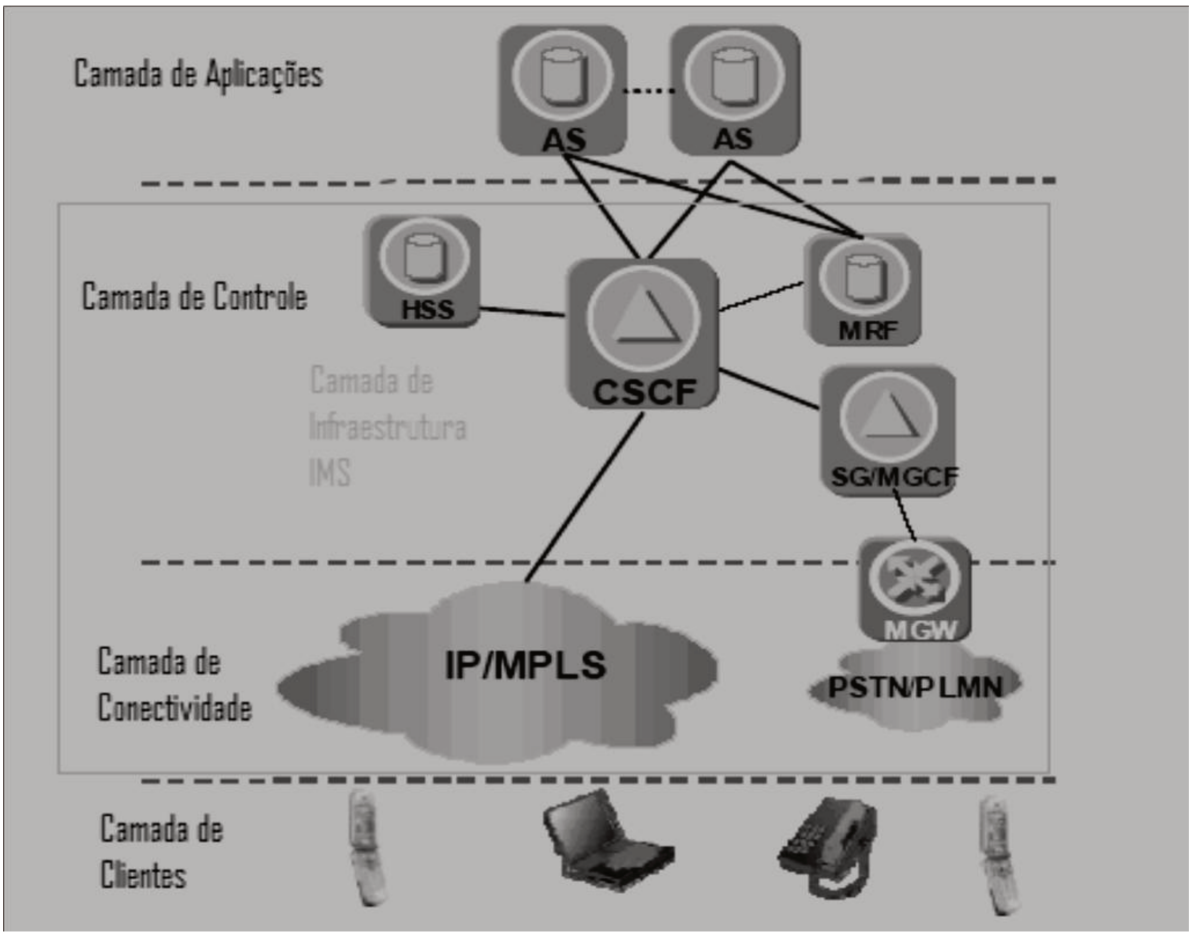

Fig. 2.13 - Arquitetura IMS [14].

2.6.4. O Servidor de Aplicação

O servidor de aplicação - AS (*Application Server*) é um elemento SIP que hospeda e executa serviços.

Dependendo do serviço definido, o AS pode operar no modo *proxy* SIP, no modo agente usuário – UA (*User Agent*) SIP, isso é, como um terminal, ou no modo agente usuário fim-a-fim - B2BUA (*Back-to-Back User Agent*), ou seja, uma concatenação de dois agentes usuário SIP.

O AS se comunica com o S-CSCF utilizando o protocolo SIP, através da interface ISC (IMS *Service Control*). A Fig. 2.14 descreve os diferentes tipos de Servidores de Aplicação, que são detalhados a seguir [4]:

• SIP AS (Servidor de Aplicação): Esse é um servidor de aplicação nativo que hospeda e executa serviços multimídia IP baseados em SIP. É esperado que todos os novos serviços, específicos do subsistema IMS, sejam desenvolvidos nos servidores de aplicações SIP.

• OSA – SCS (*Open Service Access – Service Capability Server*): Esse servidor de aplicação provê uma interface para o servidor de aplicação OSA (*Open Service Access*). Ele herda todas as facilidades OSA, especialmente a capacidade de acessar a rede IMS a partir de redes externas.

Esse nó atua, de um lado, como um servidor de aplicação (fazendo interface com o S-CSCF através de SIP) e, do outro lado, como uma interface entre o servidor de aplicação OSA e as API OSA [8].

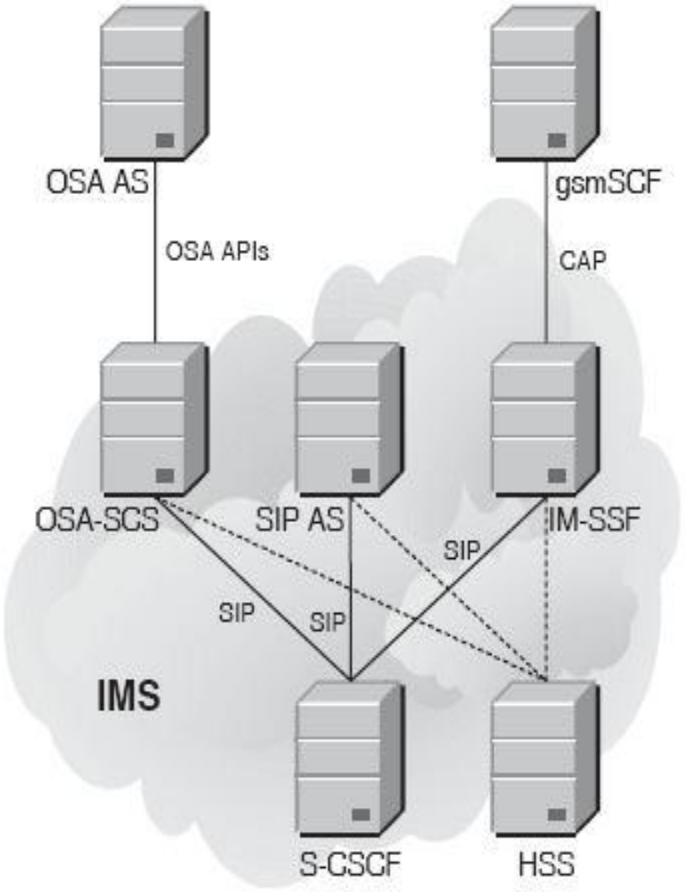

Fig. 2.14 - Tipos de servidores de aplicação [14].

• IM – SSF (*IP Multimedia - Service Switching Function*): esse servidor de aplicação especializado permite o reuso, na rede IMS, dos serviços CAMEL (*Customized Applications for Mobile network Enhanced Logic*) que foram desenvolvidos para a rede GSM. O IM – SSF permite um gsmSCF (*GSM Service Control Function*) controlar uma sessão IMS.

O IM – SSF atua, de um lado, como um servidor de aplicação, fazendo interface com o S-CSCF através de SIP. Do outro lado, ele atua como um SSF (*Service Switch Function*), fazendo interface como o gsmSCF através de protocolo baseado em CAP (CAMEL *Application Part*).

Todos os três tipos de servidores de aplicação comportam-se como servidores de aplicação SIP para a rede IMS, isso é, eles atuam tanto como um servidor *proxy* SIP, um agente usuário SIP, um servidor de redirecionamento SIP, ou como um agente usuário SIP fim-a-fim.

Os servidores de aplicação IM – SSF e OSA – SCS possuem, ainda, outras funções quando fazem interface com CAMEL ou OSA, respectivamente.

Além da interface SIP, o AS pode, opcionalmente, suportar uma interface com o HSS.

A interface do servidor de aplicação SIP e do OSA – SCS com o HSS é baseada no protocolo *diameter* e é utilizada para receber e enviar dados relacionados ao usuário e que estão armazenados no HSS.

A interface do IM – SSF para o HSS é baseada em MAP (*Mobile Application Part*).

O AS pode estar localizado tanto na rede de origem quanto na rede visitada ou em uma rede externa de terceiros com a qual a operadora de origem mantenha contrato de serviço.

Em qualquer um dos casos, se o AS utilizado estiver localizado fora da rede de origem, ele não tem interface de comunicação com o HSS.

2.6.5. MRF

O MRF (*Media Resource Function*) fornece uma fonte de mídias na rede local.

O MRF fornece à rede local a habilidade de tocar anúncios, misturar canais de mídia (por exemplo, uma ponte centralizada da conferência), transcodificar diferentes *codec's*, obtêm estatísticas, e faz toda análise das mídias.

O MRF é dividido em um nó do plano de sinalização chamado de MRFC (*Media Resource Function Controller*) e em um nó do plano de mídia chamado de MRFP (*Media Resource Function Processor*).

O MRFC atua como um SIP *user agent* (*endpoint*) e contêm uma interface SIP com o S-CSCF. O MRFC controla os recursos no MRFP através de uma interface H.248.

Como responsável pelo plano de mídia, o MRFP implementa todas as funções relacionadas a mídia.

O MRF é o nó que de fato armazena e toca os anúncios, combina os fluxos de mídia que chegam, e realiza o processamento de mídia (por exemplo, transcodificação de áudio, análise de mídia, etc.) [2,3].

Do ponto de vista de localização, o MRF está sempre instalado na rede de origem.

2.6.6. BGCF

O BGCF (*Breakout Gateway Control Function*) é essencialmente um SIP *server* que inclui a funcionalidade de roteamento baseada em números de telefone.

O BGCF é usado somente nas sessões que são iniciadas por um terminal IMS e dirigidas a um usuário em uma rede de comutação de circuito, tal como a PSTN ou a PLMN. As funcionalidades principais do BGCF são:

• Selecionar uma rede apropriada onde o *interworking* com o domínio de circuitos possa ocorrer.

• Selecionar um *gateway* apropriado para o tratamento da mídia PSTN/CS, se o *interworking* ocorrer na mesma rede onde o BGCF está alocado.

2.6.7. PSTN/CS *Gateway* para Rede Pública Comutada por Circuito

O PSTN *Gateway* fornece a interface com a rede de comutação por circuito, permitindo que os terminais IMS estabeleçam e recebam chamadas da PSTN (ou de alguma outra rede baseada em comutação por circuito).

A Fig. 2.15 mostra a conexão entre um BGCF e um PSTN *Gateway* decomposto.

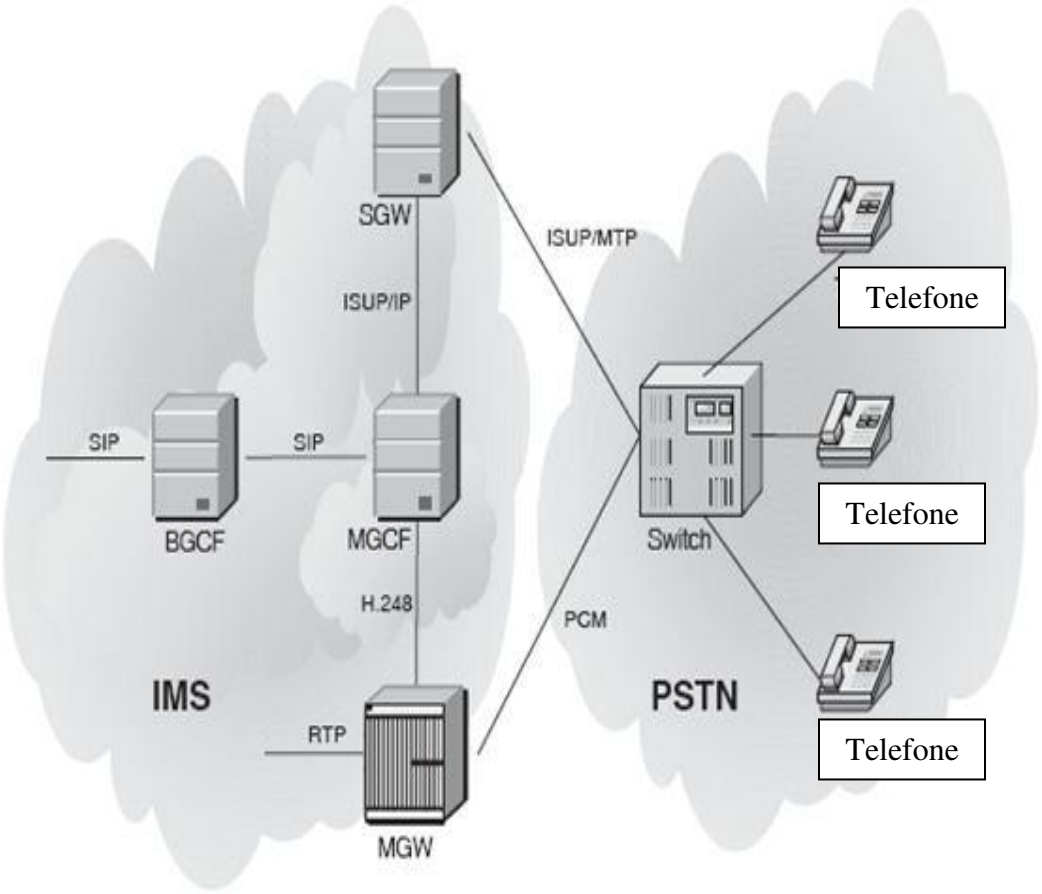

Fig. 2.15 - *Gateway* de interface com a rede PSTN/CS [14].

O PSTN *Gateway* é composto pelas seguintes funções:

• SGW: O *Signaling Gateway* é a interface com o plano de sinalização da rede CS (por exemplo, a PSTN). O SGW executa a conversão de protocolo da camada mais baixa.

Por exemplo, um SGW é responsável por substituir o transporte MTP pelo SCTP (*Stream Control Transmission Protocol*) sobre IP. Assim, o SGW transforma o ISUP ou BICC sobre MTP por ISUP ou BICC sobre SCTP/IP.

• MGCF: O *Media Gateway Control Function* é o nó central do PSTN/CS *gateway*.

Executa uma máquina de estado que faz a conversão de protocolo e o mapeamento SIP (o protocolo de controle da chamada no lado IMS) e também ISUP sobre o IP ou BICC sobre IP (BICC e ISUP são protocolos de controle da chamada em redes *circuit-switched*).

Além da conversão de protocolo e do controle da chamada, o MGCF controla os recursos dos MGW. O protocolo usado entre o MGCF e o MGW é H.248.

• MGW: O *Media Gateway* é a interface com o plano de mídia da rede PSTN ou CS. Por um lado o MGW pode enviar e receber mídias da rede IMS sobre o RTP (*Real-Time Protocol*).

Por outro lado o MGW usa um ou mais *time slots* PCM (*Pulse Code Modulation*) para conectar com a rede de CS.

Adicionalmente, o MGW executa transcodificação quando o terminal IMS não suporta o *codec* usado pelo lado CS.

Um cenário comum ocorre quando o terminal IMS está usando o *codec* AMR (*Adaptative Multi Rate*, definido pelo 3GPP) e o terminal PSTN está usando o *codec* G.711 [8].

2.6.8. Localização do P-CSCF

O IMS faz uso de alguns conceitos da rede GSM e GPRS, como, por exemplo, ter uma rede origem e rede visitada.

A maioria dos elementos IMS está localizada na rede de origem, como acontece na rede GSM/GPRS. Porém, há um nó que pode estar localizado tanto na rede de origem ou na rede visitada, esse nó é o P-CSCF.

O IMS permite duas diferentes configurações, dependendo se o P-CSCF está localizado na rede de origem ou na rede visitada.

Adicionalmente, quando a rede de acesso IP-CAN (IP *Connectivity Access Network*) é GPRS, a localização do P-CSCF é subordinada a localização do GGSN.

Nos cenários de *roaming*, o GPRS permite que o GGSN esteja localizado tanto na rede de origem ou rede visitada, porém, o SGSN está sempre localizado na rede visitada.

No IMS, ambos GGSN e P-CSCF compartilham a mesma rede. Isso permite o P-CSCF controlar o GGSN através da chamada interface Go.

Como tanto o P-CSCF e o GGSN estão localizados na mesma rede, a interface Go é sempre uma interface intra-operadora, o que torna mais simples a sua operação.

A configuração onde o P-CSCF (e o GGSN) está localizado na rede visitada representa uma visão de longo prazo do IMS, pois isso requer suporte IMS da rede visitada, ou seja, o GGSN tem que ser atualizado para ter compatibilidade com a versão cinco do 3GPP [1].

A Fig. 2.16 mostra a configuração de curto-prazo onde ambos o P-CSCF e o GGSN estão localizados na rede de origem. Essa configuração não requer nenhum suporte IMS na rede visitada.

A rede visitada somente provê os recursos de rádio e o SGSN (comutação por pacotes). Assim, essa configuração pode ser instalada logo no inicio da rede IMS.

Como conseqüência, é esperado que essa fosse a configuração mais comum nos primeiros anos de instalação das redes IMS pelas operadoras.

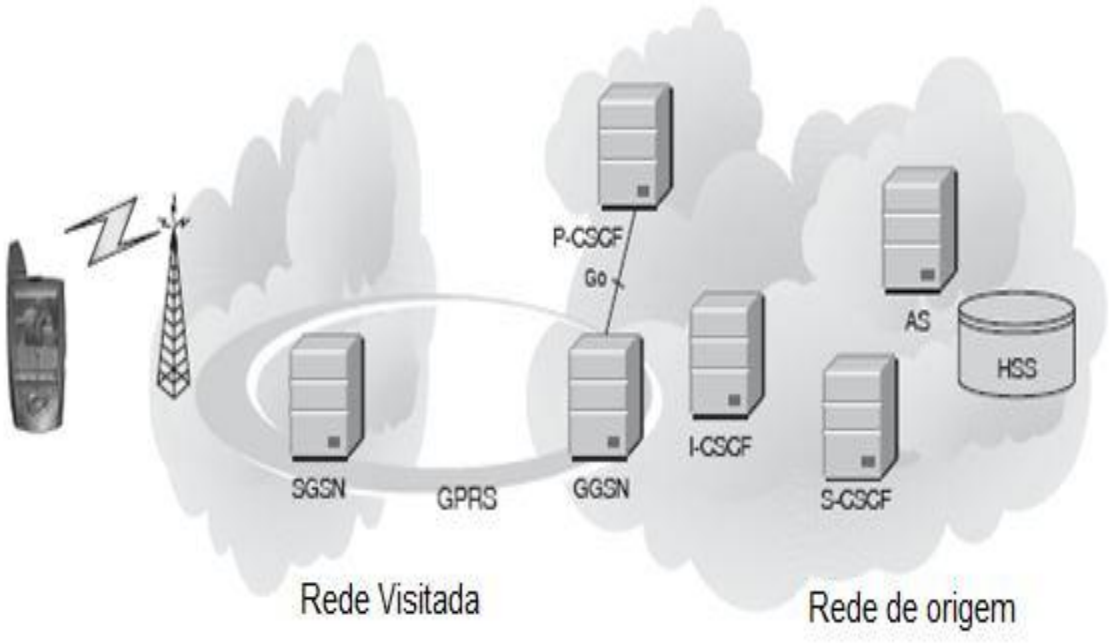

Fig. 2.16 - Localização do P-CSCF na rede de origem - modificado [14].

2.7. O Problema de Admissão de Conexão e de Sessão

Antes que um terminal IMS comece uma operação relacionada ao mundo IMS, existe uma quantidade de pré-requisitos que tem que ser atendidos. A Fig. 2.17 mostra uma visão macro dos pré-requisitos necessários.

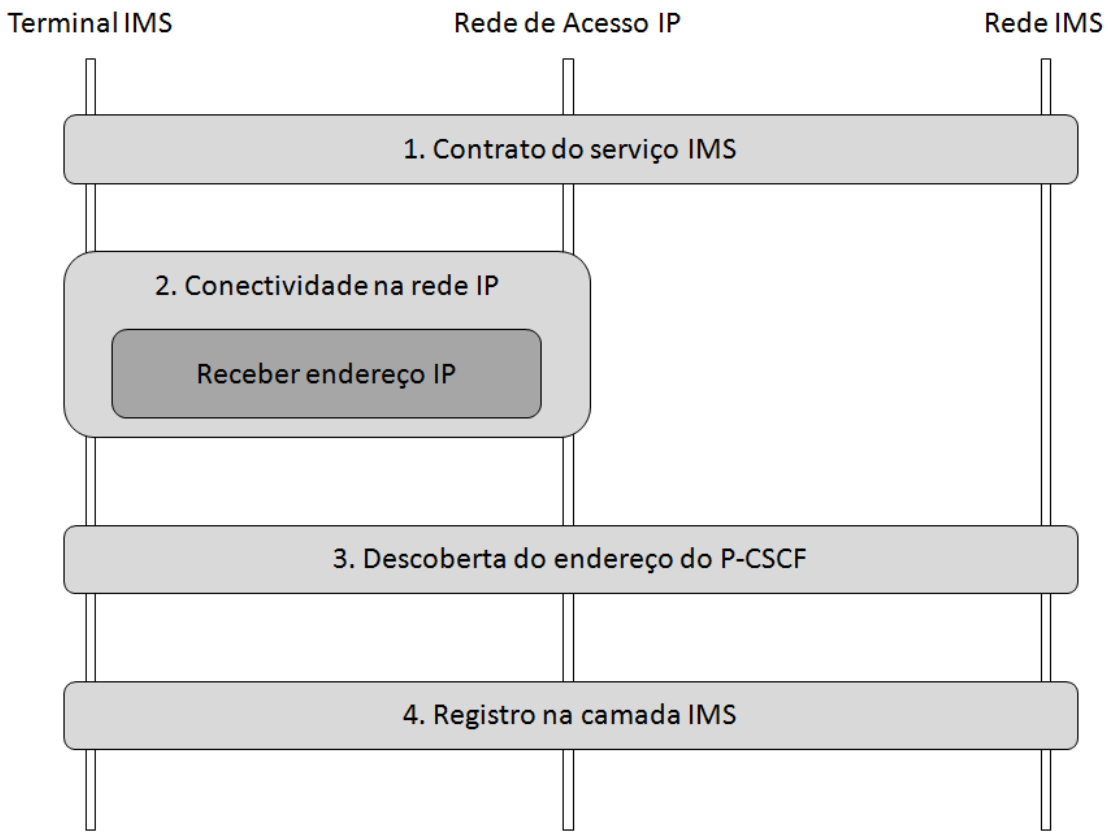

Fig. 2.17 - Pré-requisitos para operação de serviço IMS [14].

Primeiro, o provedor de serviços IMS tem que autorizar o usuário final a usar o serviço IMS. Isso requer, tipicamente, uma assinatura ou contrato assinado entre a operadora de rede IMS e o usuário.

Esse contrato é similar a assinatura que autoriza um usuário final a receber e estabelecer chamadas sobre uma rede celular.

Segundo, o terminal IMS necessitar ter acesso a um IP-CAN (IP *Connectivity Access Network*) como GPRS/EDGE (em redes GSM/UMTS), ADSL (*Asymmetric Digital Subscriber Line*) ou WLAN (*Wireless Local Access Network*).

O IP-CAN provê acesso à rede IMS de origem do acesso ou a uma rede IMS visitada. Como parte desse pré-requisito, o terminal IMS precisa adquirir um endereço IP (os procedimentos para acesso GPRS/EDGE são descritos em 3GPP TS 23.060).

Esse endereço IP, tipicamente, é alocado de forma dinâmica pela operadora do IP-CAN, por um determinado período de tempo. É possível também a alocação de endereço IP fixo, visto que para algumas empresas é fundamental ter IP fixo para gerenciamento e controle da rede.

Quando esses dois pré-requisitos são atendidos, o terminal IMS precisa descobrir o endereço IP do P-CSCF que irá atuar como seu servidor *proxy* de mensagens SIP entrante /sainte. Todas as sinalizações SIP enviadas pelo terminal IMS passam por esse P-CSCF.

Quando o procedimento de descoberta do P-CSCF é completado, o terminal IMS está habilitado a enviar e receber sinalização SIP para ou do P-CSCF.

O P-CSCF é alocado permanentemente durante todo o registro IMS, um procedimento que é tipicamente disparado quando o terminal IMS é ligado ou desligado.

Quando os pré-requisitos acima são preenchidos, o terminal IMS passa para o registro no nível de aplicação SIP da rede IMS. Isso é realizado através de um registro normal do SIP, como será visto em 3.3.4.

O termina SIP necessita estar registrado no IMS antes de iniciar ou receber qualquer outra sinalização SIP.

Como o IMS é modelado em diferentes camadas, a camada IP-CAN é independente da camada de aplicação (SIP) IMS. Por isso, o registro no nível do IMS é independente do registro com o IP-CAN (por exemplo, o attachment na rede GPRS/EDGE).

O processo de registro no IMS permite a essa rede localizar o usuário, isso é, o IMS obtém o endereço IP do terminal IMS. O registro também permite a rede IMS autenticar o usuário, estabelecer associações de segurança, e autorizar o estabelecimento de sessões.

2.8. A Utilidade do SIP para Controle de Conexão e de Sessão

O SIP (*Session Initiation Protocol*) é um protocolo especificado pelo IETF (*Internet Engineering Task Force*) como um protocolo para estabelecer e gerenciar sessões multimídia sobre redes IP.

O SIP foi escolhido pelo 3GPP como o protocolo de controle de sessão para ser utilizado na rede IMS.

O SIP segue o conhecido modelo de cliente-servidor, bastante utilizado por muitos protocolos desenvolvidos pelo IETF. O desenvolvimento do SIP utilizou princípios de projeto do SMTP (*Simple Mail Transfer Protocol*), e especialmente, do HTTP (*HyperText Transfer Protocol*).

Assim, o SIP herdou muitas de suas características desses dois protocolos. Isso traz uma força importante para o SIP, porque o HTTP e o SMTP são os protocolos de mais sucesso na *internet*.

O SIP, ao contrário de outros protocolos de rede, não diferencia a interface rede-usuário –UNI (*User-to-Network Interface*) da interface rede-rede – NNI (*Network-to-Network Interface*). O SIP é um protocolo simples que trabalha fim-a-fim.

Diferentemente de protocolos como BICC e ISUP, o SIP é um protocolo baseado em texto. Isso significa que ele é mais fácil de entender, de analisar falhas e de ser utilizado para construir novos serviços.

Esse fato, do SIP tornar fácil a criação de novos serviços, foi de grande peso na escolha e decisão do SIP como o protocolo de controle de sessão.

2.9. QoS Suporte no IMS

O IETF definiu duas abordagens bem conhecidas para a solução de QoS na camada IP, o modelo de integração de serviços (IntServ) e o modelo de serviços diferenciados (DiffServ), além do que recentemente foi proposto um novo modelo que permite o uso de IntServ sobre domínios DiffServ.

Duas estratégias são consideradas para providenciar um bom nível da QoS em pacotes de rede, o primeiro envolve evitar o congestionamento.

Isso pode ser feito através da implementação do CAC (*Connection Admission Control*), reservando recursos ou simplesmente super-dimensionando a rede (*over-provisioning*), um exemplo da QoS baseado na reservação de recursos é a integração de serviços (IntServ).

O segundo método seria o gerenciamento de congestionamento. A diferenciação para providenciar melhor QoS seria simplesmente conceder o melhor serviço para os fluxos mais importantes, um dos padrões mais conhecidos usando esse método seria o DiffServ.

Com relação ao gerenciamento da QoS podemos destacar dois tipos, o primeiro focado no provisionamento garantido da QoS enquanto o outro é focado em QoS relativo.

No garantido com *delay* ou perda de taxas pode ser providenciado pelo esquema de reserva de recursos, na QoS relativo pode ser implementado por diferenciação de tráfego.

As redes IMS suportam ambos o controle de admissão e diferenciação da QoS.

2.10. *Charging*

O *charging* ou tarifação não é um elemento da rede IMS, é um conceito. Contudo, alguns elementos anteriormente apresentados como o P-CSCF, I-CSCF, S-CSCF, BGCF, MRFC, MGCF e AS usam interfaces de tarifação que torna importante a apresentação deste conceito.

No IMS há dois tipos de charging: online e offline.

A Fig. 2.18 abaixo mostra uma conjugação da arquitectura de charging online e offline especificada na norma TS 32.260.

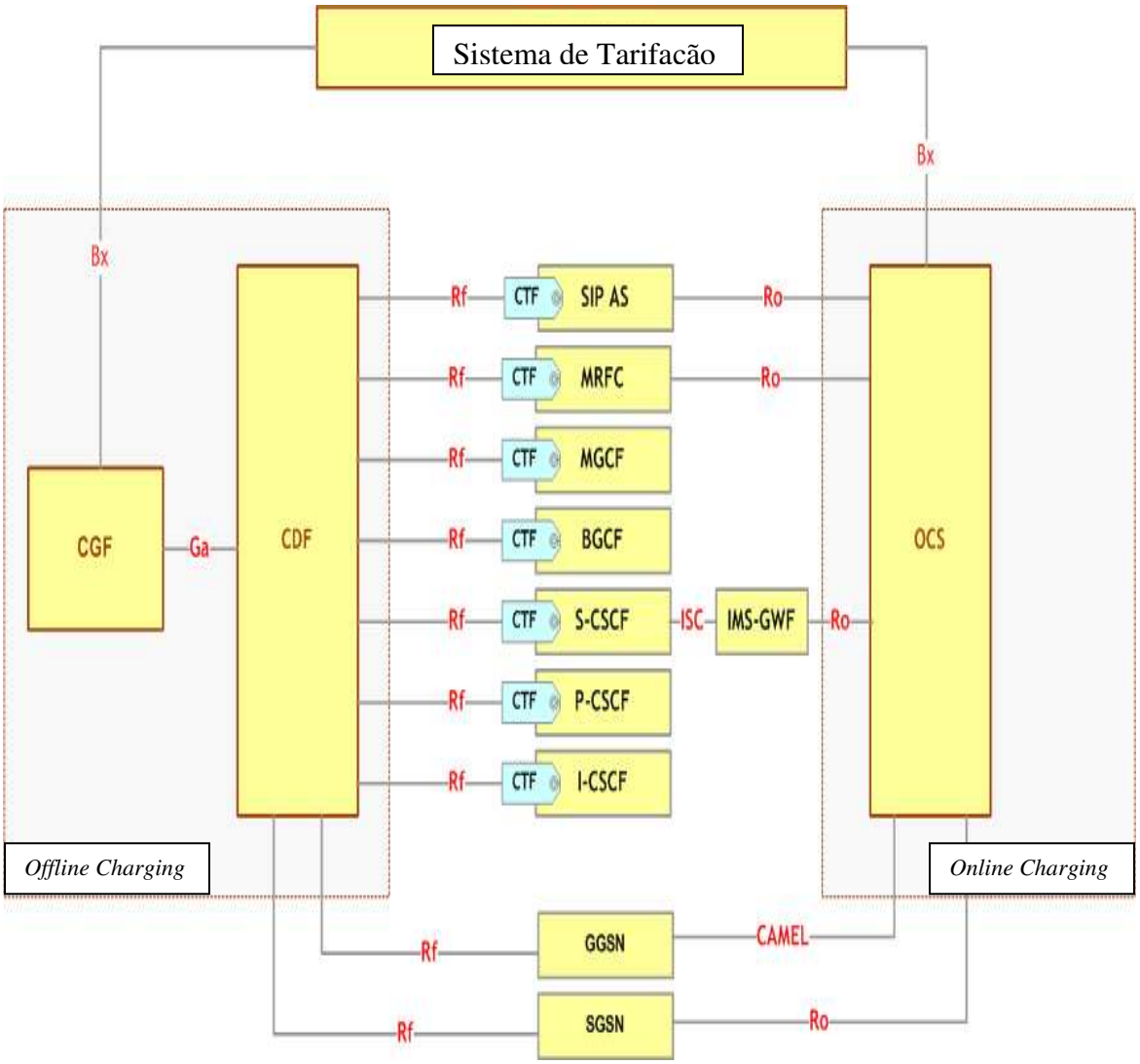

Fig. 2.18 – Arquitetura de *charging* IMS [13].

No *online charging*, como o nome indica as funções de tarifação são usadas imediatamente.

Por exemplo, se for usado o IEC (*Immediate Event Charging*), o número de unidades de crédito são instantaneamente deduzidas na conta do utilizador pelo ECF (*Event Charging Function*) e o MRFC ou AS são assim autorizados a disponibilizar ou não o serviço.

O S-CSCF fala com um SCF (*Session Charging Function*) que age como um SIP AS comum. Esse SCF pode comunicar ao S-CSCF que termine a chamada quando terminarem os créditos.

A interface Diameter Ro permite que os CTF (*Charging Trigger Function*) enviem eventos de charging para o OCF (*Online Charging Function*). Esses eventos podem ser baseados em eventos ou em sessões.

Quando é usado o ECUR (*Event Charging* com *Unit Reservation*), o ECF primeiro reserva o número de créditos da conta do utilizador e só depois autoriza o MRFC ou o AS. No final do serviço, o número de créditos gasto é deduzido da conta.

No *offline charging*, como o nome indica a tarifação é feita posteriormente. Um exemplo de *offline charging* é a criação de CDR (*Call Detail Records*).

O *offline charging* é aplicado aos utilizadores que usam os serviços periodicamente (ex: uma assinatura). O *online charging* por sua vez é usado para serviços pré-pagos ou para controle de crédito *realtime* de pós-pagos.

Todos os elementos SIP da rede envolvidos numa sessão (P-CSCF, I-CSCF, S-CSCF, BGCF, MRFC, MGCF, AS) usam a interface *diameter* Rf para enviar informação de *accounting* para o CCF (*Charging Collector Function*).

O CCF agrega essa informação e constrói um CDR que é enviado para o BS (*Billing System*), tanto o *offline* como o *online charging* podem ser usados numa sessão, inclusive simultaneamente.

2.11. Interfaces

As interfaces IMS permitem que cada elemento da rede comunique com outros através de um protocolo definido para essa *interface* [1].

A Tabela 2.1 faz uma descrição de todas as interfaces existentes numa rede IMS. Ao analisar essa tabela, fica claro que protocolos como o SIP e o *diameter* são usados extensivamente nas redes IMS.

Em relação ao *diameter*, foram criadas *interfaces* IMS específicos para tornar um protocolo normalizado nessas redes. Por exemplo, o *diameter* é usado para implementar autenticação, autorização e *accounting* (AAA).

Tabela 2.1 - Interfaces IMS [1].

Nome Interface	**Entidades IMS**	**Descrição**	**Protocolo**
Cr	MRFC, AS	Usado pelo MRFC para buscar documentos (*scripts* e outros recursos) de um AS	HTTP sobre canais TCP/SCTP dedicados
Cx	I-CSCF, S-CSCF,	Usado para comunicar entre I-CSCF/S-CSCF e	*Diameter*

	HSS	HSS	
Dh	SIP AS, OSA, SCF, IM-SSF, HSS	Usado pelo AS para encontrar um HSS correto em um ambiente multi-HSS	*Diameter*
Dx	I-CSCF, S-CSCF, SLF	Usado pelo I-CSCF/S-CSCF para encontrar um HSS correto em um ambiente multi-HSS	*Diameter*
Gm	UE, P-CSCF	Usado para troca de mensagens entre UE e CSCFs	SIP
Go	PDF, GGSN	Permite as operadoras controlar a QoS no plano do usuário e trocar informações correlacionadas a tarifação entre o IMS e a rede GPRS	COPS (Rel5), *Diameter* (Rel6+)
Gq	P-CSCF, PDF	Usado para a troca de políticas de decisões relacionadas com informação entre P-CSCF e PDF	*Diameter*
ISC	S-CSCF, I-CSCF, AS	Usado para troca de mensagens entre CSCF e AS	SIP
Ma	I-CSCF -> AS	Usado para diretamente encaminhar as requisições SIP que são destinadas para uma identidade de serviço público pelo AS	SIP
Mg	MGCF -> I-CSCF	MGCF converte sinalização ISUP para sinalização SIP e encaminha a sinalização SIP para o I-CSCF	SIP
Mi	S-CSCF -> BGCF	Usado para troca de mensagens entre S-CSCF e BGCF	SIP
Mj	BGCF -> MGCF	Usado para troca de mensagens entre BGCF e MGCF na mesma rede IMS	SIP
Mk	BGCF -> BGCF	Usado para troca de mensagens entre BGCFs em diferentes redes IMS	SIP
Mm	I-CSCF, S-CSCF, rede IP externa	Usado para troca de mensagens entre IMS e redes IP externas	Não especificado
Mn	MGCF, IM-MGW	Permite controlar os recursos do plano do usuário	H.248

Mp	MRFC, MRFP	Usado para troca de mensagens entre MRFC e MRFP	H.248
Mr	S-CSCF, MRFC	Usado para troca de mensagens entre S-CSCF e MRFC	SIP
Mw	P-CSCF, I-CSCF, S-CSCF	Usado para troca de mensagens entre CSCFs	SIP
Rf	P-CSCF, I-CSCF, S-CSCF, BGCF, MRFC, MGCF, AS	Usado para trocar informação de tarifação *offline* com CCF	*Diameter*
Ro	AS, MRFC	Usado para trocar informação de tarifação *online* com ECF	*Diameter*
Sh	SIP AS, OSA SCS, HSS	Usado para trocar informação entre SIP AS/OSA SCS e HSS	*Diameter*
Si	IM-SSF, HSS	Usado para trocar informação entre IM-SSF e HSS	MAP
Sr	MRFC, AS	Usado pelo MRFC para buscar documentos (*scripts* e outros recursos) de um AS	HTTP
Ut	UE, AS (SIP AS, OSA SCS, IM-SSF)	Habilita UE gerenciar informação relacionada com seus serviços	HTTP(s)

2.12. Arquitetura Lógica do IMS

O IMS é uma rede de mídia sobre IP e usa o SIP (*Session Initiation Protocol*), que originalmente foi padronizado pela IETF, como protocolo base do IMS.

O 3GPP escolheu o SIP como seu protocolo base devido ao fato de que os protocolos de sinalização tradicionalmente empregados nas telecomunicações falharam em requisitos básicos do IMS.

Uma vez que o SIP é um protocolo de i*nternet*, ele suporta convergência e potencialmente atende a todas as necessidades da arquitetura IMS. Por exemplo, o SIP pode sinalizar através de diferentes entidades de rede, incluindo servidores e *endpoints*.

No IMS, cada servidor de rede tem sua própria função, o que contrasta com as redes tradicionais, onde um escritório central de comutação faz tudo, incluindo controle de chamadas e de serviços. Além disso, o SIP utiliza alguns mecanismos de extensão da i*nternet*.

Um provedor de serviços com rede IMS inicialmente terá um pequeno número de assinantes, assim que essa base crescer, as redes IMS precisam ser suficientemente escaláveis para atender mais assinantes.

O SIP também é um protocolo muito flexível e extensamente padronizado, o que provê às redes IMS a capacidade de se adaptar e modificar protcolos de sinalização dinamicamente, conforme as necessidades de mercado.

Outra justificativa para o emprego do protocolo SIP é que ele provê mecanismos de segurança adequados, tanto para elementos internos quanto para elementos externos da rede.

O suporte aos esquemas de provisionamento de serviços numa arquitetura como essa certamente gera aplicações complexas que podem vir a causar uma carga muito alta de sinalizaçao SIP na rede.

As operadoras devem se preparar previamente para absorver esse impacto que pode ser causado no desempenho da rede. As interfaces da arquitetura lógica do IMS, definidas pelo 3GPP R10 é exibido na Fig. 2.19.

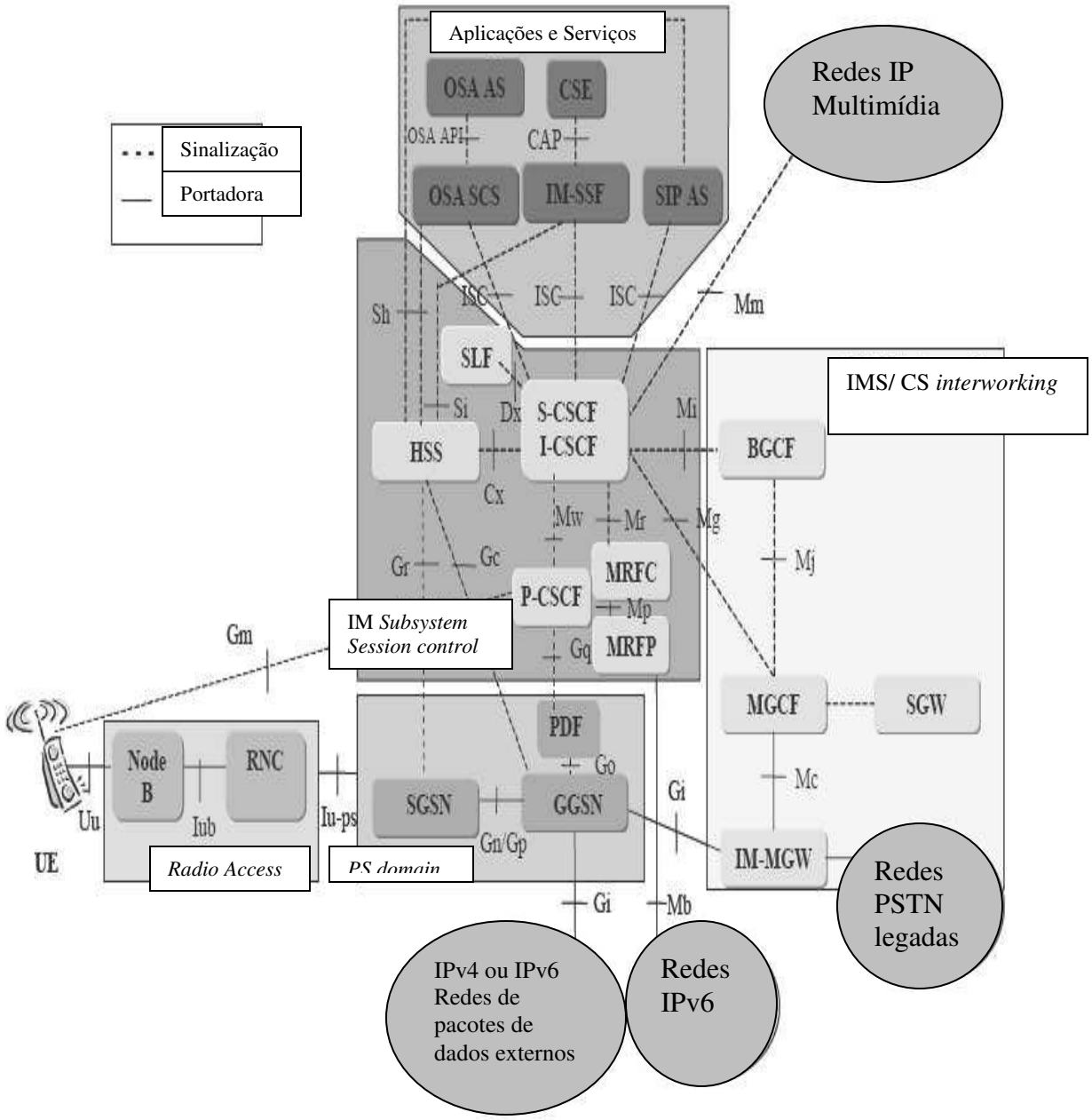

Fig. 2.19 - Arquitetura lógica do 3GPP IMS R10 [1].

CAPÍTULO 3

REDES IMS - APLICAÇÕES E BENEFÍCIOS

As redes IMS são anunciadas como redes de próxima geração que terão como benefício principal uma verdadeira convergência de serviços, aplicações, redes e terminais. Essa convergência é potencializada através da arquitetura de rede em camadas [*2*].

A convergência de terminais permite que qualquer terminal fixo ou móvel, como telefones, PDAs, computadores pessoais ou televisores, possa acessar a rede.

A convergência de redes significa que a rede móvel, a rede fixa e as redes de banda larga são vistas como uma entidade para a camada de abstração IMS. Dessa forma, serviços de rede são oferecidos independentemente do tipo de acesso.

A convergência de rede envolve todas as funcionalidades necessárias aos serviços, como acesso aos perfis dos usuários, autenticação, tarifação, serviços de localização e controle de recursos multimídia através de APIs abertas e normalizadas.

Além do que, as aplicações convergentes IMS podem residir no fornecedor de serviços ou em qualquer plataforma da operadora.

Podem aproveitar e usar serviços comuns de rede e serem acessadas por usuários a partir de qualquer rede ou terminal, inclusive podem ser aplicações de redes inteligentes (IN) portadas para a rede IMS usando o IM-SSF.

O IMS trará inúmeros benefícios para os provedores de serviços como a facilidade de criar e instalar novas aplicações e serviços já que as interfaces são normalizadas.

A complexidade desses serviços será mais reduzida, e as aplicações serão mais fáceis de desenvolver usando APIs abertas e serviços de rede compartilhados [*2*].

Como as interfaces são normalizadas e não dependem de protocolos proprietários, os provedores de serviços poderão mais facilmente fornecer pacotes de serviços oferecendo descontos por quantidade de pacotes ofertados.

Outro benefício será a reutilização, o recurso a pequenos componentes permite que sejam reutilizados na construção de novos serviços minimizando o tempo de desenvolvimento e melhorando o tempo de entrada em exploração comercial dos mesmos.

Em alguns casos, não será necessário o desenvolvimento de novos módulos, apenas recombinar os mesmos.

Como a rede permite compartilhar recursos de rede com terceiros, os provedores de serviços externos podem acessar a rede para oferecer as suas aplicações e serviços podendo até as operadoras optar por cenários de partilha dos lucros para reduzir os riscos dos investimentos em serviços.

Mas a vantagem mais apelativa para os fornecedores de serviços será a possibilidade de criar novos serviços multimídia. O acesso a recursos multimídia (voz, vídeo e dados) estará disponível na mesma chamada.

Os serviços IMS permitirão captar novos clientes e fidelizar os existentes recorrendo a uma melhor qualidade de voz e vídeo para aplicações comerciais, como conferência, usando *wideband coders*.

Por outro lado, a convergência permite a oferta de aplicações móveis (como SMS, etc.) a usuários fixos ou de banda larga.

Os clientes empresariais também poderão se beneficiar das redes IMS como a personalização dos serviços conforme o seu modelo de negócio. Mesmo havendo dois clientes numa determinada área de negócio, os seus modelos podem ser diferentes.

Com o IMS, a implementação de serviços personalizados é mais simplificada. Por outro lado, a rede permite uma melhoria das capacidades de comunicação e *marketing*, dado que os clientes podem expandir os seus modelos de comunicação para incluir qualquer aplicação ou serviço i*nternet*.

Contudo, a vantagem que poderá fazer a grande diferença para o cliente empresarial será a redução do tempo de entrega do serviço ao cliente.

No mercado global em que as empresas competem, pode ser determinante o tempo que leva desde a concepção da ideia até a entrega da solução no mercado.

Do ponto de vista das operadoras, as redes IMS permitem aumentar o grau de satisfação dos clientes e reduzir os custos com criação de serviços (podendo mais facilmente optar por modelos de *outsourcing*) podendo usufruir de uma redução nos custos de operação e TCO (*Total Cost of Ownership*).

A própria implementação dos serviços será mais eficiente dado que um único serviço pode ser fornecido a vários tipos de acesso (fixo móvel, banda larga).

Além destas vantagens, as redes IMS podem trazer as operadoras um aumento da simplicidade de operação e manutenção das redes dado que os sistemas de gestão, provisionamento e tarifação são comuns a todas as redes.

Ou seja, podem-se diminuir custos através da simplificação de processos. Mas as vantagens econômicas estendem-se, também, aos custos com a rede de transporte que sofrerão uma redução

significativa com a migração de canais de comutação de circuitos para comutação de pacotes (infraestrutura IP).

Finalmente, as operadoras terão a capacidade de oferecer novos serviços e produtos baseados em recursos da *internet*. Portanto, a implementação de redes IMS resultará numa redução de despesas para disponibilizar conteúdos aos usuários em qualquer formato, dispositivos ou rede.

O IMS será importante para os operadores móveis porque as redes "pré-IMS" são centradas na voz. Mesmo as redes de videoconferência 3G (3G-H.324M) operam sobre canais de comutação de circuitos.

Mas as tecnologias de rádio móvel (wifi, wimax, etc.) estão aproximando-se das velocidades de banda larga. Se as operadoras não suportarem serviços baseados em IP, outros provedores o farão usando o acesso à i*nternet*.

Também será importante para as operadoras de telefonia fixa que tem perdido relevância frente operadoras móveis e de VoIP, que no mínimo, precisam oferecer convergência fixo-móvel mas também precisam fornecer novos serviços.

O IMS tem potencial para fornecer esses novos serviços com uma qualidade que a voz sobre IP comum não pode. Outra promessa do IMS é a rapidez de criação e entrega de aplicações novas ou recombinadas usando o SCIM (*Service Capability Interaction Manager*).

3.1 Serviços

Alguns dos serviços básicos previstos para uma rede IMS incluem [2,13,14]:

- Vídeo e *messaging* móvel bidireccional;
- Colaboração;
- *Call centers* baseados em IP e video *call centers*;
- *Video-on-demand* e *download* de conteúdos;
- Serviços baseados em localização;
- Evolução dos atuais serviços *push-to-talk* e conferência;
- Convergência fixo-móvel;
- PABX IP;
- VPN móvel;
- Vídeo conferência residencial;
- Vídeo conferência empresarial.

Fig. 3.1 - Exemplos dos serviços básicos IMS [3].

Serviços *Quad-Play*

O IMS utiliza o IP para disponibilizar serviços de vídeo, voz e dados sobre qualquer tipo de acesso fixo ou móvel. Desta forma, o IMS tem a capacidade de criar uma oferta *quad-play* sem precedentes.

Ao unir a IPTV (*Television over IP)* com o IMS, as *set-top boxes* tornam-se terminais IMS, tal qual qualquer outro tipo de terminal (PC, celular, etc.).

Desta forma, os usuários podem usufruir, consistentemente, de uma vasta gama de serviços entre redes de acesso. Os serviços de voz e dados podem ser expandidos à IPTV da mesma forma que a um terminal fixo ou móvel.

As operadoras podem oferecer novos serviços que ajudam os usuários a gerir e acessar bibliotecas pessoais de conteúdos comerciais ou privados fazendo-o a partir de qualquer terminal. Os serviços de vídeo como DVR (Digital Video Recorder) em rede, podem ser expandidos da TV para o terminal móvel permitindo aos usuários levar os seus conteúdos consigo.

Esses tipos de serviços avançados não só compete no preço, como representa uma oferta integrada que proporciona uma experiencia mais rica.

Ao aumentar o valor dos serviços fornecidos, a operadora pode aumentar os ganhos por usuários e aumentar a fidelização dos mesmos.

Exemplos de serviços de telefonia na TV:

• Visualização do número de chamada
• *Click-to-Call*
• Gestão de chamadas:
• Ignorar ou rejeitar chamadas
• Encaminhamento para *voicemail*
• Indicador de *voicemail*
• Chamada de vídeo
• Vídeo-conferência

Exemplos de serviços de dados na TV:

• *Chat – Instant Messaging*
• Compartilhamento de informação
• Compartilhamento de fotos
• *Upload* para *blogs* ou *webpage*
• Lista de amigos e presença
• Lista de endereços como o *Outlook*/PDA.

Esses serviços que resultam da união da IPTV com as redes IMS trazem perspectivas muito animadoras.

Essas novas capacidades vão enriquecer a experiência do usuário através da utilização de um conjunto de terminais para ver TV ou sessões interativas, mas também podem acrescentar capacidades multimídia à TV ou a terminais móveis.

Essa convergência entre terminais e televisão permitirão compartilhar conteúdos pessoais com outros usuários e gerir ou acessar conteúdos de vídeo em qualquer lugar.

Essa combinação do vídeo com serviços de comunicação aumentará a produtividade e entretenimento agregando mais valor em todas as soluções.

3.2. Desafios

Apesar de o IMS parecer a evolução lógica das redes de telecomunicações, ainda enfrenta alguns obstáculos na sua implantação e globalização [*7*]:

O primeiro é a complexidade. Há muitas especificações IMS com múltiplas versões que continuam a evoluir e os testes de interoperabilidade não têm acompanhado o desenvolvimento e a introdução do produto.

O segundo desafio é o dos serviços. O IMS é uma plataforma que pode suportar novos serviços, mas a operadora de telefonia não ganha dinheiro enquanto esses não são lançados e se tornam rentáveis.

Atualmente, há um número relativamente pequeno de novos serviços disponíveis com o IMS e, quando comparado com a i*nternet*, tem uma pequena comunidade de desenvolvedores.

O terceiro é a normalização. A especificação R7 esteve parada em termos de novas funcionalidades o que fez com que funcionalidades como o suporte para telefonia a cabo tenham sido relegadas para a Release 8.

A especificação R5 é considerada incompleta e várias alterações significativas foram introduzidas na R6 e na R7 (como na infraestrutura) o que significa que os desenvolvimentos para a R6 terão que ser remodelados para o R7.

O quarto é o lançamento de equipamentos compatíveis. Os terminais (*handsets*) IMS são críticos para determinadas aplicações como IM e presença. No entanto, há aplicações que não necessitam ou podem contornar a necessidade, de terminais específicos.

O quinto desafio está relacionado com o lançamento de tecnologias recentes como o HSDPA *(High Speed Downlink Packet Access*) e HSUPA *(High Speed Uplink Packet Access*), sistemas rádio que fornecem banda larga a redes UMTS. Que aumentam a probabilidade de uma ou mais operadoras oferecer uma tarifa uniforme para o acesso à i*nternet*.

Esse tipo de tarifas, associados aos elevados débitos, aumentam a probabilidade de terceiros desenvolverem serviços (não IMS *compliant*) sobre essas redes.

Esses fatores aliados aos serviços implementados diretamente sobre IP ou sobre a i*nternet* trazem dificuldades à implementação do IMS. Contudo, esses serviços não usufruem da qualidade de serviço e segurança do IMS.

Como o IMS para as redes fixas só começou com a especificação R7, a maioria das implementações IMS são uma mistura de elementos SIP (IMS-*compliant* ou não) e redes tradicionais.

Sendo as redes fixas IMS tipicamente constituídas por circuitos de voz controlados por um *softswitch* com alguma infraestrutura SIP para novas aplicações como *instant messaging* ou convergência fixo-movel.

Contudo, há redes totalmente IMS a serem instaladas, mas são usadas apenas para novas aplicações como IM, FMC (*Fixed-Mobile Convergence*) e vídeo *sharing*; não como redes de telefonia básica.

Resumindo, as aplicações ou serviços atraentes ao público (aplicações rentáveis) são uma questão importante.

A normalização e interoperabilidade aumentam as opções disponíveis para a operadora quando pretende adquirir um equipamento, mas no final, só novas aplicações poderão aumentar os lucros.

No entanto, essas novas aplicações poderão não se refletir em novos serviços a baixo custo para os clientes; dependerá da abertura das operadoras ao desenvolvimento por terceiros.

O sexto desafio, como já mencionado anteriormente, são as falhas de segurança que a arquitetura IMS está sujeita e que podem atingir tanto as operadoras como os usuários da rede, questão essa que será abordada no Capítulo 5.

3.3. SIP – *Session Initiation Protocol*

O SIP (*Session Initiation Protocol*) é um protocolo da camada de controle para criação, modificação e finalização de sessões com um ou mais participantes. Essa sessão pode ser uma chamada simples ou poderia ser uma sessão de conferência multimídia colaborativa.

A habilidade de estabelecer essas sessões que suportam serviços se tornou possível, como o *e-commerce* com suporte à voz, *web-page click-to-dial, Instant Messaging* com listas de conhecidos e serviços PABX-IP.

Esse protocolo está em contínua evolução e está sendo extendido conforme a tecnologia se torna mais madura, assim como produtos que suportam SIP estão cada vez mais presentes no mercado.

A filosofia da IETF (*Internet Engineering Task Force*) é apenas especificar o que for necessário.

O SIP realiza muito desse conceito, uma vez que foi desenvolvido como um mecanismo de estabelecimento de sessões, onde não era necessário conhecer muitos detalhes das mesmas, apenas seu início, finalização e modificação.

Essa simplicidade torna o SIP escalável e extensível, uma vez que se adapta e se conecta a diferentes arquiteturas e cenários de desenvolvimento.

O SIP é um protocolo que solicita respostas (*request-response*) que se aproxima muito dos protocolos de i*nternet* HTTP e SMTP; consequentement o SIP se adapta confortavelmente com as aplicações de i*nternet*.

Ao utilizar esse protocolo, a telefonia se transforma em mais uma aplicação *web* e se integra facilmente com outros serviços da i*nternet* [14].

O SIP pode assim ser considerado uma ferramenta que os fornecedores de serviços podem utilizar para construir serviços convergentes de voz e de multimídia.

O protocolo SIP não possui nenhum mecanismo para descrever o conteúdo e suas características. Para isso, o SIP utiliza o protocolo SDP (*Session Description Protocol*) para tratar a informação de sessão. O SDP descreve a mídia a ser utilizada, *codecs*, o modo da chamada, etc.

Descreve também o destino da mídia (IP e número de porta), o nome da sessão e seu propósito, o número de vezes que a sessão foi ativada e as informações de contato.

O método SIP *INVITE* é utilizado para criar sessões que transportam descritores da sessão, o que permite que os participantes possam negociar um conjunto compatível de tipos de mídia.

O SIP foi projetado para solucionar apenas uma pequena quantidade de problemas e para trabalhar com uma gama de protocolos IP. Para exercer essa função, o SIP possui algumas funções básicas [14]:

- Estabelecimento de localização do usuário;
- Negociação de aplicações para que todos os participantes de uma sessão possam concordar quais aplicações são suportadas entre eles;
- Fornece gerenciamento de chamadas, através da adiçao, desligamento ou transferência de participantes.

3.3.1. Funcionalidade SIP

O principal objetivo do SIP é entregar uma descrição de sessão para um usuário na sua localização corrente.

Uma vez que o usuário tenha sido descoberto e a descrição de sessão inicial entregue, o SIP pode entregar novas descrições de sessão para modificar as características da sessão em curso e terminar a sessão sempre que o usuário ou a operadora desejarem.

Uma descrição de sessão é como o próprio nome indica a descrição de uma sessão a ser estabelecida. Ela contém informações suficientes para que o usuário remoto possa se juntar a sessão.

Em sessões multimídia sobre a i*nternet* essa informação inclui o endereço IP e o número da porta onde a mídia necessita ser enviada e os *codecs* usados para codificar a voz e as imagens dos participantes.

As descrições de sessão são criadas usando formatos padrões. O formato mais comum para descrever sessões multimídia é o SDP (*Session Description Protocol*), definido na RFC 2327 [40]. A Fig. 3.2 mostra um exemplo de uma descrição de sessão SDP enviada de Alice para Bob.

Ela contém, entre outras coisas, o assunto da conversação ("*Swimming techniques*"), o endereço IP da Alice (192.0.0.1), o número da porta onde Alice deseja receber áudio (20000), o número da porta onde Alice deseja receber vídeo (20002), e os *codecs* de áudio e vídeo que Alice suporta (0 corresponde ao *codec* de áudio G.711 μ-law e 31 corresponde ao *codec* de vídeo H.261).

```
v=0
o=Alice 2790844676 2867892807 IN IP4 192.0.0.1
s=Vamos falar sobre técnicas de natação
c=IN IP4 192.0.0.1
t=0 0
m=audio 20000 RTP/AVP 0
a=sendrecv
m=video 20002 RTP/AVP 31
a=sendrecv
```

Fig. 3.2 - Exemplo de uma descrição de sessão SDP [14].

Como se pode observar na Fig. 3.2 uma descrição SDP consiste em duas partes: informações do nível de sessão e informações do nível de mídia. As informações do nível de sessão se aplicam a sessão inteira e aparecem sempre antes das linhas m=.

A informação do nível de mídia refere-se a um fluxo de mídia específico e consiste de uma linha m= e de uma quantidade de linhas opcionais a= que provêem mais informações sobre o fluxo da mídia.

Como a Fig. 3.2 ilustra, o formato de toda linha SDP é da forma tipo=valor, onde tipo tem sempre o tamanho de um caractere.

No exemplo da Fig. 3.2 a descrição de sessão enviada, que contem o endereço de transporte do dono da sessão, não possui informação suficiente para estabelecer a sessão, pois o dono da sessão precisa saber o endereço de transporte da outra parte.

Assim, o SIP provê um modelo de troca de descrição de sessão em dois caminhos, chamado de modelo desafio/resposta, definido na RFC 3264 [42].

Nesse modelo, um dos usuários (o "desafiador") gera a descrição de sessão (o desafio) e envia-a para o usuário remoto (o "respondedor") o qual gera uma nova descrição de sessão (a resposta) e envia-a para o desafiador.

A RFC 3264 [42] fornece as regras para a geração do desafio e da resposta. Após a troca do desafio/resposta, ambos os usuários possuem uma visão comum da sessão a ser estabelecida.

Eles sabem, no mínimo, os formatos que poderão utilizar de *codecs* e os endereços de transporte para a sessão.

A troca do desafio/resposta também pode fornecer informação extra, como chave de cifragem para o tráfego cifrado.

No SIP, os usuários são identificados por SIP URI (*Uniform Resource Identifier*), as quais tem um formato de endereçamento similar ao endereço de e-mail, ou seja, consistem de um nome de usuário e de um nome de domínio.

Adicionalmente, as SIP URI podem conter parâmetros (por exemplo, transporte), que são inseridos utilizando-se ponto-e-vírgula.

Alguns exemplos de SIP URI são:

sip:Alice.Smith@*domain.com*

sip:Bob.Brown@*example.com*

sip:carol@ws1234.*domain2.com*;*transport*=tcp

O SIP provê a mobilidade do usuário através dos registros. Assim, o usuário pode ser encontrado usando o mesmo identificador não importando onde ele esteja. Por exemplo, Alice pode ser encontrada no endereço SIP URI abaixo a despeito de sua localização atual.

sip:Alice.Smith@*domain.com*

Esse é o seu SIP URI público, também conhecido como AoR (*Address of Record*). De outra forma, quando, por exemplo, Alice está conectada no trabalho, a sua SIP URI é:

sip:asmith@ws1234.*company.com*

Ou quando ela está em seu computador pessoal na universidade, a sua SIP URI é:

sip:alice@pc12.*university.edu*

Portanto, é necessária uma forma de mapear o endereço público SIP URI como endereço URI corrente (no trabalho ou na universidade) para qualquer dado momento.

Para fazer isso, o SIP introduz um elemento de rede chamado de servidor de registro (registrar ou *register server*) localizado no domínio particular, que manipula as requisições endereçadas para o seu domínio [14].

Isso significa que as requisições SIP enviadas para o endereço público SIP URI serão gerenciadas pelo servidor de registro do seu domínio.

Sempre que o usuário se registra em um novo local, ele registra sua nova localização no seu servidor de registro de domínio, como o exemplo mostrado na Fig. 3.3.

Dessa forma o servidor de registro de um domínio específico pode sempre encaminhar as requisições que chegam para um usuário de seu domínio onde quer que ele esteja, pois ele sempre terá a informação da localização atual do usuário.

Essa informação pode tanto ser armazenada no próprio registrar quanto pode ser mapeada em um servidor de localização. O registrar ou *register server* pode ser incluído em um servidor *proxy* ou em um *redirect server*.

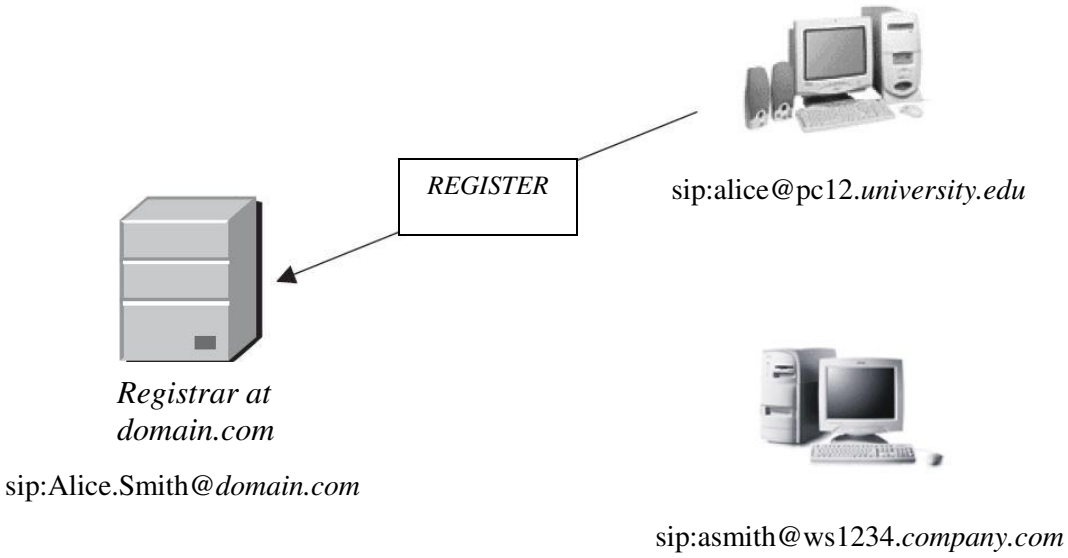

Fig. 3.3 - Exemplo de registro no servidor de registro de domínio "*domain.com*" [14].

3.3.2. Entidades SIP

Além dos *registrars*, o SIP define agentes usuário (UA - *User Agents*), servidores *proxy* (*proxy servers*) e servidores de redirecionamento (*redirect servers*). Os UA são pontos finais da comunicação multimídia e normalmente são utilizados por um usuário.

Porém, também há a possibilidade do UA estabelecer sessões automaticamente, sem intervenção do usuário, como no caso de uma caixa postal de voz SIP. No SIP, as sessões são tipicamente estabelecidas entre UA [2].

O UA possui dois componentes: um UAC (*User Agent Client*), que é responsável por iniciar as chamadas enviando as requisições, e um UAS (*User Agent Server*) responsável por responder as requisições do UAC.

Um UA tem a capacidade de atuar como UAC e UAS, porém de um modo a cada transação, dependendo de quem inicia o pedido. Os SIP UA, como mostrado na Fig. 3.4, são implementados em diversos tipos de sistemas.

Eles podem, por exemplo, operarem em um computador ou um dispositivo móvel PDA e celulares, através de uma aplicação, ou podem ser implementados em dispositivos dedicados como um telefone SIP.

Fig. 3.4 - Exemplos de UA [2].

Os *proxy servers*, normalmente chamados apenas de *proxy*, são roteadores SIP. O SIP *proxy server* recebe uma mensagem SIP de um UA ou de outro *proxy* e a redireciona até o seu destino.

Esse redirecionamento da requisição envolve a retransmissão da mensagem para o UA destinatário ou para outro *proxy* no caminho.

O SIP *proxy server* também disponibiliza serviços como: autenticação, autorização, controle de acessos, roteamento, retransmissões de pedidos e segurança.

Os *redirect servers* também são usados para rotear mensagens SIP, mas eles não simplesmente retransmitem a mensagem para o seu destino ou para o próximo *proxy*, como um servidor *proxy* faz.

O *redirect server* instrui a entidade que enviou a mensagem (um *user agent* ou um *proxy server*) para tentar uma nova localização ou outro endereço de destino.

A Fig. 3.5 mostra como um *redirect server* trabalha. Um agente usuário envia uma mensagem SIP para sip:Alice.Smith@*domain.com*, e o *redirect server* retorna o endereço alternativo sip:alice@pda.com.

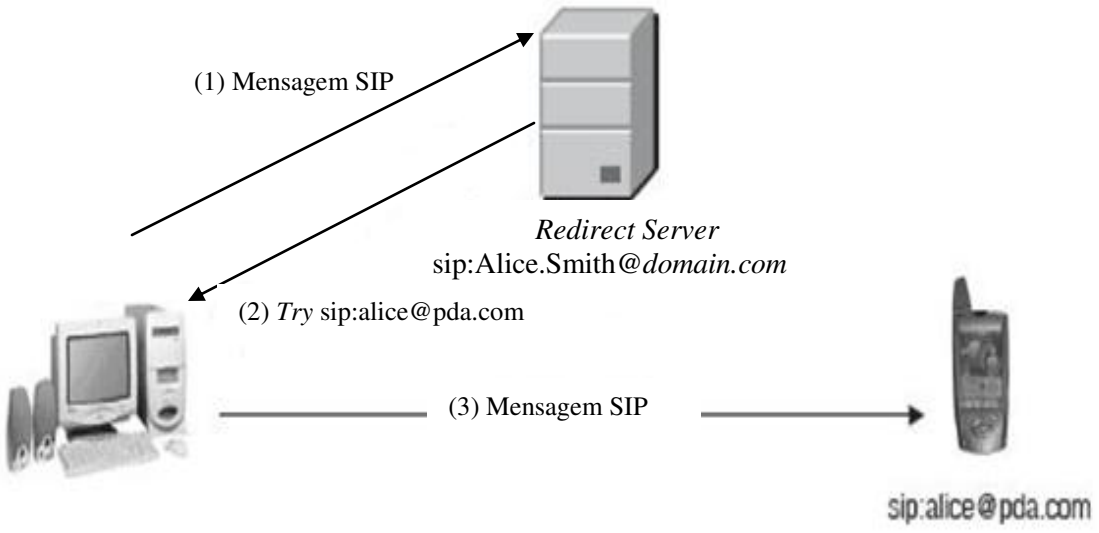

Fig. 3.5 - Exemplos de operação do *redirect server* [14].

3.3.3. Formato das Mensagens

O SIP é baseado em HTTP (*Hyper Text Transfer Protocol*) e, portanto, é um protocolo textual do tipo solicitação-resposta.

O cliente envia a solicitação e o servidor retorna com a resposta. Uma transação SIP consiste de uma solicitação de um cliente, nenhuma ou mais respostas provisórias e uma resposta final do servidor.

A Fig. 3.6 mostra o formato das mensagens SIP. Elas começam com o *start line*, o qual é chamado de *request line* nas solicitações e de *status line* nas respostas.

A *start line* é seguida por uma quantidade de *header fields* que possuem o formato nome: valor e uma linha vazia que separa os *header fields* da parte opcional do corpo da mensagem

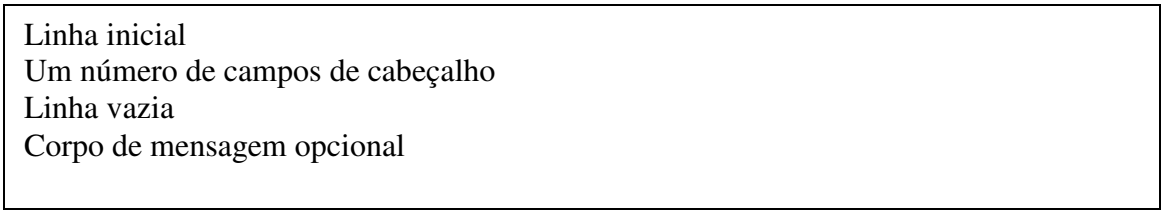

Fig. 3.6 - Formato da mensagem SIP [14].

A linha de *status* (*status line*), que é quando se tem a linha de *start line* como sendo de uma resposta, contém a versão do protocolo (SIP/2.0) e o status da transação, a qual é dada nos formatos de valor numérico (código de *status*) e texto (frase motivo).

A linha a seguir é um exemplo de linha de status:

SIP/2.0 180 *Ringing*

A versão do protocolo é sempre configurada para SIP/2.0. O código de status 180 indica que o usuário remoto está sendo alertado com relação a uma solicitação prévia.

Ringing é a frase motivo e se destina a ser lida por qualquer usuário (por exemplo, pode ser mostrada em um monitor ou *display* de dispositivo).

As respostas são classificadas por seus códigos de *status*, os quais são números inteiros na faixa de 100 a 699. A Tabela 3.1 mostra como os códigos de *status* são classificados de acordo com seus respectivos valores:

Tabela 3.1 - Faixa de códigos de status de resposta SIP [29].

Faixa do código de status	Significado
100 - 199	**Provisório (informativo)**
200 - 299	**Sucesso**
300 - 399	**Redireção**
400 - 499	**Erro no Cliente**
500 - 599	**Erro no Servidor**
600 - 699	**Falha Geral**

A linha de solicitação (*request line*), que é quando se tem a linha de *start line* como sendo de um pedido, contém o nome do método, endereço *request*-URI e a versão do protocolo (SIP/2.0).

O nome do método indica a finalidade do pedido e o *request*-URI o destinatário da solicitação. A linha a seguir é um exemplo de linha de solicitação:

INVITE sip:Alice.Smith@*domain.com* SIP/2.0

Nesse exemplo, o nome do método é *INVITE*, que indica que a finalidade desse pedido é convidar um usuário para uma sessão. O *request*-URI mostra que a solicitação é destinada para Alice.Smith.

A Tabela 3.2 mostra os métodos que atualmente estão definidos no SIP e seus significados.

Tabela 3.2 - Nome dos métodos nas requisições SIP [29].

Nome do método	Significado
ACK	**Reconhece o estabelecimento de uma sessão**
BYE	**Termina uma sessão**
CANCEL	**Cancela uma requisição pendente**
INFO	**Transporta sinalização de telefonia PSTN**
INVITE	**Estabelece uma sessão**
NOTIFY	**Notifica o *user agent* sobre um evento particular**
OPTIONs	**Consulta um servidor sobre seus recursos**
PRACK	**Reconhece a recepção de uma resposta provisória**
PUBLISH	**Carrega informação para um servidor**
REGISTER	**Mapeia um URI público com a localização corrente do usuário**
SUBSCRIBE	**Requisita para ser notificado sobre um determinado evento**
UPDATE	**Modifica algumas características de uma sessão**
MESSAGE	**Carrega uma mensagem instantânea**
REFER	**Instrui um servidor para enviar uma requisição**

Para exemplificar, a Fig. 3.7 mostra uma transação SIP. O agente usuário cliente (UAC) envia um pedido *BYE* e o agente usuário servidor (UAS) retorna a resposta 200 (OK).

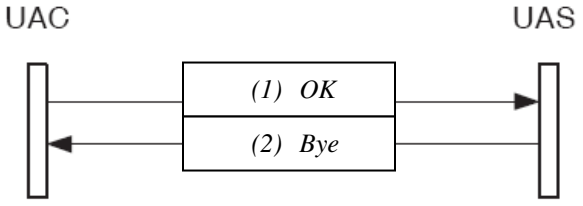

Fig. 3.7 - Transação SIP [14].

Logo após o *start line*, as mensagens SIP (tanto de solicitação quanto de resposta) contêm um conjunto de *header fields*.

Alguns *headeres fields* são mandatórios, que aparecem em todas as mensagens, e *header fields* opcionais, que somente aparecem quando são necessários.

Um *header field* é composto pelo nome do campo, o sinal de dois-pontos, e o valor do campo, como nos exemplos abaixo:

To: Alice Smith <sip:Alice.smith@domain.com>;tag=1234

Route: <sip:p1.domain1.com>, <sip:p34.domain2.com>

Existem seis campos mandatórios de *header fields* que devem aparecer em toda mensagem SIP. São eles: *To, From, Cseq, Call-ID, Max-Forwards e Via*.

- *To*: o campo *To* contém o endereço URI do destinatário da solicitação. Porém, esse URI não é usado para encaminhar a requisição. Basicamente é utilizado em interface humana e com finalidade de filtragem pelo campo do destinatário.
- *From*: esse campo contém o endereço URI do originador da requisição. Como no campo *To*, é principalmente para fins de interface e de filtragem.
- Cseq: o campo Cseq contém um numero seqüencial e o nome do método. Eles são usados para fazer a correspondência entre requisições e respostas.
- *Call*-ID: o *Call*-ID fornece um identificador único para a troca de mensagem SIP.
- Max-*Forwards*: esse campo é utilizado para evitar *loops* de roteamento. Cada *proxy* que trata uma requisição decrementa o valor desse campo de um. Se o campo *max-forwards* alcança o valor de zero, a requisição é descartada.
- Via: o campo Via monitora o caminho trilhado por uma requisição através dos *proxies* que passou. A resposta utiliza as informações armazenadas no campo Via para enviar-las através dos mesmos *proxies*, na direção oposta.

Como visto na Fig. 3.8, o corpo da mensagem é separado do *header fields* por uma linha vazia. O SIP pode transportar qualquer corpo de mensagem e até mesmo corpo de mensagem multi-partes usando a codificação MIME (*Multipurpose Internet Mail Extensions*).

O formato MIME permite o envio de *e-mails* com múltiplos arquivos anexos e em diferentes formatos. Assim, o SIP utiliza o MIME para codificar o corpo das mensagens da que os anexos de uma mensagem de *e-mail*.

O conjunto de *header fields* fornece informação sobre o corpo da mensagem: seu tamanho, formato, e como deve ser manuseado.

Um exemplo de corpo de mensagem multi-parte codificado usando MIME é mostrado na Fig. 3.8. A primeira parte do corpo da mensagem é uma descrição de sessão SDP e a segunda parte consiste do texto "*This is the second body part*".

MIME-*Version*: 5.0
Content-Type: multipart/mixed; boundary=frontier
Content-Length: 384

-- *frontier*
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64

v=0
o=Alice 2790844676 2867892807 IN IP4 192.0.0.1
s=Vamos falar sobre técnicas de natação
c=IN IP4 192.0.0.1
t=0 0
m=audio 20000 RTP/AVP 0
a=*sendrecv*
m=video 20002 RTP/AVP 31
a=*sendrecv*
-- *frontier*
Content-Type: text/plain;

Esta é a segunda parte do corpo de mensagem
-- *frontier*

Fig. 3.8 - Codificação MIME de corpo de mensagem multi-parte [14].

Uma propriedade importante dos corpos de mensagem é que eles são transmitidos fim-a-fim. Isso significa que os *proxies* não necessitam decodificar o corpo da mensagem.

De fato, os agentes usuários podem escolher cifrar o conteúdo do corpo da mensagem fim-a-fim. Nesse caso, os *proxies* não são capazes de dizer qual o tipo de sessão será estabelecido entre ambos os agentes usuários.

3.3.4. Fluxo de Mensagens para Estabelecimento de Sessão

O SIP define três tipos de transações, dependendo do tipo da solicitação inicial. São elas: transações regulares, transações do tipo *INVITE-ACK*, e transações do tipo *CANCEL*.

As transações regulares são iniciadas por qualquer pedido menos *INVITE, ACK* ou *CANCEL*. A Fig. 3.9 mostra uma transação regular *BYE*. Em uma transação regular o usuário agente servidor (UAS) recebe um pedido e gera uma resposta final que termina a transação.

Em teoria, seria possível para o agente usuário servidor (UAS) gerar uma ou mais respostas provisórias antes de gerar a resposta final, embora na prática, respostas provisórias raramente são enviadas dentro de uma transação regular.

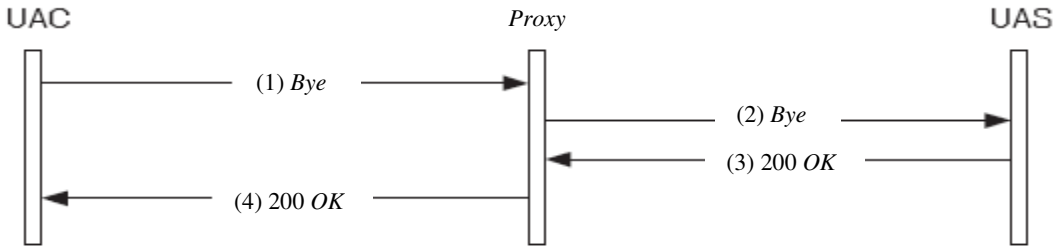

Fig. 3.9 - Transação regular [14].

Uma transação *INVITE-ACK* envolve duas transações: uma transação *INVITE* e uma transação *ACK*, como mostra a Fig. 3.10.

O usuário agente servidor (UAS) recebe uma requisição *INVITE* e gera nenhuma ou mais respostas provisórias e uma resposta final.

Quando o agente usuário cliente (UAC) recebe a resposta final, ele gera uma requisição *ACK*, a qual não tem nenhuma resposta associada a ela.

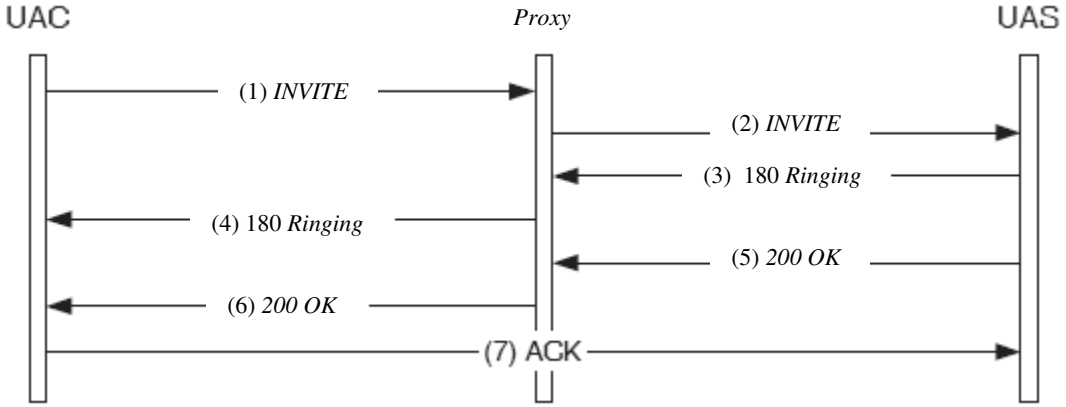

Fig. 3.10 - Transação *INVITE-ACK* [14].

As transações do tipo *CANCEL* são iniciadas por uma solicitação *CANCEL* e estão sempre relacionadas a uma transação previa (a transação a ser cancelada).

As transações *CANCEL* são similares às transações regulares, com a diferença de que a resposta final é gerada pelo próximo salto SIP (tipicamente um *proxy*) ao invés de ser gerada pelo usuário agente servidor.

Para exemplificar, a Fig. 3.11 mostra uma transação *CANCEL* cancelando uma transação *INVITE*.

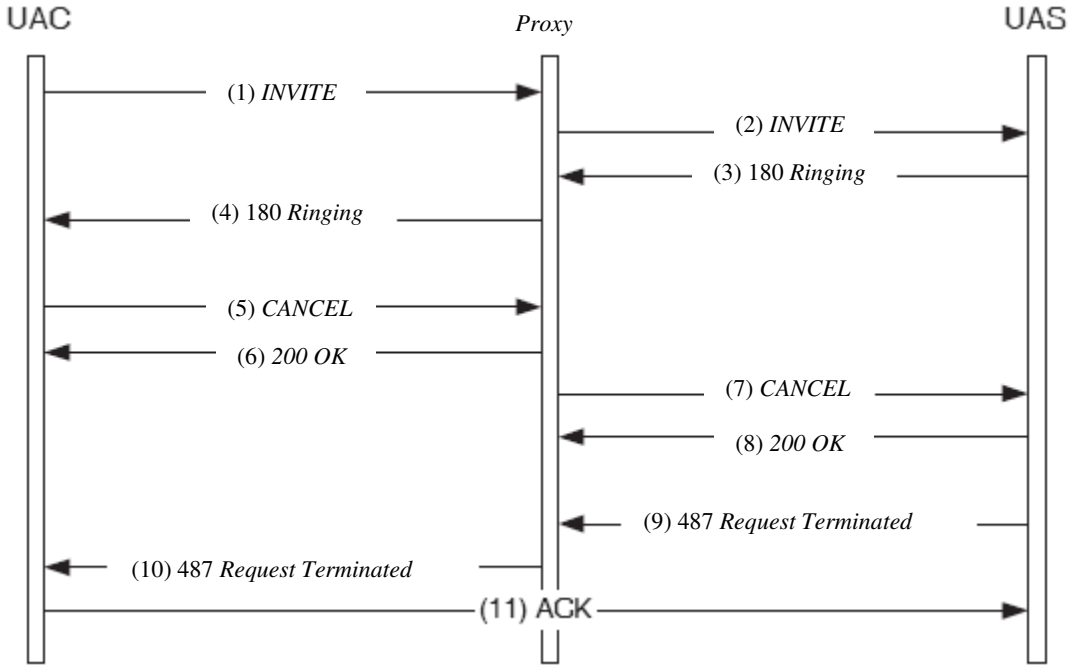

Fig. 3.11 - Transação *CANCEL* [14].

A partir do conhecimento dos diferentes tipos de transações SIP, pode-se verificar como o SIP é utilizado para estabelecer sessões multimídia.

O primeiro evento necessário é o registro do usuário, com sua localização corrente no servidor de registro (registrar), como mostrado na Fig. 3.12.

Fig. 3.12 - Registro de usuário com sua localização [14].

Para que o registro aconteça, o usuário envia uma requisição do tipo *REGISTER*, como descrito na Fig. 3.13, indicando que os pedidos dirigidos para o endereço URI no campo To do *header field* deve ser retransmitido para o endereço URI do campo *contact* do *header filed*.

REGISTER sip: *domain*.com SIP/2.0
Via: SIP/2.0/UDP 192.0.0.0:5060; *branch*=z9hG4bKna43f
Max-Forwards: 70
To: <sip: Alice.Smith@*domain*.com>
From: <sip:Alice@pda.com>; tag=453448
Call-ID: 843528637684230@998sdasdsfgt
Cseq: 1 *REGISTER*
Contact: <sip: alice@pda.com>
Expires: 7200
Content-Length: 0

Fig. 3.13 - Exemplo de mensagem SIP *REGISTER* [14].

O servidor de registro retorna com uma resposta 200 (OK), como descrito na Fig. 3.14, indicando que a transação foi completada com sucesso.

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.0.0:5060; *branch*=z9hG4bKna43f
; *received*=192.0.0.1
To: <sip: Alice.Smith@*domain*.com>; *tag*=54262
From: <sip:Alice@pda.com>; tag=453448
Call-ID: 843528637684230@998sdasdsfgt
Cseq: 1 *REGISTER*
Contact: <sip: alice@pda.com>
Expires: 7200
Content-Length: 0

Fig. 3.14 - Exemplo de resposta 200 (OK) à solicitação SIP *REGISTER* [14].

Após o registro do usuário é possível, dessa forma, o estabelecimento de uma sessão multimídia.

Para se estabelecer esse tipo de sessão, um usuário deve enviar uma solicitação do tipo *INVITE* usando o endereço URI público do outro usuário como endereço URI de requisição, como mostra a Fig. 3.15, através de um servidor *proxy* do domínio.

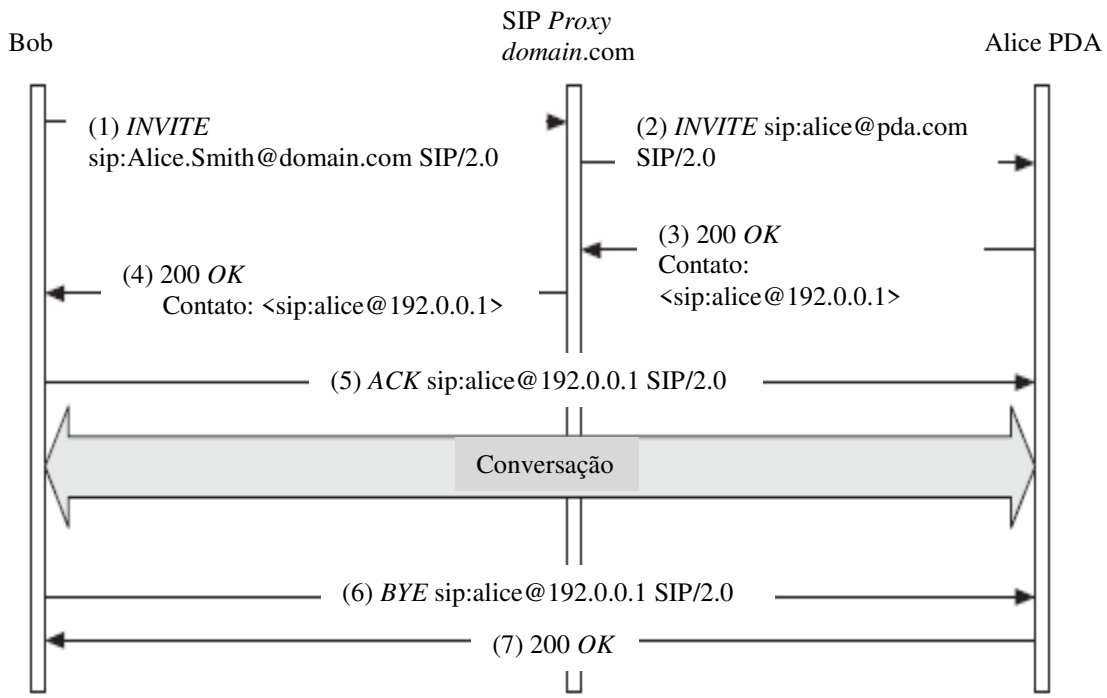

Fig. 3.15 - Estabelecimento de sessão através de um *proxy* [14].

No caso de uma sessão de áudio, a mensagem de requisição teria o formato mostrado na Fig. 3.16.

INVITE sip: Alice.Smith@*domain*.com SIP/2.0
Via: SIP/2.0/UDP ws1.*domain*2.com:5060; *branch*=z9hG4bK74gh5
Max-Forwards: 70
From: Bob <sip: Bob.Brown@*domain*2.com>; *tag*=9hx34576s1
To: Alice <sip: Alice.Smith@*domain*.com>
Call-ID: 6328776298220188511@192.0.100.2
Cseq: 1 *INVITE*
Contato: <sip: bob@192.0.100.2>
Content-Type: *application*/sdp
Content-Length: 151

v=0
o=bob 2890844526 2890844526 IN IP4 ws1.*domain*2.com
s=-
c=IN IP4 192.0.100.2
t=0 0
m=audio 20000 RTP/AVP 0
a= rtpmap: 0 PCMU/8000

Fig. 3.16 - Exemplo de mensagem *INVITE* para estabelecimento de sessão [14].

Nesse caso, o *proxy* que recebe a mensagem externa, retransmite a requisição de *INVITE* até o destinatário, porém em sua localização corrente (por exemplo, se o último registro for um dispositivo PDA, a requisição será enviada para esse UAC).

O usuário requisitado então aceita o convite enviando uma resposta do tipo 200 (OK), que é retransmitida para o usuário requisitante, como mostra a Fig. 3.17.

SIP/2.0 200 *OK*
Via: SIP/2.0/UDP ws1.*domain*2.com:5060; *branch*=z9hG4bK74gh5
; *received*=192.0.100.2
From: Bob <sip: Bob.Brown@*domain*2.com>; *tag*=9hx34576s1
To: Alice <sip: Alice.Smith@*domain*.com>; *tag*=1df345fkj
Call-ID: 6328776298220188511@192.0.100.2
Cseq: 1 *INVITE*
Contato: <sip: alice@192.0.0.1>
Content-Type: *application*/sdp
Content-Length: 151

v=0
o=alice 2890844545 2890844545 IN IP4 192.0.0.1
s=-
c=IN IP4 192.0.0.1
t=0 0
m=audio 30000 RTP/AVP 0
a= rtpmap: 0 PCMU/8000

Fig. 3.17 - Resposta 200 (OK) para um *INVITE* de estabelecimento de sessão [14].

Em ambas as mensagens, a requisição *INVITE* e a resposta de confirmação 200 (OK), os usuários incluem o campo *contact* no *header field*, para que dessa forma possam trocar mensagens, depois de estabelecida a sessão, diretamente, sem necessidade do *proxy server*.

Para que a sessão finalmente se estabeleça e haja a troca de mídia (por exemplo, áudio), o usuário deve, após o recebimento da resposta 200 (OK), confirmar a sessão enviando a mensagem de reconhecimento *ACK* (transação *INVITE-ACK*).

Se, após o estabelecimento da sessão, os usuários queiram fazer qualquer modificação na mesma, por exemplo, adicionar vídeo, tudo o que necessitam fazer é enviar outra requisição de *INVITE* com uma atualização da descrição da sessão.

Quando os usuários terminam a conversação, qualquer um deles pode terminar a sessão enviando uma mensagem de requisição *BYE*, como exemplificada na Fig. 3.18.

BYE sip: alice@192.0.0.1 SIP/2.0
Via: SIP/2.0/UDP ws1.*domain*2.com:5060; *branch*=z9hG4bK74gh5
Max-Forwards: 70
From: Bob <sip: Bob.Brown@*domain*2.com>; *tag*=9hx34576s1
To: Alice <sip: Alice.Smith@*domain*.com>; *tag*=1df345fkj
Call-ID: 6328776298220188511@192.0.100.2
Cseq: 2 *BYE*
Contato: <sip: bob@192.0.100.2>
Content-Length: 0

Fig. 3.18 - Exemplo de mensagem *BYE* para terminar uma sessão [14].

A mensagem de requisição *BYE* é respondida pelo outro usuário com a resposta 200 (OK), como mostra a Fig. 3.19.

SIP/2.0 200 *OK*
Via: SIP/2.0/UDP ws1.*domain*2.com:5060; *branch*=z9hG4bK74gh5
; received=192.0.100.2
From: Bob <sip: Bob.Brown@*domain*2.com>; *tag*=9hx34576s1
To: Alice <sip: Alice.Smith@*domain*.com>; *tag*=1df345fkj
Call-ID: 6328776298220188511@192.0.100.2
Cseq: 2 *BYE*
Contato: <sip: alice@192.0.0.1>
Content-Length: 0

Fig. 3.19 - Resposta 200 (OK) para a requisição *BYE* [14].

Dessa forma, para estabelecer, atualizar ou terminar sessões é necessário o fluxo e a troca de mensagens SIP.

A essa troca de um conjunto de mensagens SIP entre dois agentes usuários é dado o nome de diálogo SIP.

Portanto, os diálogos SIP são montados de acordo com o tipo de transação utilizada no estabelecimento, atualização ou termino de sessões.

3.3.5. Extensão do SIP

O mecanismo de negociação de extensão do SIP utiliza três campos do *header fields*: *supported*, *required*, e *unsupported*.

Quando um diálogo SIP está sendo estabelecido, o agente usuário cliente lista todos os nomes de extensões que ele quer usar para o diálogo.

No campo *require* dentro do *header field*, e todos os nomes de extensões que ele suporta não listados previamente no campo *supported*. Os nomes das extensões são referenciados como *option tags*.

O agente usuário servidor inspeciona o campo *require* dentro do *header field* e, se ele não suportar qualquer das extensões listadas no campo, ele envia para o agente usuário cliente uma resposta de erro indicando que o diálogo não pode ser estabelecido.

Essa resposta de erro contém o campo *supported* no *header field* listando as extensões que o agente usuário servidor não suporta.

Se o agente usuário servidor suportar todas as extensões requeridas, ele decidirá se quer ou não usar qualquer extensão extra para esse diálogo.

Em caso afirmativo, deverá incluir o *option tag* para a extensão extra no campo *require* do *header field*, na sua resposta. A partir daí o diálogo será estabelecido.

A Fig. 3.20 mostra uma negociação de extensão com sucesso. Eles concluem a negociação usando as extensões cujos *option tags* são foo1, foo2 e foo4.

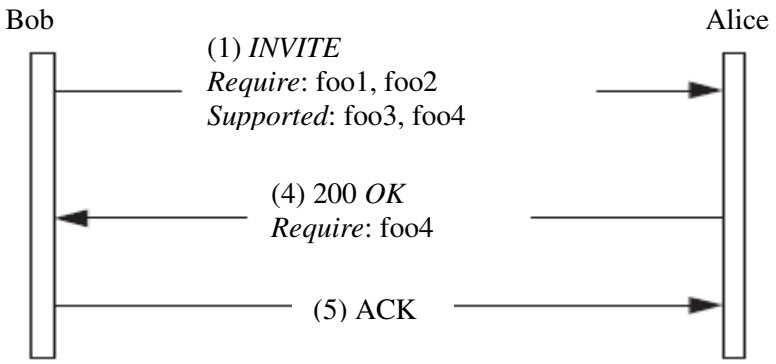

Fig. 3.20 - Negociação de extensão no SIP [14].

Além dos *option tags*, o SIP pode ser estendido através da definição de novos métodos. A Tabela 3.2 mostra que existem muitos métodos SIP, mas o núcleo do protocolo apenas usa um subconjunto deles. Os demais métodos são definidos em extensões do SIP.

3.3.6. Pré-Condições

Para que uma sessão SIP seja estabelecida, além do aceite do usuário chamado e que o usuário agente servidor suporte as extensões requeridas, algumas pré-condições podem ser requeridas antes do estabelecimento de uma sessão.

Por exemplo, um usuário pode querer falar com outro usuário contanto que a qualidade de voz seja aceitável. Nesse caso, se a rede não pode assegurar certa banda ou *throughput* durante toda a sessão, o chamador pode preferir não estabelecer a sessão.

A extensão que permite um agente usuário expressar uma pré-condição, cujo *option tag* é *precondition*, é uma mistura de extensão do SIP e do SDP.

Quando um agente usuário recebe uma oferta com precondições, ele não alerta o usuário até que aquelas precondições sejam encontradas. Essas pré-condições são codificadas no corpo SDP da mensagem.

Existem dois tipos de pré-condições: pré-condições de acesso e pré-condições fim-a-fim. A Fig. 3.21 mostra um SDP com pré-condições de acesso.

O agente usuário que gerou essa descrição de sessão está requisitando (a=des:qos significa que deseja QoS) QoS em ambas as direções (sendrecv) em ambos os acessos; no acesso local (local) e no acesso remoto (*remote*).A linha a=curr:qos indica que, no momento, não há QoS em qualquer dos acessos.

```
m=audio 20000 RTP/AVP 0
a=curr: qos local none
a=curr: qos remote none
a=des: qos mandatory local sendrecv
a=des: qos mandatory remote sendrecv
```

Fig. 3.21 - Pré-condição de acesso [14].

A Fig. 3.22 mostra um SDP com pré-condições fim-a-fim. O agente usuário que gerou essa descrição de sessão está requisitando a opção da QoS fim-a-fim (e2e) em ambas as direções (sendrecv).

```
m=audio 20000 RTP/AVP 0
a=curr: qos e2e none
a=des: qos optional e2e sendrecv
```

Fig. 3.22 - Pré-condição fim-a-fim [14].

Quando uma precondição mandatória aparece em uma descrição de sessão o usuário chamado somente é alertado quando as condições da QoS corrente são iguais ou melhores que as condições desejadas.

De forma, a saber, quando todas as pré-condições são encontradas, ambos os agentes necessitam trocar descrições de sessão. Essa troca de descrição de sessão é enviada usando o método UPDATE, como mostrado na Fig. 3.23.

Usando esse método, ambos os agentes mantém um ao outro atualizado sobre o *status* das pré-condições.

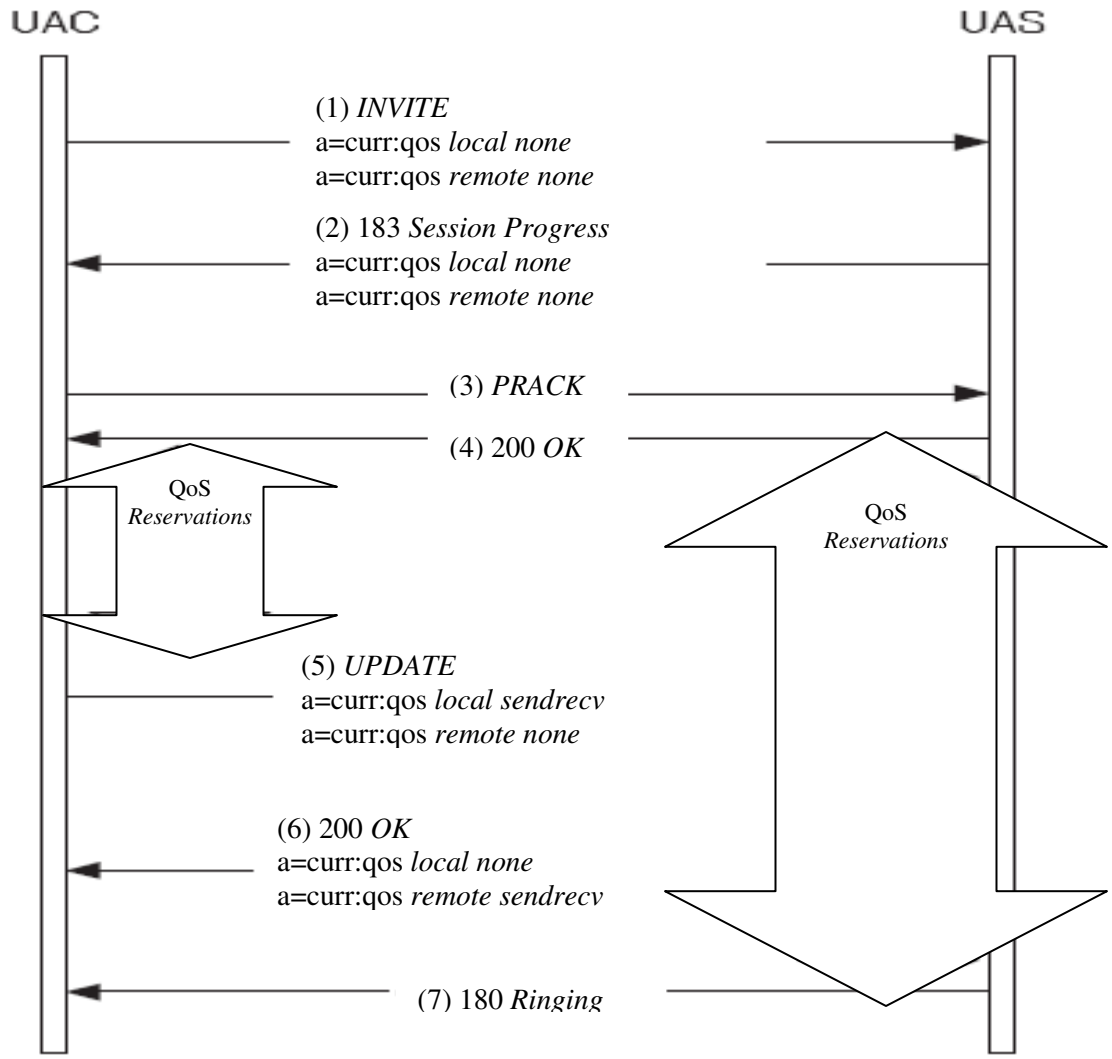

Fig. 3.23 - O método *UPDATE* [14].

Na Fig. 3.24, uma vez que a primeira descrição de sessão foi trocada, ambos os usuários executam a reserva da QoS em seus respectivos acessos.

Quando o agente usuário cliente termina sua reserva, ele envia uma requisição de UPDATE informando ao agente usuário servidor (a=curr: qos local sendrecv).

Quando o agente usuário servidor finalizar sua reserva da QoS, todas as pré-condições serão encontradas e o usuário chamado será alertado.

```
m=audio 20000 RTP/AVP 0
a=curr: qos local sendrecv
a=curr: qos remote none
a=des: qos mandatory local sendrecv
a=des: qos mandatory remote sendrecv
```

Fig. 3.24 - Atualização das condições da QoS corrente [14].

CAPÍTULO 4

A ARQUITETURA DE SEGURANÇA DO IMS

No PS (*Packet-Switched)* domínio, o serviço não é inicializado até uma associação de segurança ser estabelecida entre o UE (*User Equipament*) e a rede. O IMS é essencialmente um *overlay* para o *PS-domain* e tem uma dependência baixa do *PS-domain*.

Conseqüentemente, uma associação de segurança separada é necessária entre o cliente multimídia e o IMS para obter acesso aos serviços multimídia. A Arquitetura de Segurança do IMS é mostrada na Fig. 4.1.

Chaves de autenticação do IMS e funções para o usuário devem ser armazenadas em um UICC. Conforme [5] é recomendado que as chaves de autenticação do IMS e funções fiquem logicamente independentes das chaves e funções usadas para a autenticação no PS-*domain*.

O ISIM é um termo que indica a coleção de dados e funções de segurança do IMS no UICC.

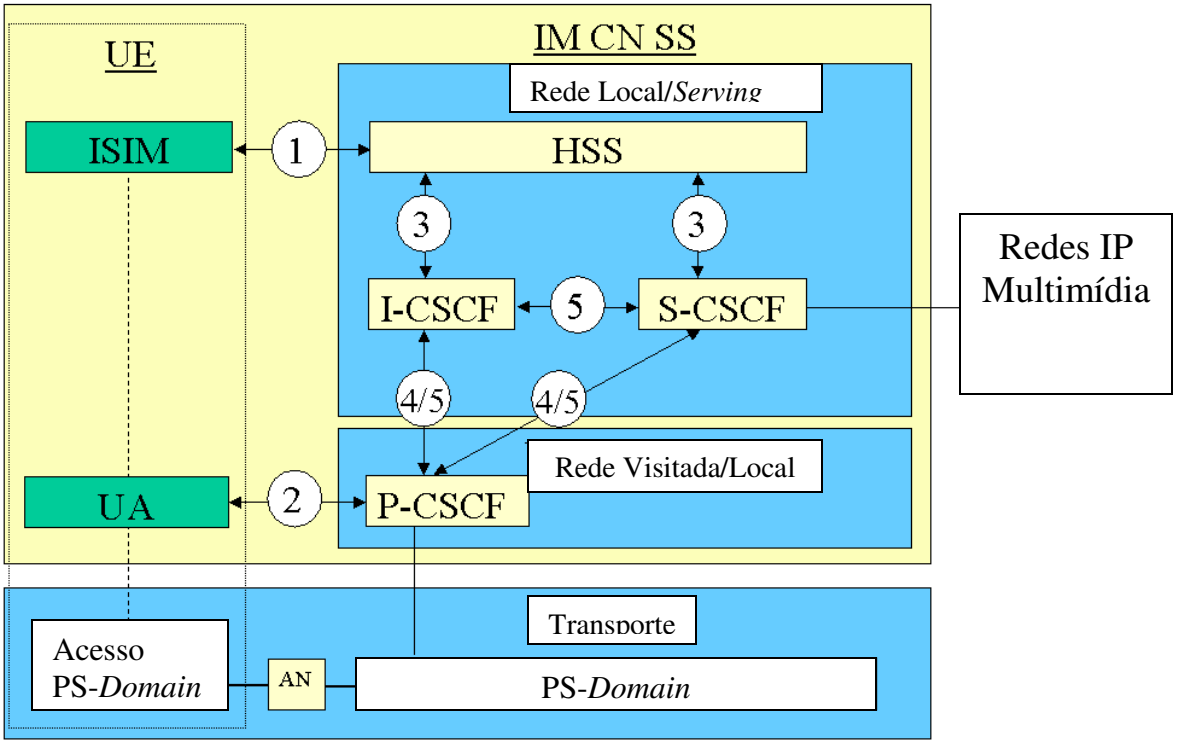

Fig. 4.1 - Arquitetura de segurança do IMS [5].

A arquitetura identifica cinco diferentes associações de segurança e necessidades para implementar uma proteção segura para o IMS [3GPP], que são numerados de 1 a 5 na Fig. 4.1 acima, onde [5]:

1. Autenticação mútua entre o UE (*User Equipment*) e o IMS. O HSS (*Home Subscriber Server*) delega essa função para o S-CSCF (*Serving - Call Session Control Function*) mas o HSS é reponsável por gerar as chaves de segurança.

As chaves permanentes no ISIM e o HSS estão associados com o IMPI. O assinante terá uma (rede interna) identidade de usuário privada (IMPI) e no mínimo uma identidade de usuário pública externa (IMPU).

2. Link de segurança e associações de segurança entre o UE e P-CSCF (*Proxy - Call Session Control Function*) para autenticação de dados de origem.

3. Providencia segurança interna para o link entre o CSCF e HSS. Isso é conhecido como Cx *interface*. Essa associação tem um papel importante nas chaves de segurança durante o UE processo de registro.

4. Providencia segurança entre o P-CSCF e outro núcleo de serviço SIP quando o UE está em *roaming*.

5. Providencia segurança entre o P-CSCF e outro núcleo de serviço SIP quando o UE está operando em *Home Network* (HN).

Existem outras interfaces e pontos de referência no IMS, que não foram abordadas na figura acima. Essas interfaces e pontos de referência residem no IMS, quer dentro do mesmo domínio de segurança, ou entre domínios de segurança diferentes.

A proteção de todas essas *interfaces* e pontos de referência além do ponto de referência Gm são protegidas conforme especificado em [5].

Autenticação mútua é necessária entre a UE e o HN. Esses mecanismos de segurança mencionados são independentes dos mecanismos definidos para o CS e PS-*domain*.

Um mecanismo de segurança IMS independente fornece proteção adicional contra falhas de segurança. Por exemplo, se a segurança no *PS-domain* é violada o IMS vai continuar a ser protegido pelo seu mecanismo de segurança própria.

Como indicado na Fig. 4.2 e 4.3, o P-CSCF pode estar localizado tanto na rede visitada ou na rede origem. O P-CSCF será co-localizado dentro da mesma rede que o GGSN, que podem residir no VPLMN ou HPLMN de acordo com os critérios de seleção na APN[6] e GGSN.

[6] APN é um identificador de rede configurável usado por um dispositivo móvel ao conectar uma operadora GSM.

P-CSCF na Rede Visitada

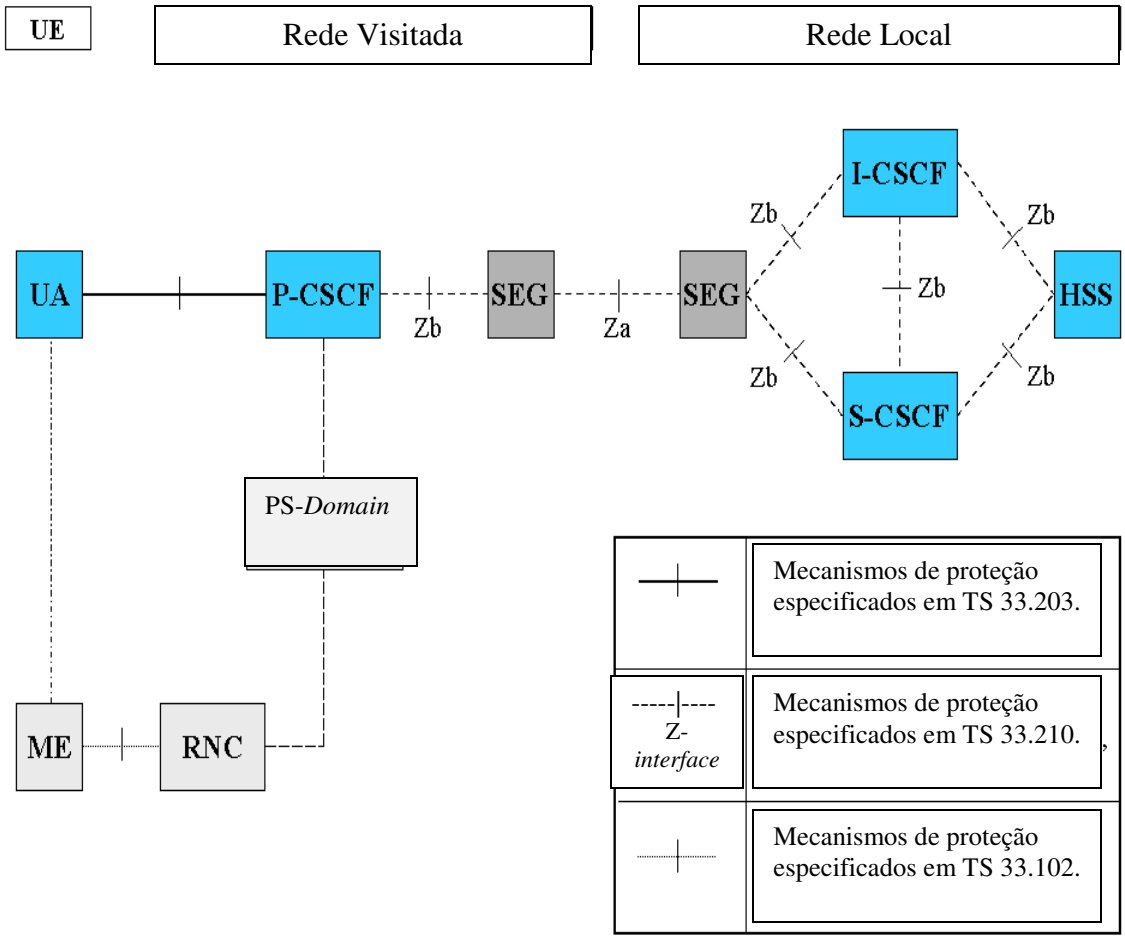

Fig. 4.2 - Arquitetura de segurança do IMS quando P-CSCF está localizado na rede visitada [5].

P-CSCF na Rede Origem

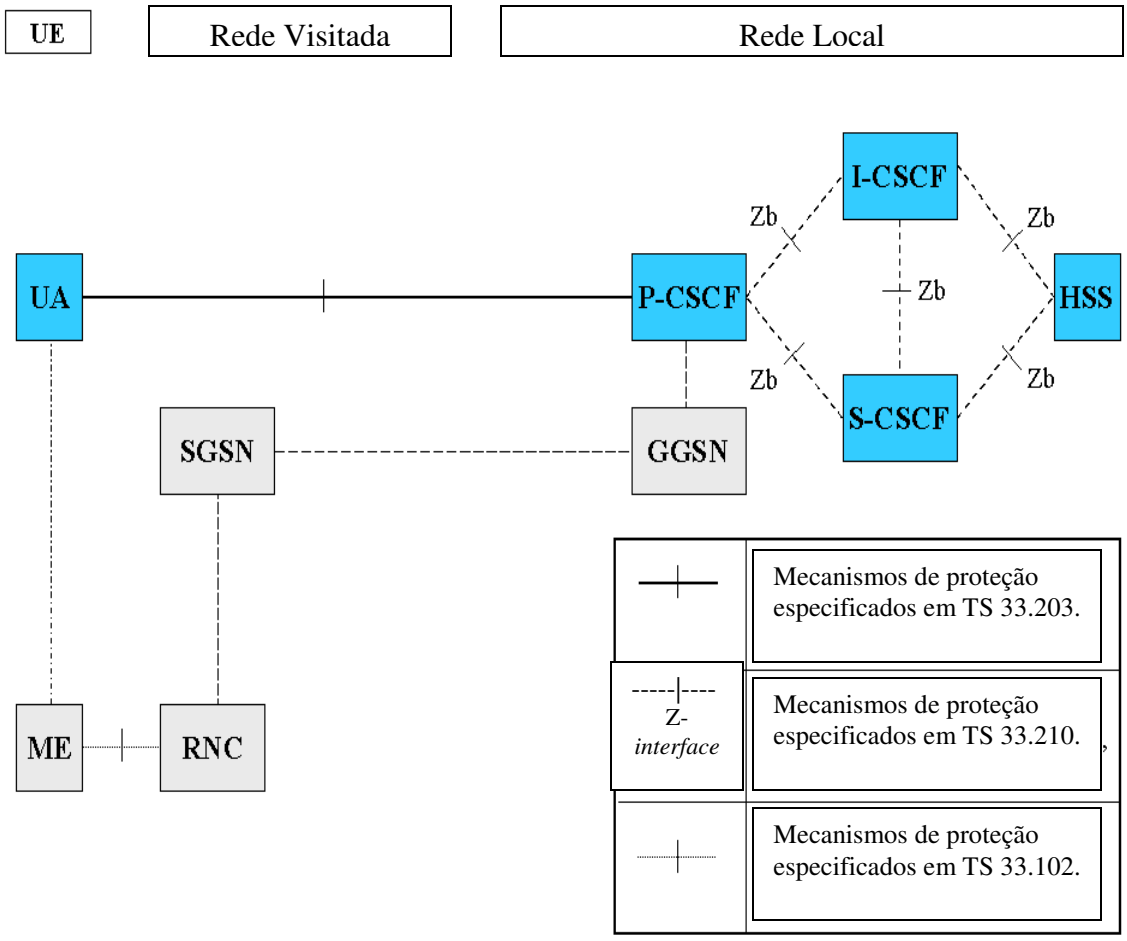

Fig. 4.3 - Arquitetura de segurança do IMS quando P-CSCF está localizado na rede origem [5].

4.1. Recursos de Segurança e Acesso Seguro ao IMS

No processo de autenticação entre o assinante e a rede, o assinante do IMS tem seu perfil de assinante localizado no HSS na rede origem. O perfil do assinante contém informações do assinante que não podem ser reveladas para usuários externos.

Durante o procedimento de *registration* um S-CSCF é atribuído para o assinante pelo I-CSCF. O perfil do assinante será baixado para o S-CSCF através do ponto Cx-reference do HSS (Cx-Pull).

Quando um assinante requisita acesso para o *IP multimedia core network subsystem* o S-CSCF fará as verificações necessárias, combinando o pedido com o perfil do assinante, se o

assinante está autorizado a continuar com o pedido ou não, o que é chamado de *home control* (*authorization* de IM-*services*).

Toda sinalização SIP é processada através do *PS-domain* no plano do usuário, porque o *IP multimedia core network subsystem* é essencialmente um *overlay* do *PS-domain*.

Portanto a rede visitada terá controle de todos os assinantes no *PS-domain*, o que é chamado de *visited control* (autorização de recursos da prestadora) desde que a rede visitada providencie o assinante com os serviços de transporte associado com QoS.

Para os serviços IMS uma nova associação de segurança é necessária entre o UE e o IMS antes que seja concedido acesso a esses serviços.

O mecanismo para autenticação mútua no UMTS é chamada UMTS AKA. O AuC (*Authentication Center*) no *home stratum* deriva as chaves de segurança, que são enviadas do *home stratum* para o *serving network*.

O *service network* compara a resposta do UE com o XRES e se eles combinam o UE é autenticado, o UE calcula o esperado MAC, XMAC, e compara esse com o MAC recebido e se eles combinam o UE é autenticado no *serving network*.

O protocolo AKA é um protocolo de segurança desenvolvido para UMTS e o mesmo conceito e princípios serão reutilizados para o *IP multimedia core network subsystem*, onde é chamado IMS AKA [5].

Embora o método de cálculo dos parâmetros em UTMS AKA e IMS AKA seja idêntico, os parâmetros são transportados de forma ligeiramente diferente.

No UMTS, o parâmetro RES é encaminhado sozinho, enquanto que no IMS RES não é encaminhado sozinho mas combinado com outros parâmetros para formar uma resposta de autenticação e a resposta de autenticação é enviada para a rede.

A rede origem autentica o assinante a qualquer momento via os procedimentos de *registration* ou *re-registration*.

O processo de *registration* inicial deve ser sempre autenticado, é política da operadora decidir quando acionar o processo de *re-autenticação* pelo S-CSCF.

Dessa forma, o processo de *re-registration* pode não precisar ser autenticado. Uma mensagem SIP *REGISTER*, que não tenha tido a integridade protegida num primeiro momento, será considerado para um processo de *registration* inicial.

O S-CSCF deve também ser capaz de iniciar uma autenticação de um processo de *re-registration* de um usuário a qualquer momento.

Com relação a proteção de confidencialidade para as mensagens de sinalização SIP entre o UE e o P-CSCF os seguintes mecanismos são fornecido na camada SIP:

· O UE encaminha algoritmos de criptografia para o P-CSCF para ser usado para a sessão;
· O P-CSCF decide se o mecanismo de criptografia específico do IMS será utilizado.

Se for utilizado, o UE e o P-CSCF devem concordar com as associações de segurança, que incluem chave de criptografia que será utilizada para a proteção da confidencialidade. O mecanismo é baseado em IMS AKA[7].

A proteção de integridade é aplicada entre o UE e o P-CSCF para proteger a sinalização SIP, dessa forma o IMS fornece os seguintes mecanismos [5]:
· O UE e o P-CSCF negociam o algoritmo de integridade que deve ser utilizados para a sessão;
· O UE e o P-CSCF mantém um acordo com as associações de segurança, que incluem as chaves de integridade que devem ser utilizados para a proteção da integridade. O mecanismo é baseado em IMS AKA;
· O UE e o P-CSCF fazem a verificação que os dados recebidos originam de um nó, que tem a chave de integridade já estabelecida. Essa verificação também é utilizada para detectar se os dados foram adulterados.

Outro ponto a salientar, seria com relação a topologia de rede das operadoras que usam o IMS. Os detalhes operacionais da rede de uma operadora são informações comerciais confidenciais e sensíveis aos negócios que as operadoras são relutantes em compartilhar com os seus concorrentes.

Embora possa haver situações (parcerias ou relações comerciais), onde o compartilhamento de tal informação é adequado, essa decisão de compartilhar ou não os detalhes operacionais da rede deve partir da própria operadora, que dessa forma deve decidir se compartilha ou não os detalhes internos de sua rede.

Dessa forma a operadora pode não revelar detalhes de sua topologia de rede, que inclui detalhes sobre número de S-CSCF, as capacidades do S-CSCF e a capacidade da rede.

O I-CSCF/IBCF tem a capacidade de criptografar os endereços de todas as entidades da rede da operadora via SIP, *record route-route* e *path headers* e depois descriptografar os endereços ao tratar a resposta a um pedido.

O P-CSCF pode receber informações de roteamento que é criptografado, mas o P-CSCF não terá a chave para descriptografar essa informação.

O IMS suporta o cenário que diferentes I-CSCF/IBCF no HN podem criptografar e descriptografar os endereços de todas as entidades da rede da operadora.

Outro recurso de segurança que poderíamos comentar seria o SIP *privacy* nas redes IMS.

[7] AKA é um protocolo de segurança usado nas redes 3G.

Privacidade pode em muitos casos, ser equivalente a confidencialidade, ou seja, ocultar informações (usando criptografia e chaves de criptografia) em todas as entidades, exceto aquelas que estejam autorizadas a compreender a informação.

As extensões de privacidade do SIP para redes IMS não fornecem essa confidencialidade. O objetivo do mecanismo seria apenas dar a um assinanente IMS a possibilidade de não revelar determinadas informações sobre a identidade do assinante.

Ademais, conforme especificado em [5], é recomendado que os mecanismos de privacidade para as redes IMS não criem mais estados no CSCFs além dos estados normais do SIP.

Quando uma rede IMS (a partir do release 6) está em operação com uma rede não-IMS, o CSCF na rede IMS fará a ligação de segurança com a outra rede.

A outra rede é confiável quando o mecanismo de segurança mencionado acima é aplicado, bem como a disponibilidade de um acordo *inter-working*.

Se a interoperabilidade de rede não-IMS não é confiável, as informações de privacidade são removidas do tráfego em direção a essa rede não-IMS.

Ao receber uma sinalização SIP, o CSCF verifica se alguma informação de privacidade está sendo mantida. Se o interfuncionamento da rede não-IMS não é confiável, a informação é removida pelo CSCF, caso contrário a informação é mantida pelo CSCF.

CSCFs separados são geralmente necessários para fazer a interface com redes IMS e não-IMS, porque a ausência de mecanismo de segurança durante a interconexão indica uma rede não-IMS não confiável.

A interface CSCF com as redes IMS implicitamente admite que todas as redes IMS estivessem acessíveis via SEG que estabelece os parâmetros de segurança.

4.2. Mecanismos de Segurança e Autenticação

A seguir descreveremos alguns dos mecanismos de segurança da Arquitetura IMS e o processo de autenticação do usuário na rede IMS.

O esquema para autenticação e acordo de chave no IMS é chamado IMS AKA. O IMS AKA realiza autenticação mútua entre o ISIM e o HN.

O IMPI que é a identidade privada, que é a identidade usada para autenticar um assinante, tem a forma de um NAI. O HSS e o ISIM compartilham uma chave permanente associada com o IMPI.

O HN usa o esquema de IMS AKA para autenticar um assinante IMS que realiza acesso através do UMTS, dessa forma os parametros de segurança, como as chaves geradas pelo esquema IMS AKA são transportadas via SIP.

A geração do vetor de autenticação AV que inclui RAND, XRES, CK, IK e AUTN é feita da mesma forma, conforme especificado em [4]. O ISIM e o HSS mantem os contadores SQN-ISIM e SQN-HSS, respectivamente.

Além disso, dois pares de associações de segurança são estabelecidos entre a UE e os P-CSCF. O assinante pode ter vários IMPUs associados com um IMPI. Esses podem pertencer a perfis de serviço iguais ou diferentes.

Somente dois pares de SAs (*Security Associations*) são ativos entre a UE e o P-CSCF. Esses dois pares de SAs são atualizados quando uma nova autenticação bem sucedida do assinante tenha ocorrido.

É política de o HN decidir se uma autenticação será realizada para registro de diferentes IMPUs, por exemplo IMPUs diferentes pertencentes a perfis de serviço iguais ou diferentes.

Antes que um usuário tenha acesso aos serviços, pelo menos um IMPU precisa ser registrado e o IMPI autenticado em nível de aplicação no IMS.

No intuito de ser registrado o UE envia uma mensagem SIP *REGISTER* para o servidor SIP *registrar*, ou seja, o S-CSCF, que irá executar a autenticação do usuário. Os fluxos de mensagens são o mesmo, independentemente se o usuário tem uma IMPU já registrada ou não.

Na Fig. 4.4 abaixo temos uma autenticação e troca de chaves no IMS para um assinante não registrado e autenticação mútua com sucesso sem erros de sincronização

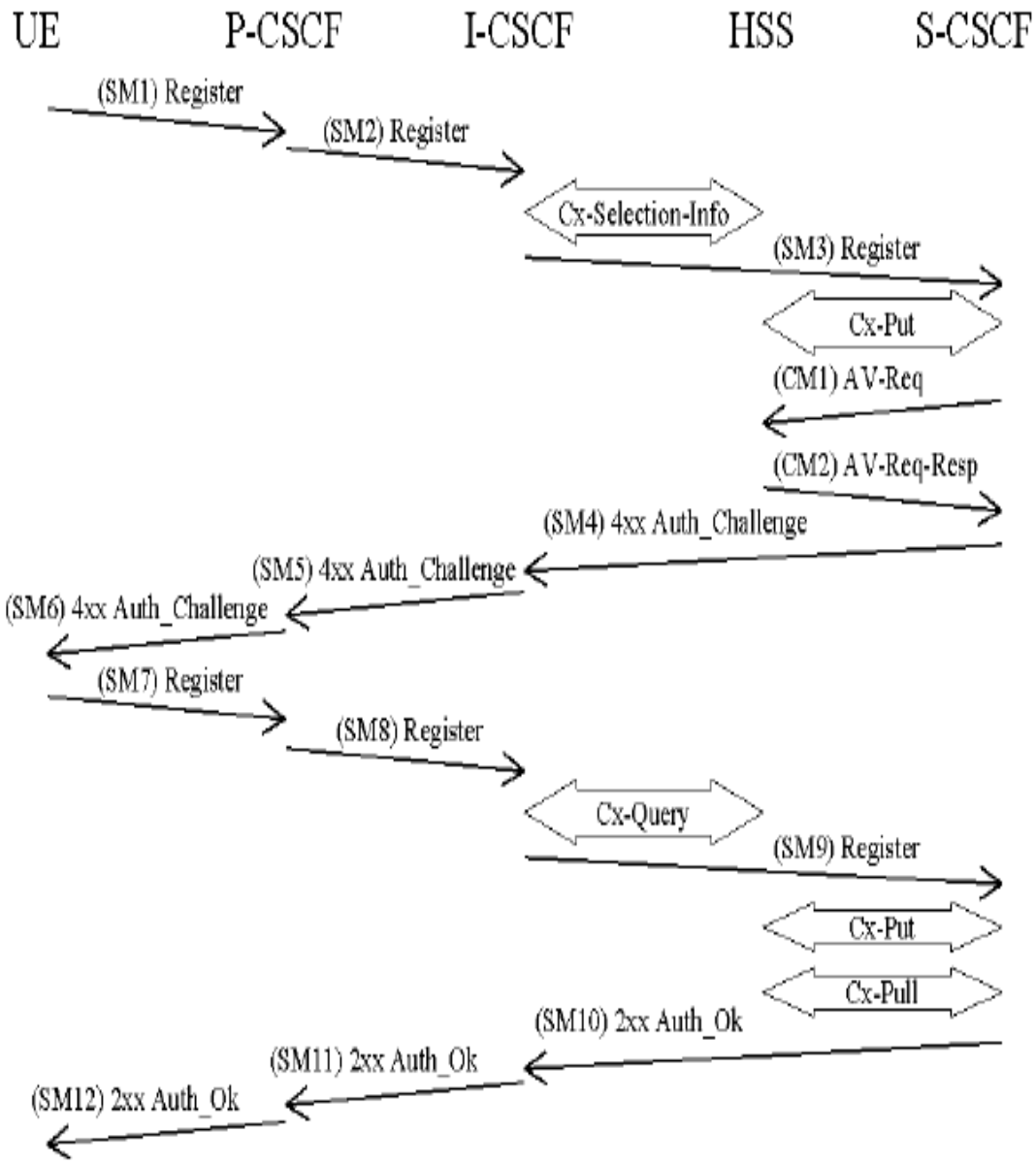

Fig. 4.4 - Autenticação e acordo de chaves no IMS [5].

SMn significa SIP Mensagem n e CMm significa Cx mensagem m que tem relação com o processo de autenticação:

SM1:

REGISTER (IMPI, IMPU).

Em SM2 e SM3 o P-CSCF e o I-CSCF, respectivamente, encaminham o SIP *REGISTER* para o S-CSCF.

Depois de receber SM3, se o IMPU não está registrado no S-CSCF, o S-CSCF precisa definir uma *flag* de registro no HSS para registro inicial pendente.

Isso é feito, a fim de tratar as chamadas terminadas no UE enquanto o registro inicial está em andamento e ainda não foi completado com sucesso.

A *flag* de registro é armazenada no HSS juntamente com o S-CSCF nome e identidade do usuário, e é usado para indicar se um determinado IMPU do usuário não está registrado ou está registrado em um determinado S-CSCF ou se o registro inicial de um determinado S-CSCF está pendente.

A *flag* de registro é definida pelo S-CSCF enviar um Cx-Put para o HSS.

Se o IMPU está registrado, o S-CSCF deixa a flag de registro definida com status registrado. Nessa fase, o HSS realiza uma verificação que o IMPI e o IMPU pertencem ao mesmo usuário.

Ao receber o SIP *REGISTER* o S-CSCF CSCF usa um vetor de autenticação (AV) para autenticação e para combinar uma chave de segurança com o usuário.

Se o S-CSCF não tem um AV válido logo o S-CSCF envia um pedido para o AV(s) para o HSS em CM1 juntamente com o número m de AVs solicitados onde m é pelo menos um.

CM1:
CX-AV-REQ (IMPI, M).

Após a recepção de um pedido do S-CSCF, o HSS envia um conjunto ordenado de vetores de autenticação n ao S-CSCF usando CM2. Os vetores de autenticação são ordenados com base no número de seqüência.

Cada vetor de autenticação consiste dos seguintes componentes: um número aleatório RAND, uma resposta esperada XRES, uma cifra de chave CK, uma chave de integridade IK e um *token* de autenticação AUTN.

É recomendado que a cada processo de autenticação e acordo de chaves entre o S-CSCF e o usuário IMS exista um vetor de autenticação.

CM2:
Cx-AV-Req-Resp (IMPI,
RAND1||AUTN1||XRES1||CK1||IK1,....,RANDn||AUTNn||XRESn||CKn||IKn)

Quando o S-CSCF precisa enviar um desafio de autenticação para o usuário, ele seleciona o próximo vetor de autenticação da matriz ordenada, ou seja, vetores de autenticação em um determinado S-CSCF são usados em uma base *first-in* / *first-out*.

O S-CSCF envia um SIP 4xx a*uth_challenge*, ou seja, um desafio de autenticação para a UE, incluindo o desafio RAND, o *token* de autenticação AUTN em SM4.

Também inclui a chave de integridade IK e a cifra de chave CK para o P-CSCF. O S-CSCF também armazena o RAND que foi enviado para o UE para uso em caso de falha de sincronização.

A verificação do SQN pelo USIM e ISIM fará o UE rejeitar uma tentativa do S-CSCF para voltar a usar um AV [5]. Isso não impede a utilização dos procedimentos normais de transmissão e retransmissão da camada de transação do SIP.

SM4:
4xx Auth_Challenge (IMPI, RAND, AUTN, IK, CK)

Quando o P-CSCF recebe SM5 ele armazena a chave (s) e remove a informação e transmiti o resto da mensagem para o UE:

SM6:
4xx Auth_Challenge (IMPI, RAND, AUTN)

Ao receber o desafio, SM6, o UE assume o AUTN, que inclui um MAC e o SQN. O UE calcula o XMAC e verifica se XMAC = MAC e que o SQN está na faixa correta. Se ambas as verificações são bem sucedidas o UE usa RES e alguns outros parâmetros para calcular a resposta de autenticação. Essa resposta é colocada no cabeçalho de Autorização e enviado de volta para o registrar em SM7. O UE nessa fase também calcula as chaves de sessão CK e IK.

SM7:
REGISTER (IMPI, Authentication response)

O P-CSCF encaminha a resposta de autenticação em SM8 para o I-CSCF, que consulta o HSS para encontrar o endereço do S-CSCF. Em SM9 o I-CSCF encaminha a resposta de autenticação para o S-CSCF.

Ao receber SM9 contendo a resposta, o S-CSCF recupera o XRES ativo para aquele usuário e usa isso para verificar a resposta de autenticação enviada pelo UE. Se a verificação for bem sucedida, dessa forma o usuário foi autenticado e o IMPU é registrado no S-CSCF.

Se o IMPU não foi registrado, o S-CSCF envia um Cx-Put para atualizar a *flag* de resgistro para registrado. Se o IMPU foi registrado a *flag* de registro não é alterada.

É possível registrar implicitamente IMPU(s), todos os IMPU (s) que estão sendo implicitamente registados são entregues pelo HSS ao S-CSCF e, posteriormente, para o P-CSCF. O S-CSCF considera todos os IMPU(s) registrados implicitamente como IMPU(s) registrados.

Quando um IMPU foi registrado esse registro será válido por um período de tempo. Tanto o UE quanto o S-CSCF acompanharam um *timer* para validar esse registro.

Mas o tempo de expiração no UE é menor do que no S-CSCF, a fim de tornar possível para a UE ser registado e acessível sem interrupções.

Um registro bem sucedido de um IMPU previamente cadastrados (incluindo IMPUs implicitamente registrados) significa que o tempo de validade do registro é atualizado.

Se o usuário foi autenticado com êxito, o S-CSCF envia uma mensagem SM10 SIP 2xx Auth_OK para o I-CSCF indicando que o registro foi bem sucedido. No SM11 e SM12 o I-CSCF e o P-CSCF, respectivamente, encaminharam o SIP 2xx Auth_OK para o UE.

Entretanto a partir do momento que o UE iniciou o procedimento para fazer um *re-registration* é aberta uma porta para um potencial ataque de negação de serviço.

Isso é, um invasor pode tentar registrar um IMPU já registrado e responder com uma resposta de autenticação incorreta, a fim de fazer o HN de-registrar o IMPU.

Por isso, o assinante quando registrado, não é de-registrado se falhar a autenticação.

A seguir descreveremos alguns cenários para falhas de autenticação, tais quais falha de autenticação do usuário, falha de autenticação da rede e autenticação incompleta.

Além disso, descreveremos cenário para falha na sincronização e autenticações iniciadas pela rede.

• Falha de autenticação do usuário

Nesse caso, a autenticação do usuário falha no S-CSCF, devido a uma resposta incorreta (recebido em SM9).

No entanto, se a resposta está incorreta, logo o IK usado para proteger SM7 normalmente estará incorreto também, que normalmente causa a verificação de integridade no P-CSCF para

falhar antes que a resposta possa ser verificada no S-CSCF. Nesse caso SM7 é descartado pela camada IPSec no P-CSCF.

Se a verificação de integridade passa, mas a resposta está incorreta, os fluxos de mensagem são idênticos até e incluindo SM9 como uma autenticação bem-sucedida.

Uma vez que o S-CSCF detecta a falha de autenticação do usuário ele procede da mesma forma como tendo recebido em SM9 uma falha de autenticação da rede.

• Falha de autenticação da rede

Nesse cenário quando a verificação do MAC na UE falha a rede não pode ser autenticado e, portanto, o registro falha, conforme Fig. 4.5. O fluxo é idêntico para o um registro bem sucedido até SM6.

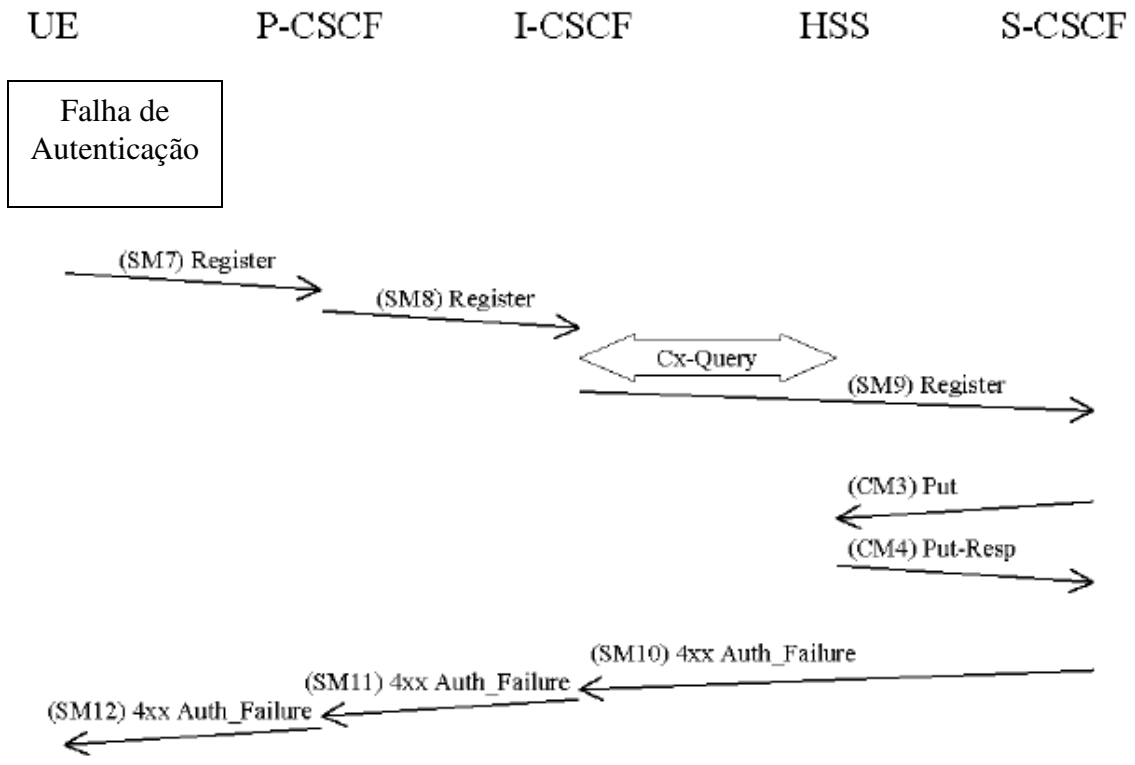

Fig. 4.5 - Falha de autenticação na rede [5].

O UE envia uma mensagem de registro para o HN incluindo uma indicação da causa da falha em SM7. O P-CSCF e o I-CSCF encaminham essa mensagem para o S-CSCF.

SM7:
REGISTER (*Failure* = *AuthenticationFailure*, IMPI)

Ao receber SM9, que inclui a causa da falha de autenticação, o S-CSCF limpa o nome S-CSCF no HSS, se o IMPU no momento não está registado. Para limpar o nome S-CSCF o S-CSCF envia em CM3 um Cx-Put para o HSS. O S-CSCF não atualiza a *flag* de registro.

CM3:
Cx-AV-Put (IMPI, *Clear* S-CSCF *name*)

O HSS responde para CM3 com um Cx-Put-Resp em CM4.

Em SM10 o S-CSCF envia um 4xx *Auth_Failure* para o UE indicando que a autenticação falhou, nessa mensagem não são incluídos parâmetros de segurança.

SM10:
SIP/2.0 4xx *Auth_Failure*

• Autenticação incompleta

Quando o S-CSCF recebe uma nova requisição de *REGISTER* e inicia o processo de autenticação, ele considera que qualquer autenticação anterior tenha falhado.

Dessa forma ele apaga qualquer informação relacionada com a autenticação anterior, embora o S-CSCF possa enviar uma resposta se o desafio anterior for questionado.

Se o S-CSCF não receber uma resposta a um desafio de autenticação dentro de um tempo aceitável, considera-se que a autenticação tenha falhado. A atualização para o HSS é realizada da mesma forma como se estivesse recebendo um SM9 indicando falha de autenticação.

• Falha na sincronização

Depois da re-sincronização, a autenticação pode ser concluída com êxito, mas também pode acontecer que em tentativas subseqüentes outras condições de falha ocorram (falha de autenticação do usuário, falha de autenticação de rede).

Na Fig. 4.6 abaixo é apresentado apenas o caso de falha de sincronização com autenticação bem-sucedida subseqüente. Os outros casos podem ser obtidos pela combinação com os fluxos para as outras condições de falhas.

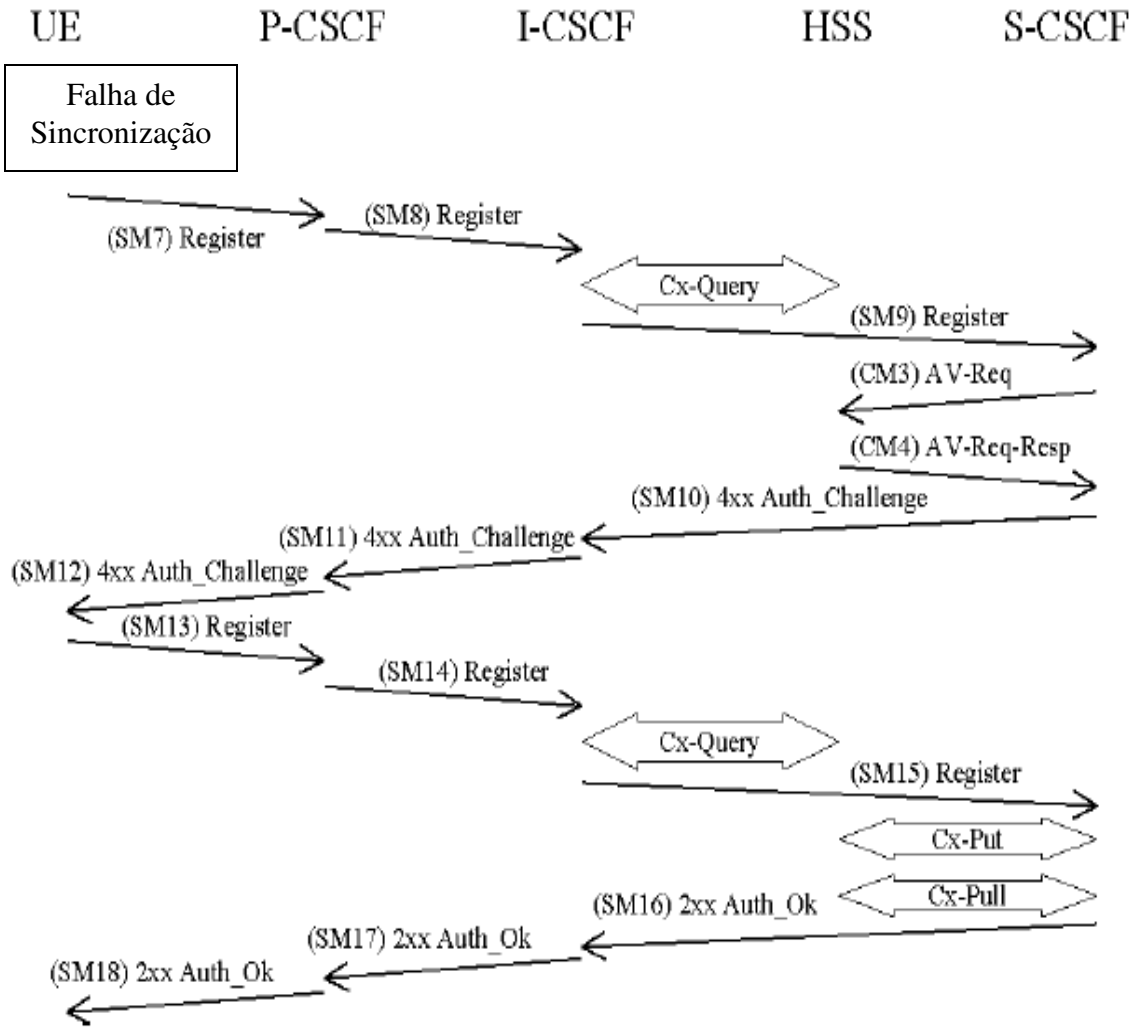

Fig. 4.6 - Falha na sincronização [5].

Quando o UE recebe SM6 ele detecta que a SQN está fora do intervalo e envia uma falha na sincronização de volta para o S-CSCF em SM7.

SM7:

REGISTER (*Failure = Synchronization Failure*, AUTS, IMPI)

Ao receber a falha de sincronização e o AUTS o S-CSCF envia um Av-Req para o HSS em CM3 incluindo o RAND armazenado pelo S-CSCF e o número solicitado de Avs, m.

CM3:
Cx-AV-Req (IMPI, RAND, AUTS, m)

Depois de atualizar o SQN, o HSS envia novo AVs para o S-CSCF em CM4.

CM4:
Cx-AV-Req-Resp(IMPI,
n,RAND1||AUTN1||XRES1||CK1||IK1,....,RANDn||AUTNn||XRESn||CKn||IKn)

Quando o S-CSCF recebe o novo lote de vetores de autenticação do HSS ele exclui os antigos para esse usuário no S-CSCF.

• Autenticações iniciadas pela rede

Para autenticar um usuário já cadastrado, o S-CSCF envia uma solicitação para o UE para iniciar um procedimento de *re-registration*. Quando o procedimento é recebido no S-CSCF, o *re-registration* dispara um novo procedimento IMS AKA que permitirá o S-CSCF re-autenticar o usuário.

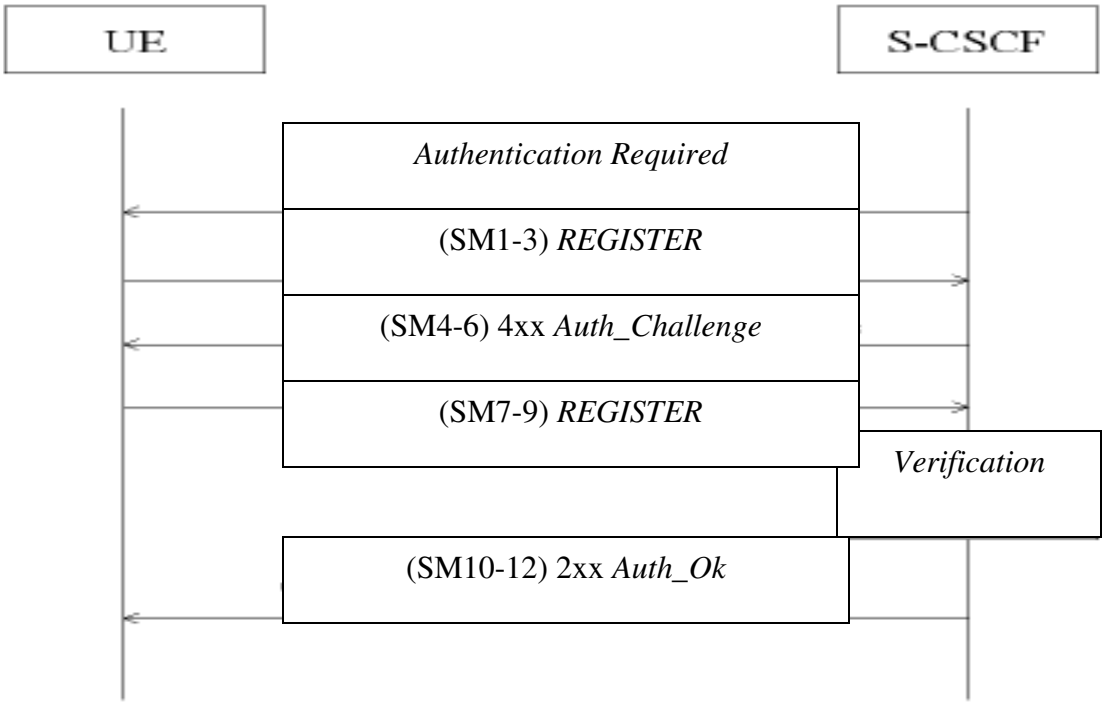

Fig. 4.7 - Autenticação iniciada pela rede [5].

O UE dará início ao *re-registration* emitindo um a*uthentication required*. No caso em que o UE não inicia o procedimento de *re-registration* após o pedido do S-CSCF, o S-CSCF pode decidir por de-registrar o assinante ou re-emitir um a*uthentication required*.

Com relação ao indicador de proteção de integridade, com o intuito de decidir se um pedido de *REGISTER* do UE precisa ser autenticado, o S-CSCF precisa saber sobre a proteção da integridade aplicada à mensagem.

O P-CSCF atribui uma indicação ao pedido de *REGISTER* para informar ao S-CSCF que a mensagem tem a integridade protegida, se [5]:

- O P-CSCF recebe um *REGISTER* contendo uma resposta de autenticação e a mensagem é protegida com um SA criado durante esse procedimento de autenticação,
- O P-CSCF recebe um *REGISTER* que não contem uma resposta de autenticação e a mensagem é protegida com um SA criado pela última autenticação bem-sucedida (na perspectiva do P-CSCF).

Para todos os outros pedidos de *REGISTER* o P-CSCF atribui uma indicação de que o pedido *REGISTER* não teve a integridade protegida.

4.3. Procedimento de Configuração da Associação de Segurança

O procedimento de configuração da associação de segurança é necessário a fim de decidir quais os serviços de segurança serão aplicados e quando os serviços de segurança serão iniciados. Na autenticação IMS de usuários é realizado durante o processo de *registration*.

Subsequentes comunicações de sinalização nessa sessão terão proteção de integridade baseado em chaves derivadas durante o processo de autenticação.

Para proteger a sinalização IMS entre a UE e o P-CSCF é necessário ter uma concordância com chaves compartilhadas (*shared keys*) que são fornecidos pelo IMS AKA, e um conjunto de parâmetros específicos para um método de proteção.

A configuração do modo de segurança é usada para negociar os parâmetros SA (*Security Association*) necessários para IPSec ESP com autenticação e confidencialidade.

Os parâmetros SA que são negociados entre o UE e o P-CSCF no procedimento de configuração do modo de segurança são os algoritmos de criptografia que é DES-EDE3-CBC ou AES-CBC com chave de 128 *bits*, os Algoritmos de Integridade que é HMAC-MD5-96 ou HMAC-SHA-1-96 e o SPI (*Security Parameter Index*) que é alocado localmente para ligação SAs.

O trio (SPI, endereço IP de destino, protocolo de segurança) identifica exclusivamente uma SA na camada IP. O UE seleciona um único SPIs que podem ser usados em qualquer SAs existente. Os SPIs selecionados pelo P-CSCF será diferente do SPIs enviado pelo UE.

No procedimento de autenticação do registro, o UE e o P-CSCF escolhem dois SPIs, ainda não associados com uma ligação SAs, para uma nova associação de segurança.

Alguns parâmetros de associação de segurança não são negociados, como tipo de vida (*life type*) que é sempre em segundos, a duração do SA que tem tamanho fixo de 232-1, o modo de transporte e o *key length* (tamanho de chave).

Na Fig. 4.8 abaixo temos um caso normal de configuração de uma associação de segurança sem falhas.

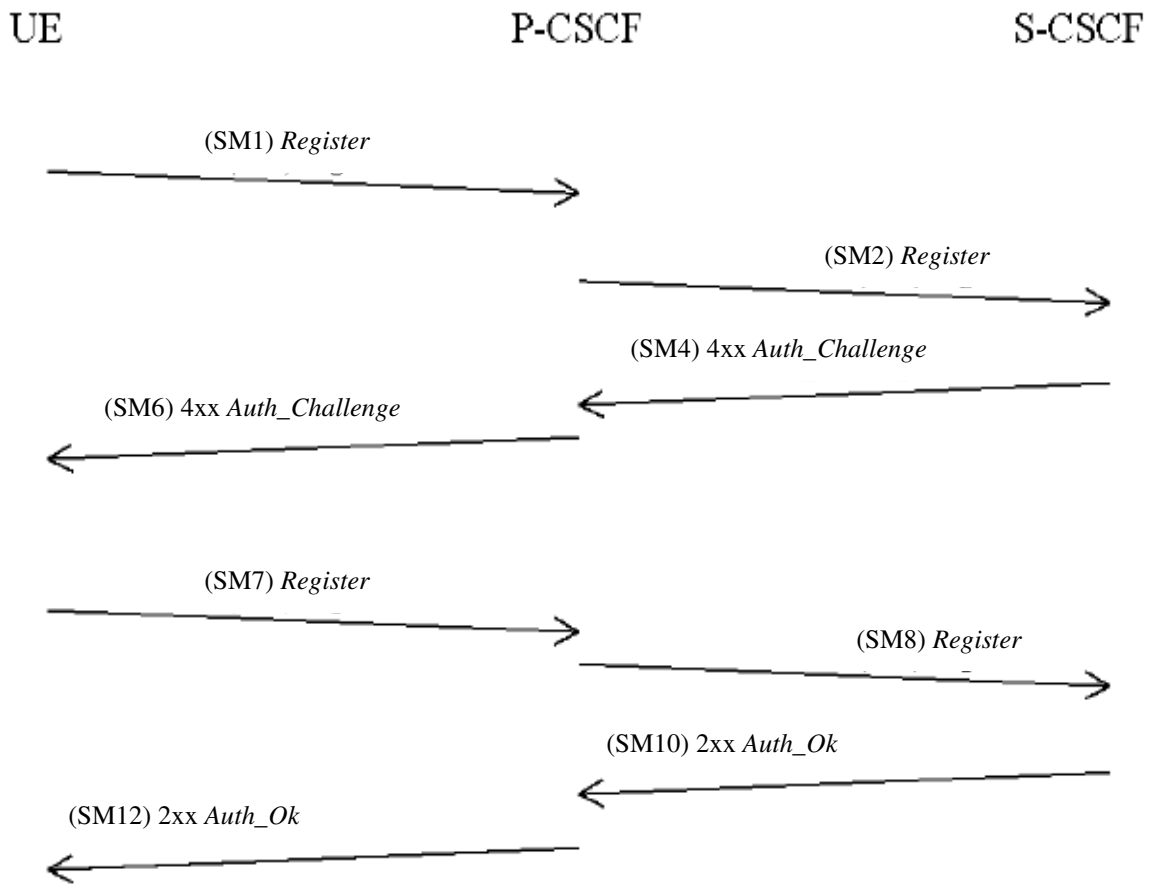

Fig. 4.8 - Configuração de uma associação de segurança sem falhas [5].

O UE envia uma mensagem de registro para o S-CSCF para registrar a localização do UE e para configurar o modo de segurança.

Para iniciar o procedimento de configuração do modo de segurança, o UE inclui uma *security-setup-line* (configuração de linha de segurança) nessa mensagem.

A configuração de linha de segurança em SM1 contém os valores dos índices dos parâmetros de segurança e as portas protegidas selecionadas pelo UE.

Ele também contém uma lista de identificadores para os algoritmos de integridade e de criptografia, que o UE suporta.

SM1:

REGISTER (*Security-setup* = SPI_U, Port_U, UE lista de algoritmos de integridade e criptografia)

SPI_U é o nome simbólico de um par de valores SPI (spi_uc, spi_us) que o UE seleciona. O spi_uc é o SPI da entrada da SA na porta cliente protegida do UE, e spi_us é o SPI da entrada da SA na porta do servidor protegido do UE.

Port_U é o nome simbólico de um par de números de porta (port_uc, port_us). Após a recepção do SM1, o P-CSCF armazena temporariamente os parâmetros recebidos na configuração de linha de segurança juntamente com o cabeçalho do pacote IP do endereço IP de origem do endereço IP do UE, o IMPI e IMPU.

Após a recepção do SM4, o P-CSCF adiciona as chaves IK-IM e CK-IM recebidos do S-CSCF com os parâmetros temporariamente armazenados.

O P-CSCF, em seguida, seleciona o SPIs para as SAs de entrada. O P-CSCF definiu o SPIs tal que eles sejam únicos e diferentes de qualquer SPIs como os recebidos pela configuração de linha de segurança do UE.

A fim de determinar o algoritmo de integridade e criptografia o P-CSCF prossegue da seguinte forma: o P-CSCF tem uma lista de algoritmos de integridade e criptografia que ele suporta ordenados por prioridade.

O P-CSCF seleciona a primeira combinação de algoritmo dessa lista, que também é suportado pelo UE.

Se o UE não incluiu nenhum algoritmo de confidencialidade em SM1 logo o P-CSCF seleciona o algoritmo de criptografia NULL ou aborta o procedimento, de acordo com sua política de confidencialidade.

O P-CSCF dessa forma estabelece dois novos pares de SAs no banco de dados local de associação de segurança.

A configuração de linha de segurança em SM6 contém os SPIs e as portas atribuídas pelo P-CSCF. Ele também contém uma lista de identificadores para os algoritmos de integridade e criptografia, que o P-CSCF suporta.

A única exceção a isso é o caso em que o P-CSCF está configurado para nunca aplicar o mecanismo de confidencialidade. Nesse caso, não são incluidos algoritmos de criptografia para a configuração de linha de segurança em SM6.

SM6:

4xx *Auth_Challenge*(*Security-setup* = SPI_P, Port_P, P-CSCF lista de algoritmos de integridade e criptografia)

SPI_P é o nome simbólico do par de valores SPI (spi_pc, spi_ps) que o P-CSCF seleciona. O spi_pc é o SPI da entrada da SA na porta cliente protegida do P-CSCF, e spi_ps é o SPI da entrada da SA na porta servidora protegida do P-CSCF. Port_P é o nome simbólico dos números de porta (port_pc, port_ps).

Após a recepção do SM6, o UE determina os algoritmos de integridade e criptografia da seguinte forma: o UE seleciona a primeira combinação de algoritmo de integridade e criptografia na lista recebida do P-CSCF em SM6, que também é suportada pelo UE. Se o P-CSCF não inclue qualquer algoritmo de confidencialidade em SM6.

Assim, o UE seleciona o algoritmo de criptografia NULL. O UE, em seguida, passa a estabelecer dois novos pares de SAs no SAD local.

O UE protege a integridade e confidencialidade em SM7 e todas as mensagens SIP seguintes. Além disso, a lista de algoritmos de integridade e criptografia, SPI_P e Port_P recebido em SM6, e SPI_U, Port_U enviado em SM1 são incluídos:

SM7:
REGISTER (*Security-setup* = SPI_U, Port_U, SPI_P, Port_P, P-CSCF lista de algoritmos de integridade e criptografia)

Depois de receber SM7 do UE, o P-CSCF verifica se a lista de algoritmos de integridade e criptografia, SPI_P e Port_P recebido em SM7 é idêntica aos correspondentes parâmetros enviados em SM6.

Além disso, verifica se SPI_U e Port_U recebido em SM7 são idênticos aos recebidos em SM1. Se essas verificações não são bem sucedidos o procedimento de registro é abortado.

O P-CSCF inclui em SM8 informações para o S-CSCF que a mensagem recebida do UE teve a integridade protegida.

O P-CSCF adiciona essas informações para todas as mensagens *REGISTER* subseqüentes recebidas do UE que passaram com sucesso no processo de verificação de integridade no P-CSCF.

SM8:
REGISTER (*Integrity-Protection* = *Successful*, IMPI)

O P-CSCF finalmente envia SM12 para o UE. SM12 não contêm informações específicas para configuração do modo de segurança (isso é a configuração de linha de segurança).

Mas com o envio de SM12 não indicando erro o P-CSCF confirma que a configuração do modo de segurança foi bem sucedida.

Depois de receber SM12 não indicando erro, o UE pode assumir que a configuração do mode de segurança foi bem-sucedida.

Um exemplo de como fazer uso de dois pares de SAs unidirecional é ilustrado na Fig. 4.9 abaixo com um exemplo de um conjunto de troca de mensagens protegidas pelos respectivos IPSec SAs onde as mensagens *INVITE* e as mensagens seguintes assume-se que transitaram via TCP.

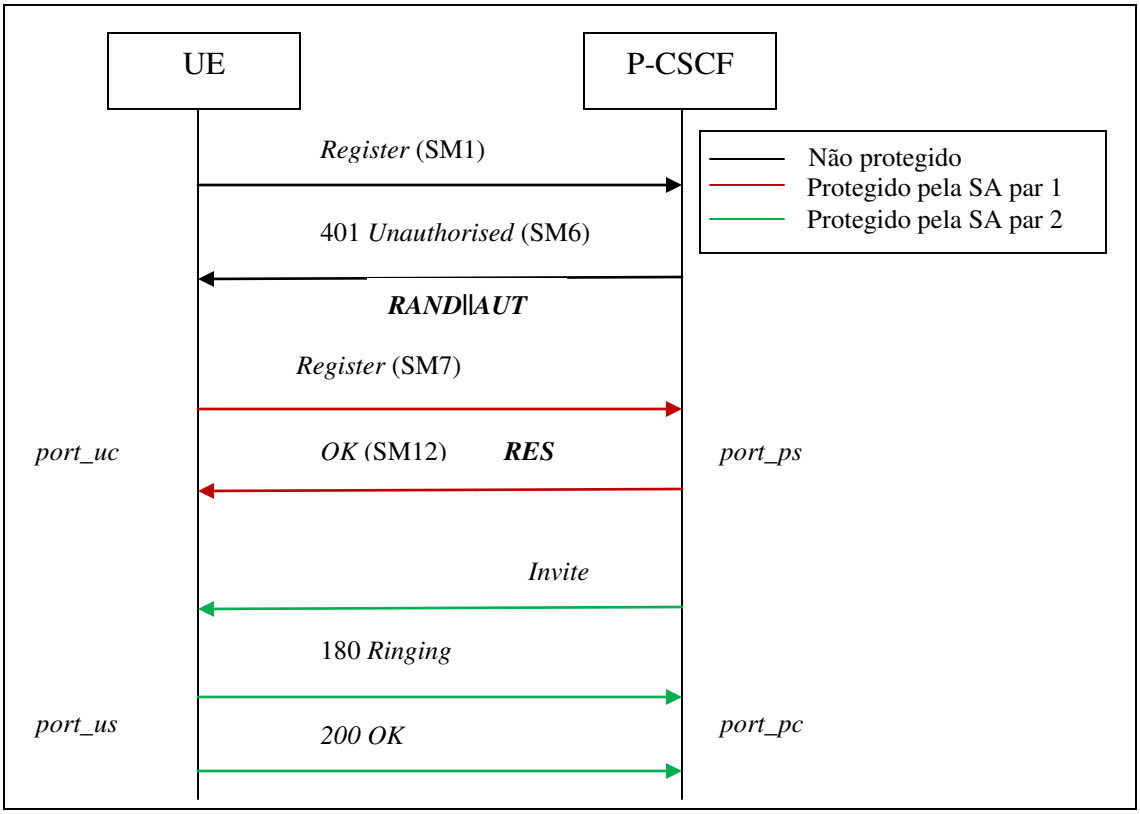

Fig. 4.9 - Troca de mensagens protegidas pelos respectivos IPSec [5].

Na medida em que a configuração das associações de segurança já foi descrita, descreveremos agora alguns casos de erros que podem acontecer na configuração das associações de segurança e como esses erros são tratados.

Basicamente existem dois tipos de casos de erros o primeiro relacionado com o IMS AKA e o segundo relacionado com a configuração da segurança.

Nos casos de erro relacionados com IMS AKA, podemos destacar:

• Falha de autenticação do usuário

Nesse caso, SM7 falha a verificação de integridade através do IPsec no P-CSCF se o IK-IM derivado de RAND no UE está errado. A aplicação SIP no P-CSCF nunca recebe SM7.

Os parâmetros de SA associados, temporariamente armazenados são apagados com esse registro depois de transcorrido o tempo limite.

No caso em que IK-IM foi derivado corretamente, mas a resposta de autenticação do usuário estava errada ocorrerá falha no S-CSCF, devido à resposta incorreta.

O S-CSCF envia uma mensagem 4xx *Auth_Failure* para o UE, através do P-CSCF, que pode passar através de uma SA já estabelecida. Posteriormente, ambos, o UE e o P-CSCF apagam as novas SAs.

• Falha de autenticação da rede

Se o UE não é capaz de se autenticar com êxito à rede, o UE envia uma mensagem *REGISTER*, que pode passar através de uma SA já estabelecida, indicando uma falha de autenticação de rede, para o P-CSCF. O P-CSCF exclui a novas SAs após receber essa mensagem.

• Falha de sincronização

Nessa situação, o UE observa que o AUTN enviado pela rede em SM6 contém uma seqüência de números *out-of-range*.

O UE envia uma mensagem REGISTER para o P-CSCF, que pode passar por uma SA já estabelecida, indicando falha de sincronização. O P-CSCF exclui as novas SAs após receber essa mensagem.

• Autenticação incompleta

Se o UE responde a um desafio de autenticação de um S-CSCF, mas não recebe uma resposta antes do tempo determinado, o UE inicia um procedimento de registro se ainda necessita de algum serviço IMS.

A primeira mensagem nesse registro é protegida com uma SA criada por uma autenticação anterior bem sucedida se houver.

Quando o P-CSCF recebe um desafio do S-CSCF e cria SAs correspondente durante o procedimento de registro, ele exclui qualquer informação relativa a qualquer processo de registro anterior (incluindo SAs criadas durante o processo de registro anterior).

Se o P-CSCF exclui um registro de SA, devido ao tempo de vida do registro ter expirado, o P-CSCF exclui qualquer informação relativa ao procedimento de registro que criou a SA.

Nos casos de erro relacionados com configuração de segurança, podemos destacar:

• Proposta inaceitável para o P-CSCF

Nesse caso, o P-CSCF não pode aceitar o conjunto de proposta enviada pelo UE no comando de configuração de segurança do SM1. O P-CSCF responde para o SM1 indicando uma falha, enviando uma resposta de erro para o UE.

• Proposta inaceitável para o UE

Se o P-CSCF envia na linha de configuração de segurança de SM6 uma proposta que não é aceitável para a UE, o UE abandona o procedimento de registro.

• Falha na verificação de consistência das linhas de configuração de segurança no P-CSCF

O P-CSCF verifica se a lista de algoritmos de autenticação e criptografia recebida em SM7 é idêntica à lista de algoritmos de autenticação e criptografia enviada em SM6. Se ambas não são idênticas o procedimento de registro é abortado.

CAPÍTULO 5

FALHAS DE SEGURANÇA DA ARQUITETURA IMS

A segurança continua sendo a maior prioridade para provedores de serviço na medida em que as ameaças continuam a evoluir, com os provedores de serviço lutando para se defender contra o crescente volume e a sofisticação de spam, spyware e códigos maliciosos.

Bem como uma nova geração de *hackers* e de crimes organizados agora motivados pelo potencial lucro de roubar informações pessoais confidenciais, dados corporativos, serviços e a interrupção de serviços.

Um número crescente de programas mal-intencionados está explorando falhas de segurança nos navegadores da i*nternet*, páginas *web* e aplicações.

Além disso, como as empresas estão ser tornando mais dependentes dos benefícios de negócios envolvendo dispositivos móveis, aplicações *web* e novos serviços como VoIP.

O uso de tecnologias de segurança e uma infraestrutura segura com políticas de segurança atualizadas torna-se mais importante para proteção contra novos riscos.

A necessidade de proporcionar acesso aberto a parceiros, clientes e fornecedores, e acessar um ambiente de segurança de empresas terceiras, define como um ambiente de comunicação segura está se tornando um fator crítico para o sucesso das organizações.

Esses desafios de segurança são intensificados para os provedores de serviços, que devem proteger seus assinantes e introduzir novos serviços e aplicações rentáveis enquanto mitigam os ataques, abusos ou a adição de tráfego que consome recursos e esgotam os recursos da rede.

Atualmente as operadoras procuram novas maneiras de se diferenciar e filtrar ataques e atividades maliciosas para os clientes de forma segura simultaneamente com o lançamento de novos serviços e a alavancagem de assinantes para as suas redes.

Com o crescimento de serviços IP, prestadores de serviços terão de enfrentar a decisão crítica de como manter níveis adequados de segurança, disponibilidade e qualidade, mantendo os seus custos e os riscos sob controle.

É importante para os provedores de serviços reconhecerem que significativa redução de custos será alcançada a partir de prevenção, detecção e mitigação de ataques antes que suas redes ou clientes sejam prejudicados.

Ademais é necessário encurtar os ciclos de implementação de novas medidas de segurança, enquanto aceleram-se novos serviços geradores de receita totalmente suportados pela rede.

Dessa forma, a questão de segurança na arquitetura IMS assume extrema importância e chama a atenção de pesquisadores, operadoras e empresas de manufatura ao redor do mundo.

Uma vez que uma arquitetura sem requisitos completos e confiáveis de segurança tende a não ter seu desenvolvimento continuado e muito menos ser adotada como solução.

O grupo 3GPP responsável pelas análises de segurança na arquitetura IMS é o TSG SA WG3, esse grupo é responsáveis por analisar potenciais novas ameaças que podem ser introduzidas nos serviços baseados em IP e por definir os requisitos de segurança para todos os sistemas 3GPP.

O objetivo do grupo seria desenvolver e implementar pelo menos o mesmo nível de segurança existente na rede 2G (GSM) além de promover melhorias.

No geral podemos observar que a arquitetura IMS apresenta inúmeros pontos de vulnerabilidade no seu mecanismo de segurança, pontos esses que são comuns em redes VoIP e IP.

Aliás, esse é o principal fator impeditivo da adoção e do desenvolvimento dessa arquitetura em escala global.

A arquitetura IMS é muito mais suscetível a ataques e interferência do que os antigos negócios com linhas fixas de companhias telefônicas.

Ao adotar o IP para a distribuição de todos os serviços, o IMS se abre a todas as mesmas vulnerabilidades de segurança enfrentadas por qualquer aplicativo da *internet* desde ataques de *denial of services* a ataques na camada de aplicação.

Da mesma forma que muitos dos primeiros aplicativos SOA permitem que os usuários criem combinações de serviços personalizados, a arquitetura IMS tem o mesmo potencial. Isso significa que os serviços distribuídos por um provedor de serviço podem ou não residir na rede dele.

Isso deixa o provedor de serviço vulnerável a vários problemas de segurança, como gerenciar problemas de autenticação e faturamento quando um usuário acessa um serviço externo ou mantiver informações sigilosas protegidas de outros usuários na rede.

Por outro lado podemos observar que algumas empresas têm implementado soluções próprias para o IMS no intuito de excluir algumas falhas de segurança da arquitetura.

Como é o caso da Verizon Wirelles que desenvolveu o A-IMS implementando alguns requisitos de segurança específicos.

O fato de a arquitetura ser aberta e distribuída facilita e flexibiliza a implementação e desenvolvimento de soluções próprias por parte das operadoras.

O mecanismo de segurança da arquitetura IMS também é limitado pelos componentes IMS da arquitetura 3G [4], ou seja, está relacionado na maneira pela qual a sinalização SIP é protegida

entre o assinante e o IMS, como o assinante é autenticado e como o assinante autentica no IMS, não especificando mecanismos de autorização de acesso.

Outro ponto importante a ser considerado nas especificações de segurança do IMS é o fato que já existem no mercado inúmeros desenvolvimentos do IMS onde nem todos os requisitos básicos de segurança foram considerados [6].

Como por exemplo, o IMS foi especificado para ser desenvolvido em IPv6, porém existem muitos casos onde a arquitetura está sendo desenvolvida em cima da infraestrutura IPv4.

Outro ponto seria que alguns dispositivos, como é o caso do celular não tem capacidade de processamento para suportar o IPSec.

Como já mencionado no Capítulo 4, a arquitetura de segurança do IMS provê diversos mecanismos e recursos de segurança como os algoritmos de criptografia e autenticação.

Entretanto ainda existem diversos pontos de vulnerabilidade na arquitetura que podem abrir falhas como, por exemplo, o consumo de recursos da rede, diminuição de desempenho da CPU [32], ocasionando assim que usuários legítimos deixem de receber serviços com uma qualidade de desempenho aceitável.

Conclui-se dessa forma, que a arquitetura de segurança proposta pelo 3GPP não é suficiente para oferecer uma proteção segura para o IMS, principalmente para proteger as redes IMS de ataques de inundação [33].

Com a padronização das redes IMS para o IPv6 muitos dos problemas de segurança da arquitetura devem ser resolvidos.

Contudo ameaças como negação de serviço (DoS), ataques de negação de serviço distrubuídos e principalmente SPIT (*Spam-over-Internet Telephony*) tendem a continuar prejudicando a arquitetura.

5.1. Principais Tipos de Ataques

Abaixo listamos os principais tipos de ataques que podem atingir as redes IMS com intuito de derrubar os serviços ou atacar os usuários da rede para obter algum acesso a recursos e informações não autorizadas:

• *Protocol fuzzing*

Protocolo de aplicação *fuzzing* é o processo de enviar dados contendo erros injetados para dispositivos da rede, o objeto desse procedimento é que o envio de dados inválidos acaba expondo partes da aplicação que geralmente não são estressadas.

Protocol fuzzing geralmente faz parte de rotinas de verificação e validação e são usados para aprimorar e avaliar a segurança de sistemas e dispositivos da rede.

Dessa forma, usuários maliciosos poderiam usar *protocol fuzzing* para atacar uma rede IMS fornecendo dados maliciosos, ou então fornecendo uma quantidade muito grande de dados no intuito de danificar a rede.

Tais usuários podem enviar mensagens cujo contexto, aparentemente seja válido e íntegro, de forma que o sistema alvo assuma que a mensagem seja realmente válida.

Contudo, a mensagem estaria "quebrada" de forma que quando o sistema alvo tentar processá-la resultaria em várias falhas, que podem incluir desde atrasos nas aplicações, perda de informação como até falhas gerais no sistema.

Mensagens *fuzzed* podem facilmente ser transmitidas usando tráfego autenticado e criptografado, atingindo o núcleo da rede IMS.

Os dispositivos de segurança existentes geralmente não conseguem descriptografar o tráfico em redes de alta velocidade, e olhar os detalhes do protocolo (*header*, *body*, *content*) para certificar-se de que não há nenhuma intenção maliciosa, e conseqüentemente não pode se proteger contra um dos mais prejudiciais ataques relativos a infra-estrutura.

• SPIT e VoIP *spam*

VoIP *spam* ou SPIT (*Spam-over-Internet Telephony*) são mensagens em massa não solicitadas transmitidas através da rede IMS.

Essas mensagens além de ser irritantes e ter o potencial de usurpar a disponibilidade e a produtividade dos recursos do sistema, são também muito difíceis de serem rastreadas, uma vez que o volume alto de chamadas em massa roteadas através de IP é dificilmente rastreado.

Além de ter a capacidade inerente para fraude, uso de recursos não autorizados e violações de privacidade, os alvos desse tipo de ataque são os assinantes dos serviços IMS.

• Fraude

A partir do momento que *hackers* (*hacker* é uma pessoa que burla intencionalmente a segurança de computadores, em geral para causar interrupções ou obter acesso a informações confidenciais como detalhes financeiros) obtêm acesso a redes e servidores IMS eles podem cometer fraude de tarifação na medida em que atuem como um *gateway* entre o PSTN local e a rede IMS.

Além do que um usuário que cometa fraude pode acessar completamente a rede e os servidores IMS cortando roteadores, *firewalls* e sistemas operacionais, que podem expor detalhes importantes dos registros de chamadas dos usuários.

No intuito de proteção contra fraude, o comportamento de todos os assinantes deve ser monitorado em tempo real, bloqueando/banindo assinantes que cometam atividades suspeitas.

• Ameaça nos dispositivos

Outro tipo potencial de ataque seria advindo justamente da própria evolução tecnológica que os dispositivos móveis vêem sofrendo ao longo dos anos.

Hoje os chamados *smartphones*, com novas capacidades de acesso, que incluem desde USB, *bluetooth* e aplicativos que são "baixados da rede", ou seja os próprios dispositivos podem não intencionalmente figurar como uma grande ameaça para as redes IMS.

Por exemplo, *hackers* podem criar aplicativos que podem ser baixados por usuários, que instalado em seu *smartphone* pode ser uma porta aberta para a proliferação de ataques dentro de redes IMS.

• *Distributed floods* e *flood* DoS

Flood DoS (inundação de negação de serviço) e ataques DDoS são aqueles ataques por meio de um usuário malicioso que envia uma quantidade extremamente grande de mensagens aleatórias para um ou mais elementos da rede IMS de uma única posição (DoS) ou de múltiplas posições (DDoS).

Obviamente o problema é que o número de mensagens que chegam seria muito além da capacidade de processamento do sistema, dessa forma esse tipo de ataque esgotaria rapidamente os recursos do sistema que passaria a negar recursos e serviços para os usuários legítimos.

Um ponto importante que deve ser salientado é que além das ameaças que a arquitetura IMS está sujeita alia-se o fato que construir uma ferramenta para ataque a essa arquitetura, assim como as demais redes IP, é algo fácil que requer pouco tempo e investimento.

Haja vista que toda a estrutura da arquitetura, como *software open-source*, requisitos e especificações está publicamente disponível no site da 3GPP.

Dessa forma, qualquer *hacker* pode facilmente escrever um conjunto de scripts que leia informações do SIM *card*, por exemplo, podendo com essas informações desencadear vários outros tipos de ataques.

5.1.1. *Flooding* Ataques no SIP

Além dos ataques já mencionados não podemos deixar de mencionar os ataques de inundação (*flooding attacks*) que podem acontecer no protocolo SIP, que é o principal protocolo de comunicação do IMS, dentre os quais podemos mencionar:

• SQL *injection*

O objetivo deste tipo de ataque não é somente causar a modificação dos dados, mas também provocar negação de serviço pela queda dos serviços do banco de dados.

SQL *injection* geralmente é lançado inserindo instruções SQL quando o UE e o P-CSCF iniciam o procedimento de autenticação.

Quando o P-CSCF requisita autenticação o UE calcula as credenciais com base no mecanismo HTTP *Digest*, essa mensagem é enviada para o S-CSCF via P-CSCF na autorização, conforme o exemplo abaixo:

REGISTER sip: *home.mobile.com* SIP/2.0
Authorization: Digest
Username=”teste01@*mobile*.com”,
Realm=”er@*mobile*.com”,
nounce =””,
uri="sip:*home.mobile*.com",
qop=auth-int,
nc=000000001
cnounce=””,

reponse="",
opaque=""

O usuário malicioso poderia lançar um SQL *injection* no IMS via inserção de código SQL malicioso no cabeçalho de autorização. Essa mensagem poderia ser qualquer mensagem SIP solicitando autenticação para o P-CSCF.

O código pode ser incorporado no nome do usuário ou em qualquer campo no cabeçalho de autorização, conforme o exemplo abaixo:

REGISTER sip: *home.mobile*.com SIP/2.0
Authorization: Digest
Username="teste01@*mobile*.com; *delete table subscriber*",
Realm="er@*mobile*.com",
nounce ="",
Uri="sip: *home.mobile*.com",
qop=auth-int,
nc=000000001
cnounce="",
reponse="",
opaque=""

Quando a P-CSCF recebe uma mensagem SIP com um cabeçalho de autorização infectado, ele gera e executa a instrução SQL ilegítima que pode apagar ou alterar dados no banco de dados.

• IP *spoofing*

Um atacante personifica um usuário legítimo com identificação falsa e envia uma mensagem *INVITE* ou *REGISTER*.

Quando uma mensagem *INVITE* é enviado para um usuário com um endereço IP arbitrário, a chamada nunca é enviada através do terminal do *hacker*.

Desta forma, ele pode executar a fraude de tarifação e fazer chamadas gratuitas.

• *INVITE flooding*

Um atacante envia mensagens *INVITE* com endereço falso e paraleliza o terminal do usuário ou o servidor SIP *proxy*, conforme mostrado na Fig. 5.1 abaixo:

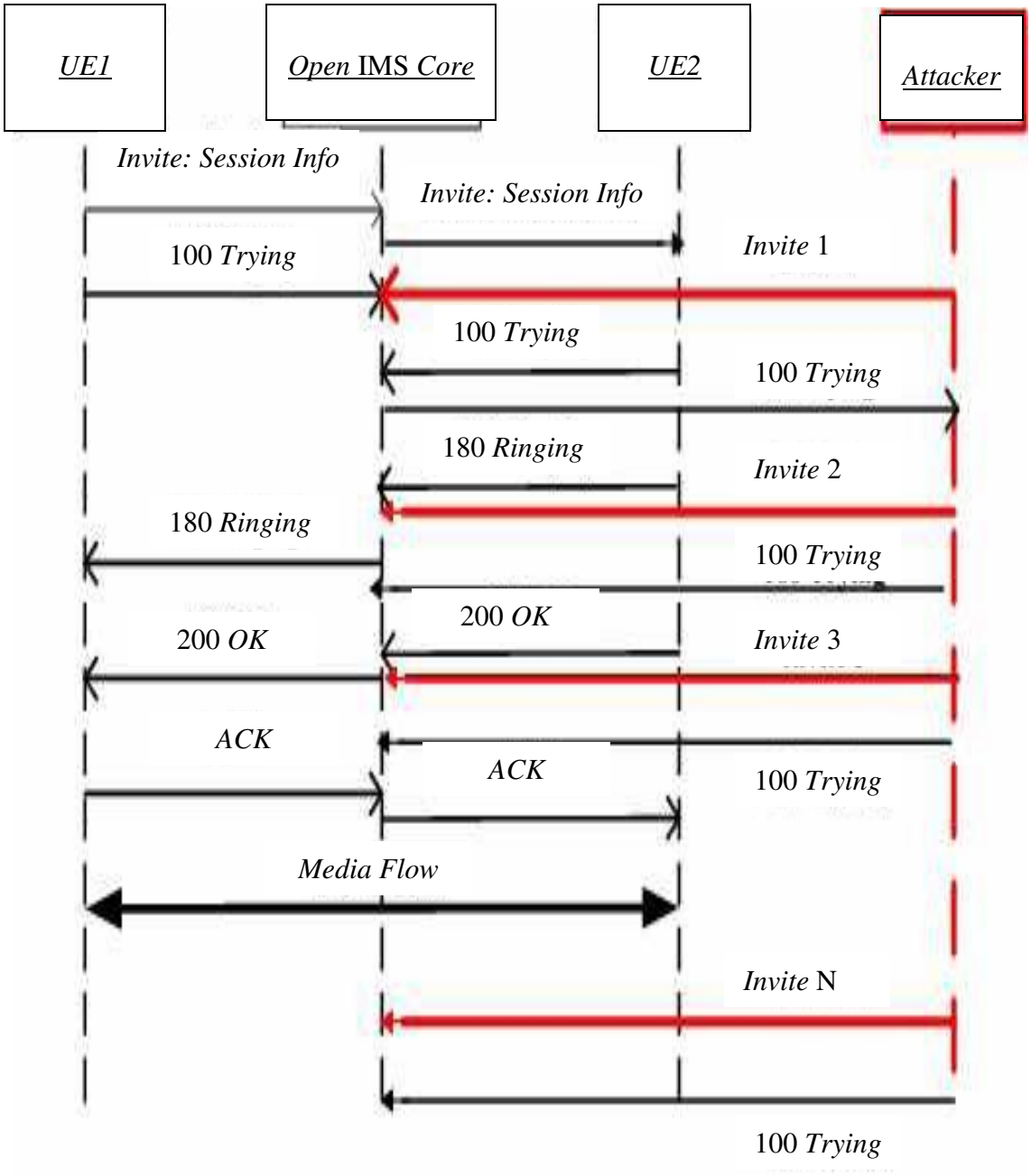

Fig. 5.1 - *INVITE flooding* [32].

• *REGISTER flooding*

A mensagem *REGISTER* é mostrada na Fig. 5.2 abaixo:

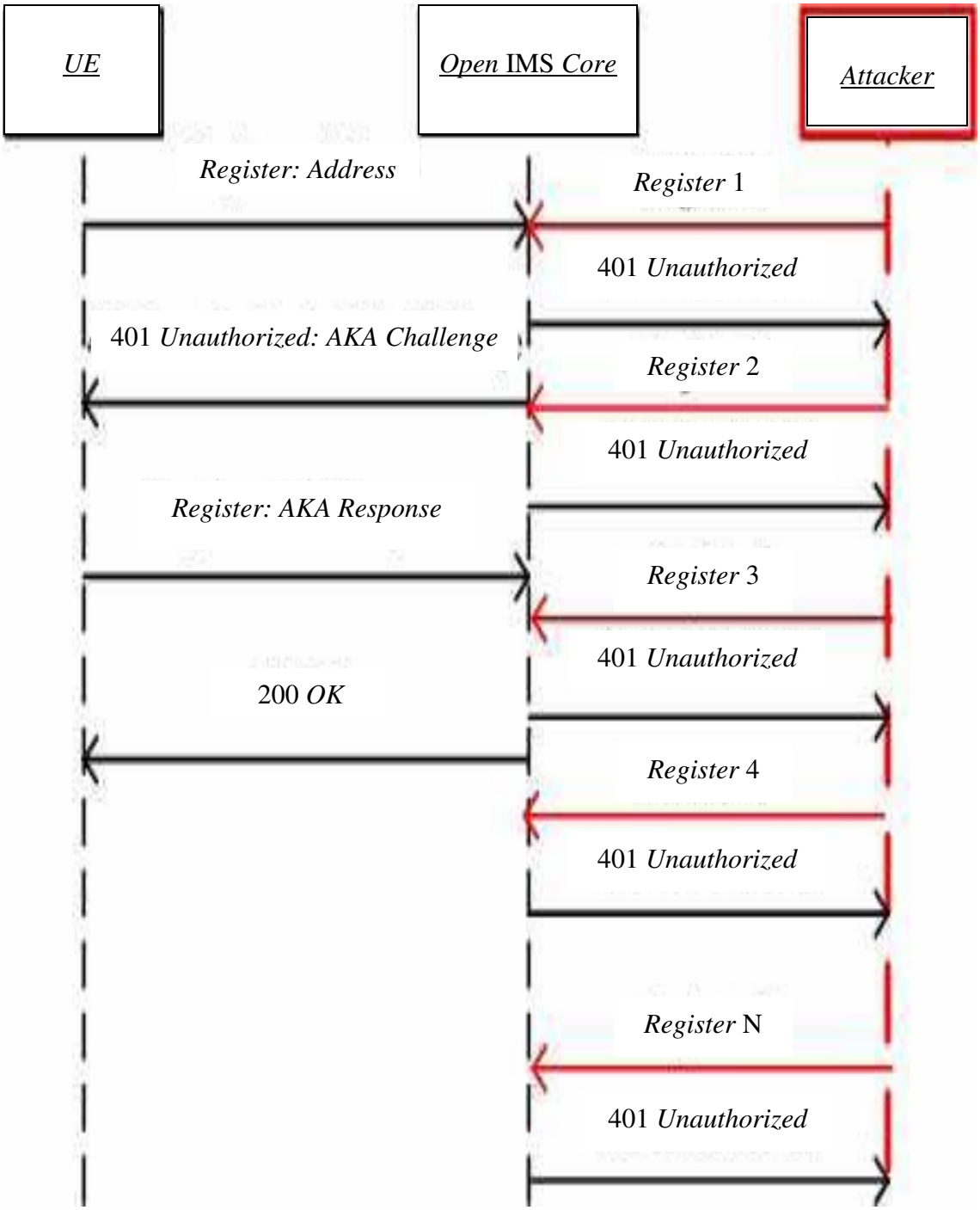

Fig. 5.2 - *REGISTER flooding* [32].

• *BYE denial of service*

Um atacante pode falsificar uma mensagem *BYE* legítima e enviá-la para uma das partes envolvidas na chamada, e dessa forma derrubar a chamada, conforme Fig. 5.3 abaixo:

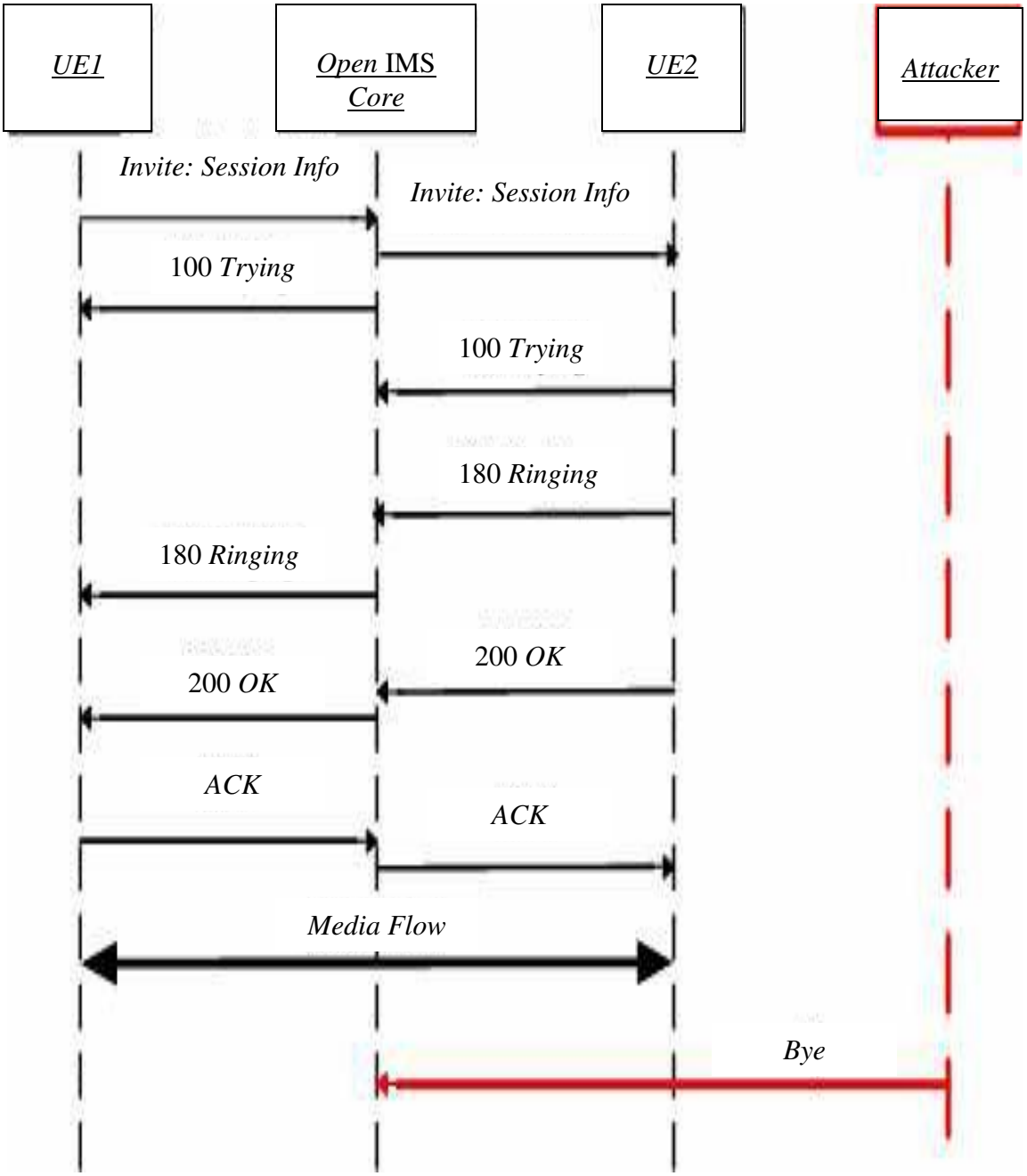

Fig. 5.3 - *BYE denial of service* [30].

• *CANCEL* ataque

O objetivo deste tipo de ataque é fazer o UA inatingível, excluindo o pedido SIP dirigidas a ele, o atacante invasor pode utilizar o *CANCEL* ataque para cancelar requisições *INVITE*, como mostrado na Fig. 5.4 abaixo.

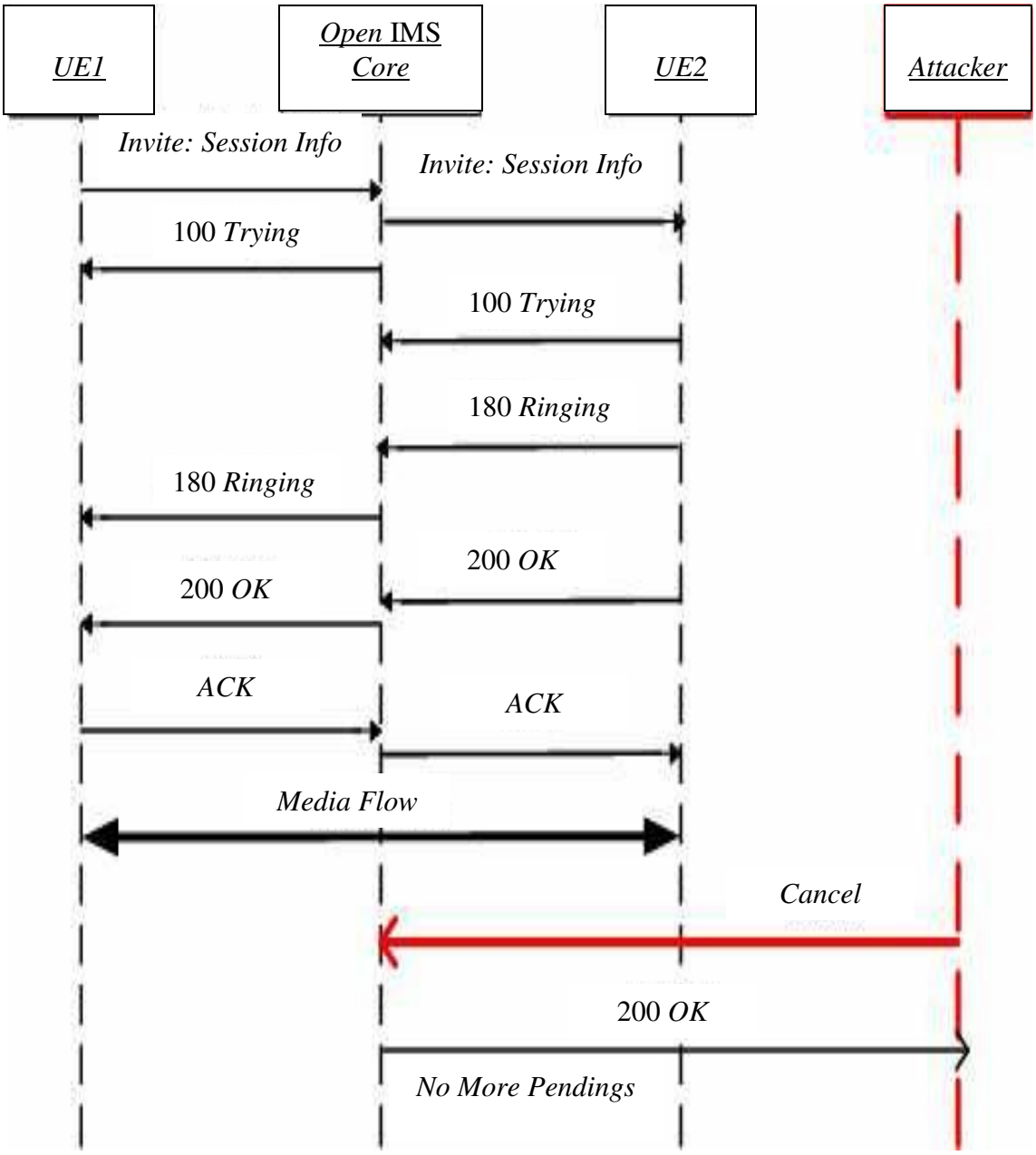

Fig. 5.4 - *CANCEL* ataque [30].

5.2. Análise de Segurança para Provedores de Serviço/Rede

A seguir faremos uma análise das principais falhas de segurança, que podem atingir as redes IMS, na perspectiva dos provedores de serviço/rede:

• A relação IPv4 e IPv6

A controversa relação do IPv4 ante o IPv6 na arquitetura IMS tem sido motivo de muita discussão e debate em relação a arquitetura pois o *design* inicial da arquitetura IMS previa a utilização do IPv6 ao invés do IPv4.

Entretanto, quando a implantação da arquitetura IMS tornou-se realidade o IPv6 não estava completamente desenvolvido e implementado para utilização e a arquitetura IMS acabou tendo que mudar seu *design* original para suportar tanto o IPv4 quanto o IPv6.

Dessa forma muitas das características da arquitetura desenhadas especificamente no IPv6 tiveram que ser modificadas para se adaptar ao IPv4 também, como por exemplo, a adoção do NAT.

No caso do IPv6 não seria necessário dado a abundância de endereços IP únicos, além do que as características do IPSec no IPv6 também deveriam providenciar transporte de dados seguro através da rede.

• Negação de serviço

A arquitetura IMS enfrenta a ameaça de negação de serviço de um maior número de fontes e tem um exposição para ataques de *denial of serv*ice (DoS) muito maior que as infraestruturas de telecomunicações anteriores.

Tal ameaça e exposição seria resultante de sua própria conectividade com a i*nternet* [7], como mencionado anteriormente ataques DoS são aqueles através do qual usuários maliciosos, com algum equipamento com conexão a *internet*, tentam enviar uma quantidade muito alta de mensagens aleatórias para algum elemento da rede IMS.

No intuito de exaurir a capacidade de processamento do sistema, uma vez sem recursos o sistema passa a negar serviços para os usuários legítimos.

Enquanto existem tecnologias que podem diminuir os ataques de DoS da i*nternet*, na arquitetura IMS um determinado atacante com recursos suficientes pode causar no mínimo uma ruptura temporária para algum i*nternet host*.

Assim um ataque mais elaborado numa implementação IMS poderia resultar numa degradação da capacidade do serviço.

Outro potencial cenário para ataques DoS seriam os *user agents* (*user agent* é uma aplicação cliente implementando um protocolo de rede usado na comunicação dentro de um sistema computacional distribuído cliente-servidor) sendo configurados maliciosamente para se tornarem vulneráveis na rede.

Considerando que o usuário acessou conteúdos maliciosos e se infectaram, *isso* resultaria em uma inundação de UAs requisitando serviços no IMS, esgotando dessa forma os recursos da rede, o que também resultaria em negação de serviço para usuários legítimos.

• Topologia de rede

Muitas operadoras preferem que suas estruturas de rede e a capacidade de seus serviços sejam mantidas confidenciais, dessa forma, há muitas maneiras de descobrir *bits* e pedaços de informações simplesmente examinando-se mais de perto os pacotes.

Por exemplo, o número de servidores CSCF na rede e como o pacote está sendo roteado podem ser revelados quando observando a via, a rota, o registro da rota ou os *paths headers* dos pacotes SIP.

No intuito de esconder a topologia da rede interna, os *headers* que podem ser decifrados tal qual o *via header* podem ser encriptados até passarem a fronteira do *gateway* IMS.

• NAT e IPSec

Dispositivos NAT (*Network Address Translation*) são instalados para amenizar a exaustão dos endereços IPv4 permitindo o uso de endereços IP privados em redes locais ou corporativas (redes internas) através de roteadores com um único endereço IP público visível na i*nternet*.

Apesar do IPv6 resolver o problema de escassez de endereços IP, o NAT é uma ferramenta que tem um papel importante na rede.

Ele fornece algum nível de segurança na medida em que limita o acesso direto para os terminais que estão atrás dele, enquanto permite os terminais internos de iniciar uma conexão com terminais externos.

Dessa forma, os endereços IP devem ser atribuídos via DHCP no intuito de resolver o problema de conflitos de IP.

O benefício do NAT também se estende ao gerenciamento da rede onde um administrador pode monitorar um único ponto na rede para avaliar a troca de dados da *internet* para sua LAN.

Apesar dos benefícios, os NATs violam a semântica fundamental dos endereços IP, que é de ser um ponto globalmente acessível para comunicação [10].

O SIP assume que todos os endereços IP usados na mensagem estão globalmente acessíveis, as mensagens SIP originadas de um UA em uma rede privada serão roteadas quando a resposta é encaminhada de volta.

Ele é, portanto necessário para estender o *SIP-aware* dos dispositivos NAT assim como dos mecanismos NAT *traversal* dentro do IMS.

As características fornecidas pelo IPSec garantem a confidencialidade, a integridade e a autenticidade totais de cada pacote emitido e recebido. O IPSec além de fornecer a encriptação do *payload* de um pacote, também garante a autenticação sem conexão da integridade e da origem do pacote individual.

Outro ponto a salientar é que o IPSec não é inteiramente compatível dentro de uma rede através do NAT. A natureza do NAT exige a manipulação do cabeçalho dos pacotes, para substituir o endereço IP privado e os números da porta com endereço e porta globalmente acessível, e vice-versa.

Entretanto, modificando o conteúdo do cabeçalho viola a garantia de integridade e a autenticação da origem do IPSec, que invalida o pacote e conseqüentemente já não pode ser considerado confiável.

Os métodos para fornecer o mesmo nível de segurança em um ambiente NAT seria criar uma passagem IPSec no UDP para o *end host*, ou realizar trocas de chaves separadas entre um terminal privado para um roteador NAT e de um roteador NAT para o terminal de destino.

Possivelmente com o mesmo sendo necessário para o par remoto, todavia dessa forma correndo o risco de se introduzir potenciais problemas de interoperabilidade.

Para que o IPsec possa trabalhar com o NAT os seguintes protocolos devem ser habilitados no firewall:

_IKE *(Internet Key Exchange*) – UDP (*User Datagram Protocol*) port 500;

_ESP (*Encapsulating Security Payload*) - IP *protocol number* 50;

_AH (*Authentication Header*) - IP *protocol number* 51;

No caso do NAT *traversal*

_ IPSec NAT-T - UDP *port* 4500

• Autenticação

A autenticação é categorizada geralmente em três maneiras: algo que você tem algo que você sabe, e algo que você é.

Embora o protocolo de autenticação ideal utilizasse todos os três fatores, o processo de autenticação tornar-se-ia demasiadamente incômodo aos usuários comuns em fazê-lo a cada vez que desejassem usar um dispositivo.

A autenticação atual dos celulares GSM é realizada usando uma chave secreta compartilhada entre a operadora e o usuário. A chave secreta é armazenada geralmente no SIM (*Subscriber Identity Module*) que pode ser removido para permitir uma identificação independente do dispositivo.

Ao contrário dos celulares, os telefones fixos VoIP e outros *softphones* não são equipados com nenhum dispositivo que permita armazenar uma chave secreta.

Desta forma a autenticação de usuário e senha é usada para os dispositivos que não tem uma chave secreta compartilhada. Entretanto, a autenticação usuário e senha implementada no IMS está propensa a ataques forçados e repetitivos, entre outros.

Por exemplo, HSS (*Home Subscriber Server)* é designado para aceitar o endereço IP da última requisição de *REGISTER* como o endereço IP do cliente, porque a autenticação é vulnerável para ataques repetitivos até que a próxima requisição de *REGISTER* seja feita.

Um usuário malicioso pode se registrar novamente usando a mesma resposta com diferentes endereços IP para redirecionar todas as características para algum outro destino.

Isso efetivamente cria uma negação de serviço e o risco de roubo de identidade do usuário legítimo, também com a falta de autenticação dupla um adversário pode assaltar a sessão usando o ataque *man-in-the-middle*.

Um dos ataques *man-in-the-middle* mais famoso consiste em explorar uma falha do protocolo ARP (*Address Resolution Protocol*) cujo objetivo é permitir reencontrar o endereço IP de uma máquina que conheça o endereço físico (endereço MAC) da sua placa de rede.

O objetivo desse ataque seria intrometer-se entre duas máquinas da rede e de transmitir a cada uma um pacote ARP falsificado indicando que o endereço ARP (endereço MAC) da outra máquina mudou, e dessa forma fornecer o endereço ARP do atacante.

Assim cada vez que uma das duas máquinas desejarem se comunicarem com a máquina remota, os pacotes serão enviados ao atacante, que os transmitirá de maneira transparente à máquina de destino.

• Ataques de *gateway*

Os *gateways* IMS são os terminais mais vulneráveis na rede devido a sua exposição ao público e o impacto que eles podem ter quando comprometidos, ou seja, o SGW (*Signaling Gateway*), o MGCF (*Media Gateway Control Function*) e o MGW (*Media Gateway*) requerem algum nível de conversão de formas de conteúdo, que requer manipulação legítima do conteúdo.

Sempre que um dado é convertido para uma mídia diferente, algumas verificações de integridade deveriam ser feitas para verificar se o conteúdo convertido é o mesmo conteúdo que antes em formato diferente e o dado resultante ainda é considerado benigno.

É possível para um usuário malicioso queira fazer uma conversão inversa de um script malicioso (que pode parecer benigno antes da conversão) para algo que pode prejudicar a rede depois que ele foi convertido.

• Fraude de tarifação

Sem dúvida uma das maiores preocupações referentes ao uso de redes IMS por parte das operadoras seria referente aos possíveis ataques que a arquitetura sofreria possibilitando ou abrindo portas para fraudes de tarifação.

Permitindo dessa forma, que usuários ou grupo de usuários possam utilizar recursos de rede da operadora sem ter a correta tarifação ou até mesmo sem tarifação nenhuma, além do que fraudes de tarifação podem acontecer tanto com telefonia móvel como fixa.

Similarmente ao canal de sinalização comum do SS7 o IMS, por ser baseado no protocolo SIP, providencia a separação do canal de sinalização e mídia.

Essa implementação fornece muitos benefícios, entretanto ele impede que as operadoras auditem ou confirmem que o mecanismo de comunicação dos UA (*User Agent*) está funcionando corretamente.

Um UA (*User Agent*) é uma aplicação cliente implementando um protocolo de rede usado na comunicação dentro de um sistema computacional distribuído cliente-servidor. O SIP usa o termo *user agent* para se referir a ambos *end points* de uma sessão de comunicação.

Essa potencial falha das operadoras em auditarem corretamente a comunicação entre os UAs gera a possibilidade de usuários utilizarem serviços não autorizados, seja intencionalmente ou não, abrindo dessa forma a possibilidade de execução de fraudes de tarifação.

Um ponto importante que deve ser levado em consideração é o fato que a maioria dos UAs são desenvolvidos por empresas terceiras e não pelas operadoras, o que dificulta que as operadoras validem a segurança de cada UA antes de permitir o acesso a suas redes.

Também é arriscado para as operadoras assumir que os UA funcionaram corretamente em sua rede, porque quando um dispositivo móvel depende dos recursos de conexão providenciados pela operadora, como as torres de celulares, a operadora consegue coletar e auditar os fluxos de dados para verificar o correto funcionamento do terminal.

Porém com o telefone *dual mode*, por exemplo, isso já não acontece visto que a maioria do tráfego de dados que atinge o IMS chega por meios que não estão sobre controle das operadoras.

No IMS, o HSS fornece o mapeamento entre o endereço IP do UA e a identidade pública fornecida durante o processo SIP *REGISTER*, porém é possível descobrir os endereços IP associados.

Porque durante o processo de setup da chamada, o endereço IP do receptor é fornecido para o originador estabelecer um canal de dados separado.

Dessa forma um UA obtém um endereço IP do UA receptor, com isso ele pode enviar um *CANCEL request* para a rede e estabelecer sua própria conexão com o receptor diretamente usando pacote de dados e voz como se estivesse usando o plano da operadora.

Outra forma de se criar fraude no mecanismo de tarifação seria através dos servidores de *proxy* SIP, os servidores de *proxy* que geralmente são utilizados em ambientes comerciais na forma de sistemas telefônicos PBX, podem também ser usados em ambientes privados para compartilhar a mesma conta entre uma comunidade de usuários.

Esse tipo de fraude pode ser facilmente implementado devido a falta de restrições de localização física dos telefones que existem no PBX tradicional, os servidores *proxy* utilizam o padrão SIP *redirect response* (3xx) para direcionar tráfego para o UA.

Dessa forma um grupo de usuários que desenvolver um UA, um servidor proxy ou construir um servidor *proxy* dedicado que registra na rede IMS, potencialmente poderia compartilhar a identidade de tarifação associada com a mesma conta.

Entende-se que essa questão específica deva gerar questões complexas de segurança para as operadoras IMS, que necessitariam implementar políticas específicas de segurança para evitar esse tipo específico de fraude.

Como mencionado anteriormente fraudes de tarifação podem acontecer tanto com telefonia móvel como fixa, e no que se refere ao caso de serviços VoIP para telefonia fixa, um possível tipo de fraude seria justamente enganar a operadora.

Por exemplo, algumas operadoras oferecem planos específicos com uso ilimitado de voz dentro do estado.

A fraude aqui seria continuar usando o mesmo serviço ilimitado de voz não somente dentro do mesmo estado, como também em outros estados sem pagar taxa extra por isso.

Assim, um UA com um plano ilimitado dentro do estado poderia fazer ligações internacionais por discagem IP depois de descobrir o endereço IP do receptor.

No caso do celular a fraude poderia estar relacionada com os minutos e/ou *kilobytes* usados, já que muitas operadoras cobram os planos por minutos e *kilobytes* usados.

A fraude seria falsificar os minutos de duração da chamada e também fazer transferência de dados entre *user agents* sem detecção ou tarifação por parte da operadora.

5.3. Análise de Segurança para os Usuários da Rede

A seguir faremos uma análise das principais falhas de segurança, que podem atingir as redes IMS, na perspectiva dos usuários:

• Considerações sobre identidade e presença

Do ponto de vista do usuário, uma das maiores preocupações é a segurança de seus dados pessoais.

Com o maior número de aplicações disponíveis conseqüentemente a ameaça à segurança de terminais de usuários, bem como as informações que são armazenadas ou passam através dos terminais aumenta consideravelmente.

Alia-se a esses fatos, o fato do IMS ter sido projetado para facilitar a habilitação de serviços para usuários que alavancam conceitos de redes sociais em nível de arquitetura.

Por exemplo, assinantes IMS podem designar vários grupos de amigos, família ou colegas como tendo acesso aos dados de presença [12], que informa esses grupos de vários atributos do usuário, tal qual status atual, disponibilidade e localização.

Em vez de definir esses grupos em um por base de UA, esses grupos são controlados preferivelmente pelo IMS de modo que o usuário pode esperar que eles funcionassem quando associado com qualquer UA.

Diversos riscos associam-se a esses benefícios tais qual o fato de vários dados de presença que devem ser protegidos contra *eavesdropping* que é uma técnica de *hacking* que se baseia na violação da confidencialidade fazendo a leitura não autorizada de mensagens.

Uma analogia bastante razoável seria a ação de grampear um telefone, ou até mesmo o risco de escalonamento de privilégios dentro de um grupo definido pelo usuário.

Outro tipo de ameaça que surge para um usuário do IMS seria o fato de um usuário malicioso se passar por outra pessoa e ser aceito pelo IMS.

Os usuários podem criar múltiplas identidades públicas distintas que seriam atreladas a uma única identidade privada, essa seria outra ameaça que mesmo não envolvendo roubo de informação pessoal do usuário poderia trazer risco a segurança do usuário.

Esse risco também atinge as operadoras, na medida em que torna inevitável o roubo de serviço, além de ser igualmente uma ameaça aos usuários individuais.

Desde que um usuário malicioso que roube alguma identidade e que use o IMS para afirmar essa identidade a outras pessoas ou serviços poderia resultar em perdas financeiras e individuais intangíveis.

• Aplicações *user agent*

Outra consideração importante é o papel essencial do IMS em fornecer aplicações de conteúdo seguro para o UA.

Como a infraestrutura IMS permite que um conjunto muito mais vasto de aplicações seja disponibilizado, o cenário de ameaças para o UA se alarga também incluindo inclusive ameaças para cada aplicação.

Isso é especialmente verdade dado o importante objetivo do IMS de habilitar operadoras para atuar como provedores de aplicação de empresas terceiras.

Enquanto os benefícios para as operadoras de trazer aplicações de empresas terceiras seria motivante, a ameaça de segurança para o UA representado por conteúdo malicioso coloca sérios riscos para os *User Agents*, e, portanto recursos do usuário.

• Dados pessoais e privacidade

Atualmente usuários estão confiando cada vez mais e mais informações pessoais para as tecnologias digitais. Muitos UAs usam tecnologia GPS que permite o usuário compartilhar suas informações de localização.

Ainda sem empregar GPS, muitas operadoras estão desenvolvendo algumas formas de serviço de determinação de localização e o serviço de localização é um núcleo habilitador do IMS.

Entretanto, o desenvolvimento de serviços baseados em localização tem sido lento como as operadoras procuram a mistura correta de demanda, disponibilidade e possibilidade de comercialização, e em grande parte por causa dos riscos associados com o compartilhamento de dados de localização pessoais.

O IMS oferece uma chance para padronizar a disseminação destes dados entre provedores de serviço de aplicação e UAs, e isso pode ser visto como uma grande conquista para os defensores da privacidade.

Por outro lado, o IMS também herda aplicações terceirizadas que acessam esses dados, além disso, assume uma grande responsabilidade no gerenciamento adequado de preferências do usuário no que diz respeito à privacidade.

Outra preocupação do usuário se refere à voz e privacidade dos dados, ou seja, criptografia, todavia, o fato de estar atrelado a processos regulatórios complexos e incompatíveis fazem com que a criptografia de voz e dados seja algo que dificilmente chegará a algum resultado concreto.

Alguns esquemas de criptografia que usam infraestrutura VoIP para troca de chaves e confiam no UA para criptografar as transmissões subseqüentes tem sido propostos.

Vários fatores fazem essa solução complexa. Como já mencionado, a atual falta de desenvolvimento IPv6 faz muitos esquemas de criptografia que confiam na integridade *end-to-end* difíceis de serem implementados na prática [6].

Além disso, o UA geralmente não tem CPU e bateria suficiente para suportar criptografia de voz, no caso de um aparelho celular, e ainda se eles tivessem, tal sistema poderia ser executado fora dos requisitos regulamentais para escutas telefônicas, visto que sistemas de escutas telefônicas devem obdecer os requisitos legais de cada país.

Conseqüentemente, operadoras IMS, que se dispõem a implementar algum tipo de criptografia devem rapidamente ter que gerenciar qualquer criptografia em nome do usuário.

As operadoras devem também combater as ameaças de usuários maliciosos que tentam disfarçar determinadas trocas a fim evitar o faturamento adequado.

Os desenvolvedores de aplicações terceirizadas poderiam criptografar dados entre o UA e suas aplicações sem permitir acesso por uma operadora (tal qual números de CPF/RG e informações médicas).

Atendendo todos esses requisitos conflitantes cria um ambiente que promove um "denominador comum mais baixo" para segurança, até mesmo para os desenvolvedores bem intencionados, e, portanto representa um risco para a segurança do usuário.

• Negação de serviço

Quando falamos em negação de serviço sempre imaginamos um problema atrelado aos provedores de rede e serviço.

Entretanto na arquitetura IMS o termo além de estarem relacionados aos provedores de rede pode também atingir e afetar os usuários que podem se tornar vítimas de DoS (*Denial of Service*).

Um dos principais atrativos da aquitetura IMS é justamente a garantia da qualidade de serviço (QoS) [3], pois bem o IMS deve garantir que um User Agent terá qualidade de serviço para receber conteúdo.

Da mesma forma que o IMS não tem responsabilidade por garantia de serviço da camada 1, tal qual uma perda repentina de sinal ou interferência RF, o IMS tem responsabilidade em assegurar que a largura de banda provisionada esteja disponível para o UA.

Na medida em que uma entidade maliciosa conseguisse fazer que toda ou pelo menos parte dessa largura de banda fique indisponível para um legítimo UA estaria constituindo um tipo de negação de serviço.

Mesmo que o usuário malicioso não esteja roubando banda para seu uso próprio, o IMS deveria ter mecanismos de proteção para impedir que um usuário malicioso pudesse consumir banda de um usuário legítimo.

5.4. Proposta de uma Metodologia para Eliminar SPIT no IMS

Abaixo apresentaremos uma proposta de uma metodologia para eliminar o SPIT (*Spam over Internet Telephony*) no IMS, basicamente a proposta consistiria em bloquear chamadas de voz não solicitadas usando *decoys* para o IMS.

O *spam* é um sério problema para o *e-mail*, causando frustação e aborrecimento para os clientes, esse problema cresce numa taxa rápida sem sinais de redução. Outra forma de *spam* que surgiu recentemente é o *spam* no VoIP chamado SPIT.

Atualmente, o número de usuário de VoIP aumento significativamente devido principalmente às taxas baratas. Com a introdução do IMS o número de usuários VoIP devem aumentar drasticamente.

As soluções recentes para bloquear o SPIT apresentam algumas falhas e defeitos como: restringir os usuários a uma lista de remetentes confiáveis, causando atrasos no *setup* das chamadas de voz, reduzindo a eficiência do sistema e exigindo modificações dramáticas nos protocolos que estão sendo usados.

A proposta de uma metodologia para eliminar SPIT no IMS seria um sistema de *decoys* para proibir e banir remetentes de SPIT.

Esse sistema de *decoys* para o IMS ajusta-se bem com a estrutura de protocolos existentes, e os clientes ficariam de fora desta operação. Adicionalmente, o método não causaria atrasos nos *setup* das chamadas.

Esquema proposto de *decoy*: os disseminadores de *spams* usam *web crawlers* ou *spiders* para parsear endereços de *email* de *newsgroups*, fóruns, grupos de discussão e a *web*.

Na implementação do IMS resultaria que a SIP URI estaria disponível na *web*. Assim, exatamente como os endereços de *email* são descobertos e recolhidos a SIP URI pode também ser descoberta e recolhida.

Colocando endereços de UEs armadilhas nessas fontes, na medida em que uma pessoa pudesse perceber que são endereços chamariz, mais que um coletor de endereço automatizada não pudesse perceber, ou seja, um recolhedor de endereços automatizado não perceberá a diferença desses endereços.

Consequentemente, os remetentes de SPIT começaram a bater nesses *decoy*. Há, todavia, uma probabilidade muito baixa de uma chamada legítima poder bater nesse *decoy*.

Conseqüentemente, para reduzir falsos positivos, uma conta IMS somente seria banida se a mesma batesse duas ou mais vezes no *decoy*. Esses *decoys* seriam dispersos através de diferentes domínios IMS esperando para pegar fontes SPIT.

Esse esquema é apropriado para o IMS que reforça uma forte autenticação usando o ISIM, impedindo remetentes de endereço *spoofing*.

Ao contrário das contas de *email*, para ter uma nova conta IMS necessitaria de um novo cartão ISIM, assim como, fazer o *subscription* para vários serviços.

Esse procedimento é demorado e resultaria em perdas financeiras para os emissores de *spam*, o que conseqüentemente tiraria o interesse deles. Como resultado, o IMS impediria os remetentes de SPIT de terem contas descartáveis.

O outro método para filtrar SPIT tal como o *feedback* do usuário, reputação do sistema, monitoramente de chamada tem pouco efeito se o remetente do SPIT se mover para um servidor de *proxy* diferente.

Uma vez que o *decoy* recebe uma mensagem SPIT, armazena a mensagem, e informa o HSS do remetente com informação para banir a conta ofensora.

Os HSSs são modificados para armazenar cada usuário em um grupo GREEN, que indicaria que eles não são emissores de *spam*. Cada vez que se bate num *decoy*, o remetente é adicionado para um grupo denotado pelo número de série de *decoy*.

Antes de adicionar para algum desses grupos, o HSS checaria se o usuário pertence a um grupo diferente de *decoy*. Em caso afirmativo, o *status* de GREEN do usuário é revogado.

Os grupos dos *decoys* seriam removidos diariamente para usuários que não tem perdido o *status* GREEN, garantindo probabilidade mínima de falso positivo.

A fim de desativar a conta de um emissor de *spam*, o *decoy* envia a identidade privada do usuário do emissor de *spam* e seu número serial para o HSS do emissor de *spam*.

Assim, temos a configuração de dois cenários, o *decoy* está baseado no mesmo domínio do HSS do remetente de *spam*, logo as mensagens baseadas em *diameter* do *decoy* são passadas via o S-CSCF para o HSS. Caso contrário o *decoy* envia essas mensagens através do P-CSCF e I-CSCF para o HSS.

O *decoy* envia uma UAR (*User Authorization Request*) para o HSS com a identidade pública e privada do usuário remetente, substitui a identificação das redes visitadas com o número de série do *decoy*, e encaixa um novo tipo de autorização de "conta *spam*".

Um UAA (*User Authorization Answer*) é enviado de volta para o *decoy* para identificação do UAR. Essas mensagens são *diameter* com segurança *end-to-end* que pode ser implementada por TLS (*Transport Layer Security*) ou IPSec.

Para proteção do mecanismo de comunicação entre os *decoys* e o HSS será estabelecido um mecanismo de criptografia com segurança IPSec, no intuito de evitar que um atacante possa falsificar ou corromper as mensagens entre o *decoy* e o usuário.

Se o status GREEN for revogado, logo o HSS remetende de *spam* informa o S-CSCF usando um PPR (*Push Profile Request Message*). Essas mensagens PPR, UAR, e UAA já são parte das estruturas de mensagem do IMS.

Uma vez que o usuário banido tenta fazer uma nova chamada, o *INVITE* é passado para o S-CSCF que realiza a filtragem inicial tendo por resultado as chamadas que serão perdidas se o *status* GREEN não estiver presente.

Além disso, o S-CSCF pode informar o remetende de spam com uma mensagem SIP de bloqueio de conta e o que seguirá uma ação legal.

Uma ação legal será possível nesse método desde que os *decoys* podem armazenar as mensagens SPIT que podem ser identificadas nos registros do HSS.

Abaixo na Fig. 5.5 apresentamos uma especificação da proposta.

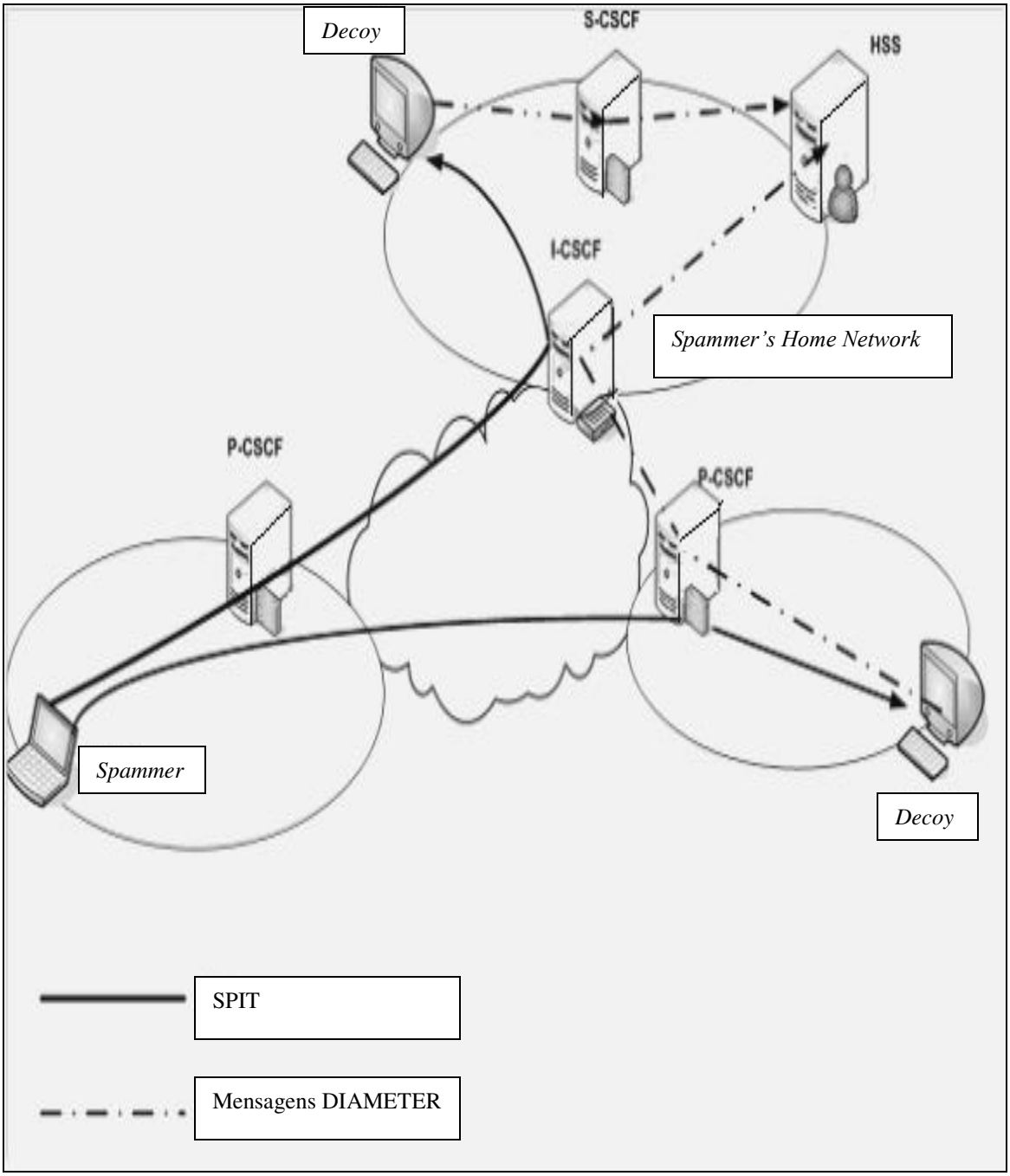

Fig. 5.5 – Especificação da proposta de uma metodologia para eliminar SPIT no IMS.

CAPÍTULO 6

MÓDULO DE SEGURANÇA PARA O IMS UTILIZANDO AIS E AGENTES MÓVEIS

O SIP é um protocolo altamente vulnerável e sujeito a falhas de segurança desde *eavesdropping*, interceptação de informações de sinalização e conversação, adulteração de chamada, ataques *man-in-the-middle* e até negação de serviço.

Os subsistemas multimídia usam o protocolo SIP para sinalização (inicializar, gerenciar e terminar sessões de voz e vídeo), sendo responsável por todo o processo de registrar, configurar e gerenciar as sessões.

Dessa forma as redes baseadas em SIP estão sujeitas a ameaças externas que são lançadas por alguém que não está envolvido no fluxo de mensagem da chamada baseada em SIP e ameaças internas geralmente lançadas por participantes de chamada SIP.

O objetivo do módulo de segurança proposta é justamente melhorar o nível de segurança existente, uma vez que protegem os componentes centrais do IMS, o P-CSCF, I-CSCF, S-CSCF e HSS de ameaças internas e externas tais quais *eavesdropping*, SQL *injection* e ataques de negação de serviço (DoS).

No módulo proposto todas as atividades relacionadas aos componentes centrais do IMS são feitas com agentes móveis. Agente móvel é uma abordagem promissora para desenvolvimento de aplicações distribuídas.

Particularmente, o crescente interesse na tecnologia de agentes é motivado pelo seu potencial uso em diversas áreas, incluindo comércio electrônico, disseminação e coleta de informação, sistemas de telecomunicações, personalização de serviços e sistemas de monitoramento [20, 21].

6.1. Análise de Vulnerabilidades nas Redes IMS

Como já abordado no Capítulo 4 o 3GPP adotou o AKA (*Authentication and Key Agreement*) protocolo para as comunicações *wireless* de terceira geração (3G).

O AKA é usado para autenticação entre o UE e o P-CSCF, na medida em que um cliente IMS necessita estabelecer associação com o P-CSCF para o estabelecimento de comunicação.

Na visão do 3GPP esse mecanismo de autenticação e protocolo de acordo com chaves usado no IMS é consistente e seguro.

Todavia, algumas pesquisas como [30] demonstraram que o mecanismo de segurança 3GPP AKA é vulnerável a vários tipos de ataques.

Tal vulnerabilidade permite que um adversário redirecione o tráfego do usuário de uma rede para outra, além de permitir o uso de vetores de autenticação corrompidos de uma rede para representar todas as outras redes, fazendo com que a corrupção de uma rede comprometa todo o sistema.

Assim, AKA tem sido criticado devido a suas vulnerabilidades e ataques de redirecionamento ativos na rede corrompida.

Dessa forma destacaremos três tipos de ataques que as redes IMS se tornam vulneráveis [31]: os ataques de redirecionamento, os ataques ativos e os ataques de re-sincronização.

Os ataques de redirecionamento ocorrem quando uma rede está corrompida e o adversário poderia falsificar uma requisição de autenticação de dados a partir da rede corrompida para obter vetores de autenticação.

Porém, o adversário poderia falsificar o número de sequência a ser definido para um valor muito alto provocando inundação de dados de autenticação na rede origem.

Dessa forma, o adversário poderia realizar ataques ativos contra todos os usuários legítimos. O adversário usaria uma falsa estação base e móvel, através de dispositivo móvel, o adversário pode representar como uma estação base genuína e estabelece conexão com uma estação base genuína.

Essa integração de falsas estações base e móvel permitiria o adversário reproduzir mensagens entre estações móveis legítimas e estações base genuínas.

O processo de autenticação seria completado com sucesso entre o usuário e a rede externa, assim o ataque de redirecionamento seria lançado com sucesso.

Nos ataques ativos, como em AKA os vetores de autenticação são transferidos entre e dentro das redes, quando uma rede é corrompida um adversário poderia falsificar solicitação de dados de autenticação da rede corrompida para obter vetores de autenticação de qualquer usuário, independente da localização do usuário.

Em seguida, o adversário poderia usar os vetores de autenticação obtidos para personificar as redes atacadas e montar uma falsa estação base para realizar ataques contra os usuários legítimos [29]. Também poderia lançar um ataque de inundação, definindo o valor do contador muito alto.

Uma vez que a corrupção de uma rede pode comprometer todo o sistema, é fundamental que medidas de segurança sejam realizadas em cada rede. Não existe um mecanismo de segurança disponível para controlar ataques em redes corrompidas.

O ataque de re-sincronização está relacionado com o requisito AKA onde a rede origem deve manter um contador para cada assinante.

Assim, caso ocorra alguma mudança no banco de dados que armazena os contadores na rede origem, isso afetará todas as estações móveis inscritas na rede origem.

Se o adversário conseguir atacar a estação base falsa, poderia corromper o contador de sincronização.

O objetivo é fazer com que a rede passe a não funcionar corretamente, enviando informações de roteamento falsas, como por exemplo, enviando uma rota que não existe.

Também poderia inundar a rede com pacotes (ataques de negação de serviço). Nesse caso, o processo para sincronizar os contadores mantidos para cada assinante será extremamente complicado e custoso, especialmente se o usuário estiver em *roaming*.

6.2. Sistemas Imunológicos e Segurança Computacional – AIS e Agente Móveis

O uso de mecanismos inspirados em sistemas de imunização no âmbito da engenharia e computação é algo que já existe e está sendo estudado há muito tempo.

A literatura existente sobre AIS (*Artificial Immune System*) revela que a maioria dos mecanismos e aplicações computacionais é escolhida com base na suposição comum de que a função principal do sistema imunológico é separar o "auto" do "não-auto".

De acordo com [22, 23], o sistema imunológico humano protege o corpo de várias bactérias e viroses, ele defende o corpo contra doenças prejudiciais e infecções.

Sendo capaz de reconhecer virtualmente qualquer célula externa ou molécula e eliminá-la do corpo. O sistema passivo e imune adaptativo é produzido principalmente por leucócitos.

Fagócitos e linfócitos são tipos diferentes de leucócitos. Fagócito é o primeiro ponto de defesa para o sistema imunológico humano, o sistema imunológico adaptativo consiste principalmente de linfócitos que circulam através do corpo no sistema sanguíneo e linfático.

Uma vez que agentes patogênicos entram no corpo, eles são tratados pelo sistema imune passivo e pela resposta adaptativa imune.

O sistema de imunização passivo é constituido principalmente de células circulatórias *scavenger* tais quais os macrófagos que ingerem moléculas e materiais extracelulares, limpando o corpo de detritos e agentes patogénicos.

A resposta do sistema de imunização adaptativo é mais sofisticada e envolve diferentes tipos de células e moléculas, sendo chamado de adaptativo porque ele é reponsável pela imunização que é adquirida adaptativamente durante o tempo de vida do organismo.

Dessa forma, chegamos ao ponto onde focaremos nossa proposta, na medida em que o sistema imune adaptativo fornece grande potencial de segurança, enfatizaremos apenas alguns detalhes relevantes à proposta de segurança.

O sistema imunológico consiste de diferentes populações de células de imunização principalmente células B ou C que circulam em vários orgãos linfóides primários e secundários do corpo. O sistema imunológico consiste de duas camadas principais que seriam as camadas passiva e adaptativa.

As camadas passivas consistem de pele, membranas, pH, temperatura e resposta de processos inflamatórios.

As camadas adaptativas consistem de mecanismos de células, todos os organismos pertencentes ao corpo humano são marcados como "auto", assim os organismos que são identificados como "não-auto" são detectados e destruídos pelo sistema de imunização.

O sistema de imunização adaptativo reage dinamicamente a células estranhas. Existem dois tipos de células que são usadas no processo de detecção de células estranhas: células-B e células-T, as células-B são geradas na medula óssea, enquanto as células-T são geradas no timo.

As células-T são por sua vez classificados como células-T auxiliares e células-T assassinas.

As células-T auxiliares ajudam as células-B detectaram as células estranhas escondidas dentro do corpo humano, enquanto células-T assassinas matam as células estranhas.

As células-B reconhecem as células estranhas e criam anticorpos com as funções que se ligaram as células estranhas. Antes das células-B serem liberadas da medula óssea elas são testadas para certificar-se que poderam detectar anomalias corretamente.

Elas passam por um estágio chamado de seleção negativa no qual as células-B que detectam os organismos como "auto" são excluídas e desqualificadas, assim que essas células-B passam no teste são liberadas no organismo.

Quando uma célula externa é detectada, células de memória separada são criadas através da detecção de células-B que lembram a célula externa detectada.

Células de memória armazenam informação sobre células externas que foram detectadas no passado, e essas células de memória tem expectativa de vida maior do que as células-B e células-T normais.

As células-T também são testadas utilizando seleção negativa antes de ser liberadas a partir do timo. As células-B e as células-T detectam tipos diferentes de células externas.

As células-T e células-B sofrem um processo chamado de mutação na informação genética. A informação genética contém todos os genes que são usados para criar diferentes tipos de células.

A informação genética adapta-se continuamente e cria projetos para criar anticorpos melhores que detectam uma maior variedade de células externas.

As informações genéticas estão em constante evolução e os genes são usados para manter a diversidade de anticorpos através da geração de diferentes tipos de genes.

O sistema imune adaptativo reage dinamicamente a células estranhas que consistem de células-B e células-C.

Os sistemas imunológicos têm muitas características que fazem com que trabalhem bem em ambientes abertos, sem controle e imperfeitos, que na realidade é o ambiente onde os sistemas computacionais residem.

A ligação entre sistemas imunológicos e segurança computacional foi primeiramente introduzida em [24,25] e elaborada em [26,27], no qual foram introduzidos atividades com agentes móveis.

Agente móvel é um pequeno objeto ativo inteligente que é capaz de realizar atividades de forma contínua e automática em um determinado ambiente, eles são uma abordagem promissora para o desenvolvimento de aplicações distribuídas.

Particularmente, o interesse crescente na tecnologia de agentes tem sido motivado pelo seu potencial uso em um grande número de áreas, incluindo comércio eletrônico, coleta de informações, sistemas de telecomunicações, serviços personalizados e monitoramento de sistemas [28].

O sistema de agentes é significativo para ser o sistema de interação de agentes, pois eles são coordenados por uma estratégia definida, mais suficientemente autônoma para realizar as suas próprias tarefas no âmbito da estratégia geral.

Dessa forma, entende-se que todas essas qualidades fazem dos agentes móveis a escolha natural para um módulo de segurança, assim iremos propor um módulo de segurança onde todas as atividades serão feitas com agentes móveis.

Para isso criaremos uma analogia entre sistemas de imunização e o módulo proposto, onde o sistema de imunização será o próprio módulo de segurança, as células-T serão o agente de detecção, as células-B serão o agente analítico, as células de memória serão o agente banco de dados, a produção de anticorpos específicos será o agente de monitoração e por fim os anticorpos serão o agente de eliminação.

Há muitas semelhanças entre o sistema de segurança computacional e o sistema imunológico biológico, o sistema imunológico humano produz anticorpos para resistir a agentes patogênicos através das células-B atuando no corpo humano e as células-T regulam a concentração de anticorpos.

A proposta do módulo de segurança seria simular o sistema biológico imunológico, onde células de imunização (agentes móveis) seriam colocadas nas redes.

Esses agentes móveis colocados na rede providenciariam uma análise determinística, onde quando um ataque for detectado, o pedido de determinado usuário que levaria a queda dos serviços IMS SIP, seria bloqueado e os detalhes do usuário seriam armazenados na memória imunológica.

Assim, o sistema desenvolvido irá realizar monitoramento em tempo real, análise e geração de resposta adequada às atividades intrusivas.

Basicamente, assim que uma solicitação entrasse na rede, o agente de detecção seria notificado, acionando o agente analisador, que procederia com a requisição de acordo com a análise determinística realizada, encaminhando a requisição para o agente de monitoração, ou para o agente de eliminação e assim encaminhando para o agente banco de dados.

6.3. Proposta de Módulo de Segurança para o IMS Utilizando AIS e Agentes Móveis

Uma das principais questões de segurança que o IMS enfrenta são os ataques de inundação (*flooding attacks*) que causa a queda ou o colapso dos recursos e serviços IMS.

Como já mencionado, *flood DoS* e ataques DDoS são aqueles ataques em que um usuário mal-intencionado deliberadamente envia uma quantidade tremendamente grande de mensagens aleatórias para elementos do núcleo de rede IMS a partir de uma única localização (DoS) ou de múltiplas localizações (DDoS).

Como a quantidade de mensagens está muito acima da capacidade de processamento do sistema, rapidamente os recursos do sistema são exauridos e esgotados, consequentemente acaba resultado na negação de serviços para usuários legítimos.

Sem dúvida, esse tipo de ataque é um dos mais ameaçadores que a arquitetura IMS enfrenta, e como os requisitos de segurança apresentados pelo 3GPP não conseguem eliminar essa ameaça, a principal proposta do módulo de segurança apresentado seria detectar e proteger o núcleo da rede IMS contra ataques de inundação DoS e DDoS.

Dessa forma, o módulo proposto deverá detectar e eliminar os ataques de SQL *injection* durante o procedimento de autenticação do UE e P-CSCF.

Além do que, na medida em que é detectada uma sobrecarga de CPU no P-CSCF alguns procedimentos deverão ser executados.

O processo de autenticação contínua de usuários legítimos deverá ser executado, assim as mensagens *REGISTER* / *INVITE* de UEs legítimos e conhecidos, que já obtiveram anterior autenticação de usuário com sucesso ainda serão aceitas.

Mensagens *REGISTER* de usuários desconhecidos serão bloqueadas, uma vez que essas mensagens podem ser a causa da sobrecarga no núcleo do IMS.

O módulo proposto é baseado no núcleo do IMS e está integrada com o P-CSCF, a localização seria entre o cliente IMS e o núcleo do IMS.

Assim, o objetivo do módulo proposto seria proteger o núcleo do IMS dos ataques já mencionados, principalmente os mencionados em 5.1.1 e 6.1, dessa forma todas as mensagens de entrada e saída passariam e seriam processadas através do módulo proposto.

Por questões de desempenho do sistema, o módulo proposto investigará os ataques no núcleo IMS baseado nas condições de carga de processamento da CPU.

Assim quando a CPU está com carga normal de processamento, todas as mensagens de entrada e saída serão investigadas para detectar e previnir ataques de SQL *injection*.

Em outro nível serão considerados ataques de negação de serviço (DoS) quando a carga de processamento da CPU excedeu um limite pré-estabelecido.

Assim no módulo proposto estaremos realizando monitoramento da carga de processamento da CPU, e se o limite de processamento estabelecido for ultrapassado determinadas ações serão tomadas.

O P-CSCF é o primeiro ponto de contato com o núcleo IMS, o P-CSCF é atribuído para um núcleo IMS durante o processo de registro e continua sendo atribuído durante toda a duração do registro.

O P-CSCF autentica o usuário e estabelece uma associação de segurança IPSec com o terminal IMS e estabelece as mensagens de sinalização.

Dessa forma, todas as requisições que entrarem no núcleo IMS serão processadas pelo módulo proposto e depois de realizada a verificação da solicitação que está entrando ela será enviada ao I-CSCF, as requisições ou mensagens que forem identificadas como ataques serão bloqueados.

Na Fig. 6.1 abaixo apresentaremos a localização do módulo de segurança proposto que será definido entre o cliente IMS e o núcleo IMS.

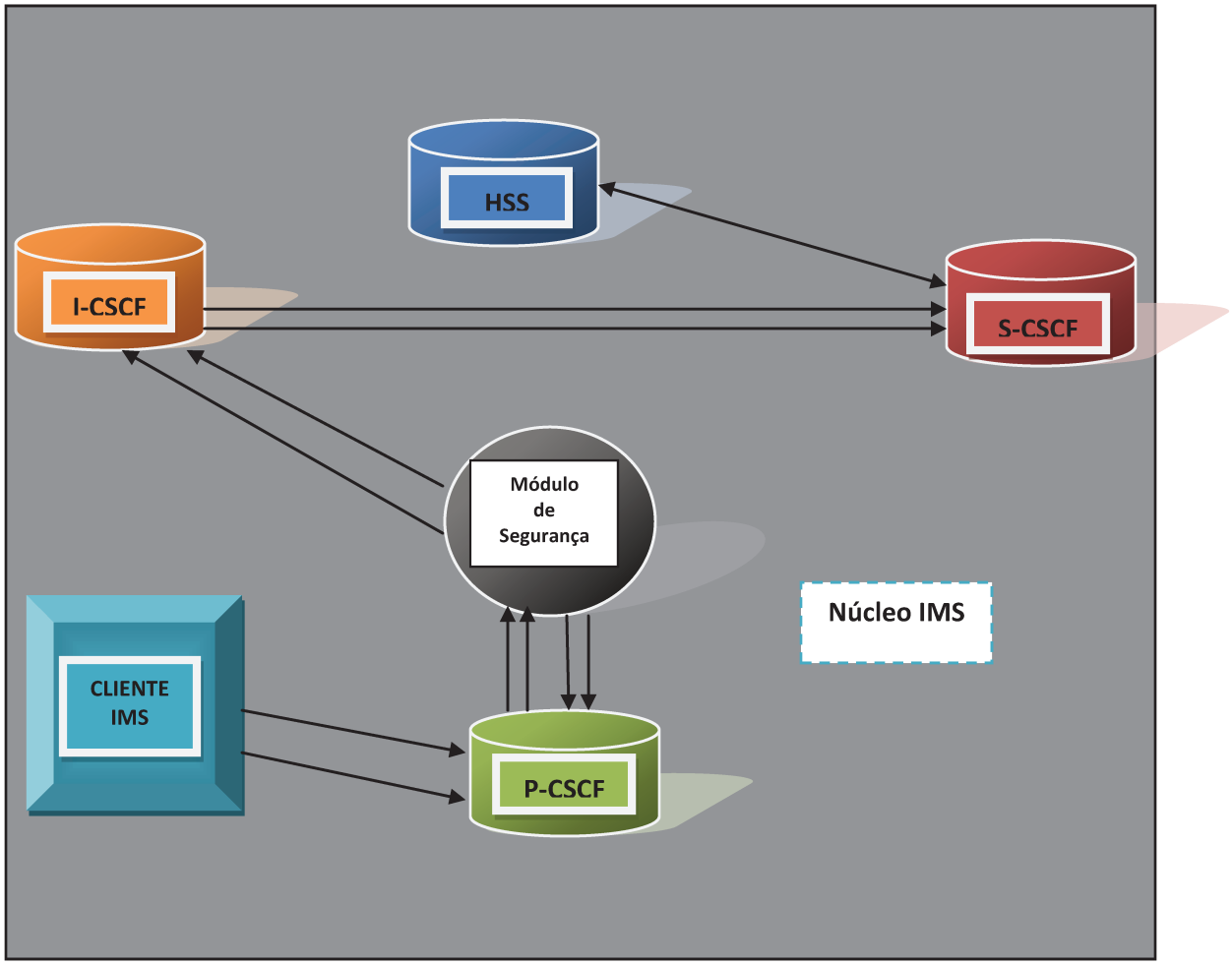

Fig. 6.1 - Esboço da localização do módulo de segurança.

O módulo proposto para segurança do núcleo IMS é baseada em AIS que é capaz de detectar, identificar e se recuperar de um ataque, dessa forma no módulo de segurança proposto o AIS atuará em parceira com os agentes móveis, conforme a Fig. 6.2 abaixo:

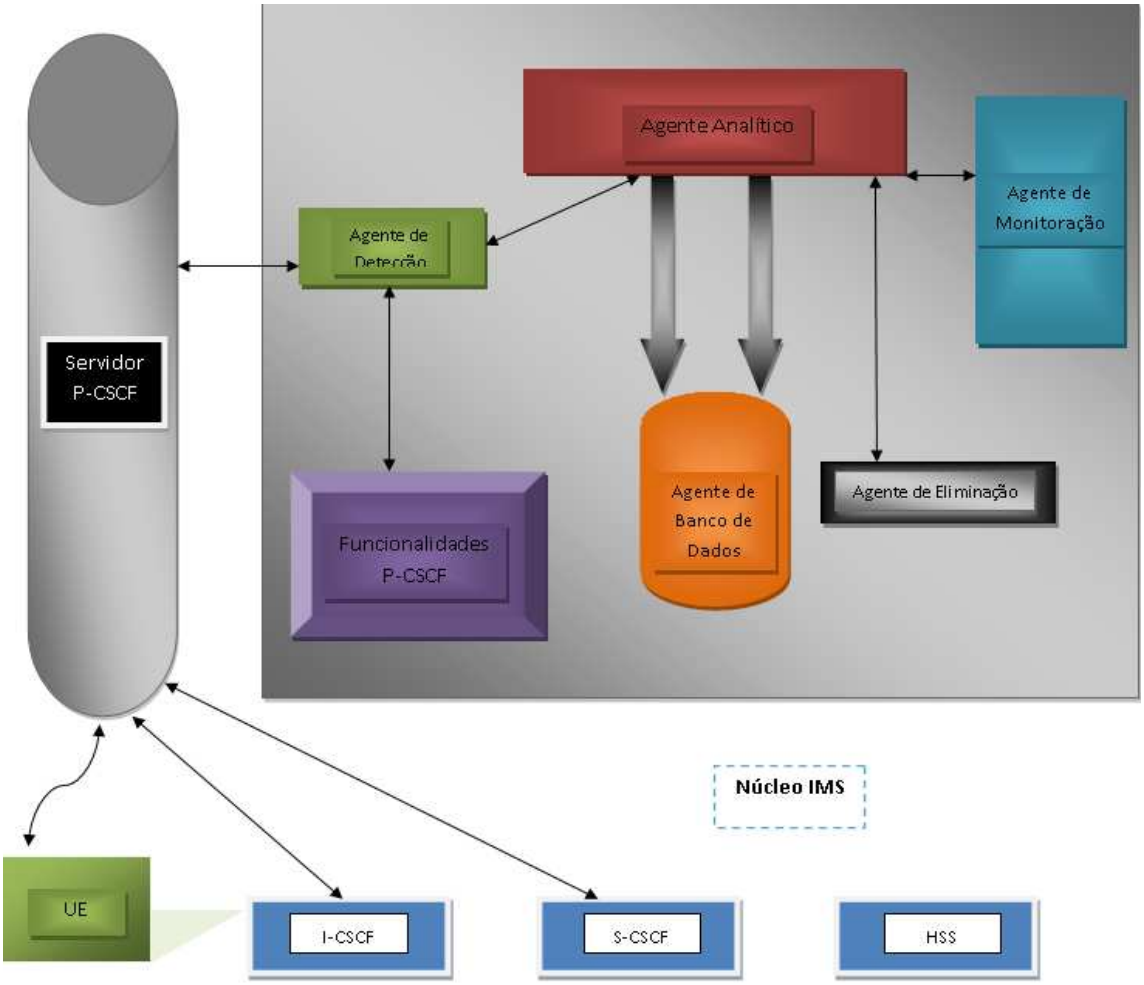

Fig. 6.2 - Módulo de segurança para o IMS utilizando AIS e agentes móveis.

6.3.1. Componentes do Módulo

Abaixo apresentaremos os componentes essencias do módulo proposto:

• Agente de detecção

No organismo humano, na medida que, os linfócitos encontram antígenos estranhos no organismo eles o subjugam e o destroem, sendo o antígeno estranho já é conhecido pelo sistema imunológico, anticorpos específicos podem ligar-se diretamente ao antígeno, fazendo os micróbios atraentes para outras células do sistema imunológico.

Assim, consideraria-se um agente de detecção similar a uma célula-T que residiria em cada nó em uma rede móvel. O agente de detecção monitoraria as mensagens SIP de entrada tanto do UE quanto do P-CSCF e encaminharia para o agente analítico para posterior processamento.

• Agente analítico

O agente analítico é o cérebro e o agente principal do módulo proposto, sendo responsável pela análise e pela tomada de decisões para proteger o núcleo do IMS contra os ataques de *flooding* e *fuzzing*.

Como mencionado anteriormente o agente de detecção já encaminhou todas as informações para o agente analítico, de posse dessas informações começa o trabalho do agente analítico.

As células-B produzem anticorpos que os distinguem como vírus, a própria célula-B não tem capacidade para eliminar antígenos.

Assim, a memória armazenada sobre um ataque anterior permite com que futuros ataques tenham resposta a ataques muito mais rápidos.

Da mesma forma o agente analítico mantém a lista de usuários confiáveis que são registradas na base de dados e, posteriormente, ele compara essa informação no banco de dados com a ajuda do agente banco de dados.

Assim, os pacotes de entrada (pacotes SIP que entram na rede) são comparados com a memória de imunização para detectar se eles podem ser classificados como "auto" ou "não-auto".

Dessa maneira, o mecanismo de segurança é fornecido para os pacotes SIP, evitando *flooding* (inundação), SQL *injection* e *message overflow* (estouro de mensagem).

O agente analítico usa diversas regras na tomada de decisão para iniciar uma ação particular, esse conjunto de regras pode ser alterado a medida que o sistema ganha maturidade e também evoluirá através dos dados armazenados.

O procedimento de análise detecta a razão da sobrecarga e decide interromper a comunicação de usuários ilegítimos dentre um intervalo de tempo definido.

• Agente de monitoração

O agente de monitoração trabalharia monitorando a carga de processamento do P-CSCF CPU, comparando-a com os limites pré-estabelecidos indicando dessa forma o nível crítico.

• Agente banco de dados

A memória imunológica do organismo humano é um banco de dados de assinaturas de antígenos perigosos conhecidos, e os anticorpos e células-B receptoras são assinaturas de antígenos específicos que o sistema imunológico já encontrou.

Esses componentes do sistema imunológico permitem responder de forma mais eficiente a novas exposições a um invasor já conhecido.

Da mesma forma o agente banco de dados no módulo proposto mantém lista de usuários de confiança que já tenham sido registrados com sucesso.

• Agente de eliminação

Quando um patógeno entra no corpo, o sistema imunológico adaptativo, que consiste de linfócitos que circulam através do sangue, as células-B, que no módulo proposto seriam agentes de detecção, através dos linfócitos produzem anticorpos em resposta aos anticorpos estranhos.

Quando os anticorpos se ligam a antígenos eles enviam um sinal para as células fagocíticas ou células-T de eliminação para engolir e eliminar os antígenos do organismo.

Dessa forma, as células-T de eliminação são fundamentais na eliminação de antígenos do organismo. Essas células no módulo proposto seriam representadas pelo agente de eliminação cuja função seria bloquear um determinado endereço ou remetente IP.

6.3.2. Metodologias para Detecção de Ataques

Depois de termos destacados os componentes centrais do módulo proposto, iremos agora destacar como o módulo procederia na detecção e eliminação dos ataques de inundação, apresentaremos dessa forma a metodologia de detecção para os ataques de SQL *injection*, *REGISTER flooding* e *INVITE flooding*, conforme abaixo:

• SQL *injection*

O módulo proposto irá detectar ataques de SQL *injection* que tem por objetivo causar atraso no fluxo de processamento das mensagens SIP *REGISTER*.

Esse ataque pode ser lançado simplesmente pela inserção de instruções SQL no início do procedimento de autenticação entre o UE e o P-CSCF.

Quando o P-CSCF solicita autenticação o UE calcula as credenciais com base no mecanismo HTTP *Digest* [35], essa mensagem é enviada ao S-CSCF via P-CSCF.

O usuário malicioso poderia lançar o SQL *injection* no IMS inserindo código SQL malicioso no cabeçalho de autorização, essa mensagem poderia ser qualquer mensagem SIP que fosse requisitar autenticação pelo P-CSCF.

O código pode ser incorporado no nome do usuário ou em campos do cabeçalho de autorização e se parece com o exemplo apresentado em 5.1.1

O P-CSCF recebe uma mensagem SIP com um cabeçalho de autorização infectado, ele gera e executa a instrução SQL maliciosa que pode deletar ou modificar dados no banco de dados [35].

No módulo proposto para detectar SQL *injection*, o agente analítico irá examinar a mensagem SIP e verificará a mensagem contendo nome de usuário SIP com ponto e vírgula na instrução SQL.

Caso esse comportamento seja detectado, o agente analítico reconhece o ataque de SQL *injection* e o posterior processamento de mensagens SIP será interrompido para esse usuário.

• *REGISTER flooding*

O sequestro do processo de registro ocorre quando uma mensagem *REGISTER* é enviada pelo *hacker* com dados roubados do assinante.

O ataque de *REGISTER flooding* pode ser lançado através da geração de múltiplas mensagens SIP *REGISTER* de um único ou de múltiplos *hosts* para fazer com que os recursos IMS entrem em colapso.

Dessa forma, o atacante envia uma grande quantidade de mensagens SIP *REGISTER* para a vítima, fazendo assim com que a CPU esteja ocupada processando essa grande quantidade de mensagens.

Esse tipo de ataque exaure os recursos disponíveis, como ciclos de CPU, amazenamento e principalmente a largura de banda da rede, fazendo com que a máquina de destino não consiga mais responder a nenhum tipo de requisição, portanto o tráfego legítimo sofre os danos colaterais.

O objetivo do módulo de detecção é detectar o início de um ataque e identificar a vítima através do monitoramento das estatísticas do tráfego.

O método de detecção de *REGISTER flooding* vêem em ação quando o fluxo de mensagens SIP se inicia, assim quando for detectado um comportamento anormal o procedimento será inicializar um contador e checar o endereço IP de origem e o número da porta.

O agente de monitoração faz a verificação periódica da carga de processamento da CPU e a contagem de mensagens SIP com o contador.

Dessa forma, o limite máximo de mensagem *REGISTER* padrão foi atribuído a 15 para um período de tempo de 60 segundos, assim a chegada do décimo quinto pacote dispara o estado de suspeita, fazendo com que o agente analítico passe a processar todas as mensagens SIP usando o processo de detecção de anomalia.

A técnica de detecção de anomalia cria perfis normais de estados do sistema ou comportamento do usuário, mantendo-o no banco de dados e comparando-o com as atividades atuais.

Se algum desvio significativo é observado, o sistema dispara um alarme e assume que o núcleo do IMS está sob ataque de inundação.

Nesse ponto o agente analítico analisa e rejeita todas as requisições *REGISTER* desconhecidas enquanto continua processando todas outras mensagens SIP.

• *INVITE flooding*

O método de detecção de inundações de *INVITE* é similar ao método de inundações de *REGISTER*.

O agente de monitoração inicializa um contador para contar as mensagens de *INVITE* ou assinantes SIP, se uma inundação for detectada, o agente de monitoração sugere ao agente analítico a mudança do estado de normal para crítico e continua processando todas as outras mensagens SIP.

Depois de 60 segundos um timer é inicializado e novamente a condição de sobrecarga é verificada.

Quando o limite pré-estabelecido é ultrapassado, ou seja, se exceder 15 mensagens em 60 segundos, o agente analítico verifica que a inundação é resultado das mensagens *INVITE* e o agente analítico interrompe todas as mensagens desconhecidas que usam essa anomalia.

6.3.3. Especificação de Cenários

Simularemos os cenários para os ataques mencionados acima, na medida em que o P-CSCF recebe requisição do UE, a requisição é encaminhada pelo agente de detecção para o agente analítico para realizar os processamentos, todavia para as mensagens de *REGISTER* e *INVITE* primeiramente será feita a verificação para SQL *injection*.

• Especificação de cenário para *REGISTER flooding*

O agente de monitoração verifica a inundação de mensagens *REGISTER* através da análise da carga de processamento da CPU.

Caso sejam encontradas falhas criadas por determinados usuários, todos os detalhes relacionados ao processo serão armazenados e o agente de eliminação bloqueará esse endereço IP, conforme especificado na Fig. 6.3 abaixo, que mostra o mecanismo de detecção e prevenção:

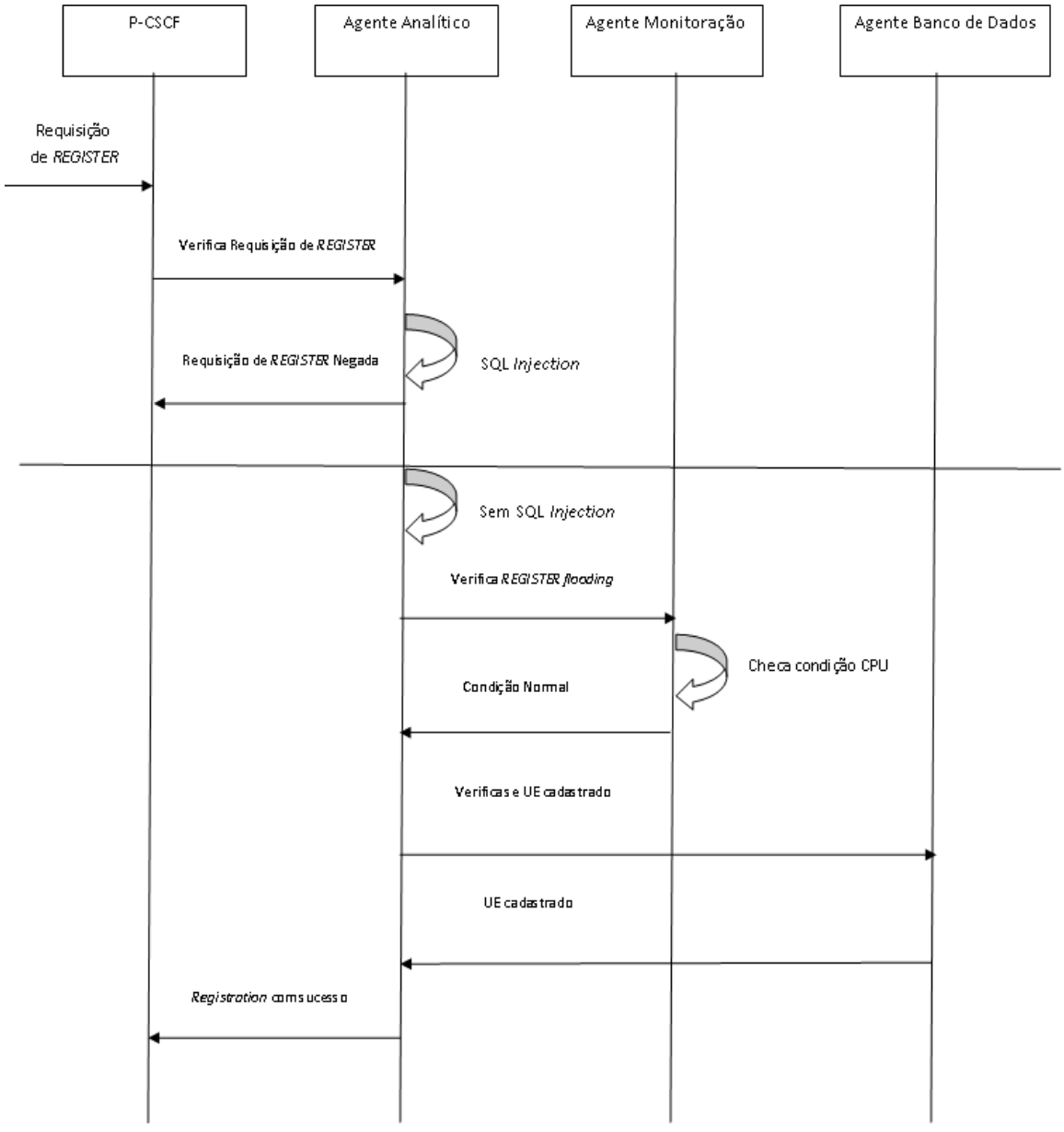

Fig. 6.3 – Especificação de cenário para *REGISTER flooding*.

A requisição de *REGISTER* é enviada do UE para o P-CSCF, que transfere a requisição de *REGISTER* para o agente analítico, que procederá a verificação contra SQL *injection* ataques, se esse tipo de ataque for encontrado a requisição de *REGISTER* será negada.

Caso o agente analítico não encontre ataques de SQL *injection*, logo a requisição será encaminhada para o agente de monitoração, que procederá com a checagem da carga de processamento da CPU.

A carga de processamento da CPU estando sob condições normais de processamento, o agente de monitoração enviará uma resposta indicando o *status* normal.

Nessas condições normais de processamento, o agente analítico encaminhará a requisição de *REGISTER* para o agente banco de dados. Assim, será encaminhada uma resposta de retorno para o UE existente.

• Especificação de cenário para *INVITE flooding*

A requisição de *INVITE* é enviada do UE para o P-CSCF, que encaminha a requisição de *INVITE* para o agente analítico, que procederá a verificação contra SQL *injection* ataques, se esse tipo de ataque for encontrado a requisição de *INVITE* será negada.

Se o agente analítico não encontrou ataques de SQL *injection*, logo a requisição é encaminhada para o agente de monitoração que procederá com a verificação de ataques de inundação de *INVITE* pela checagem das condições e carga de processamento da CPU.

Se as condições de processamento e a carga da CPU estiverem em condições normais, será informado ao agente analítico que encaminhará uma mensagem de pedido de *INVITE* obtido e a requisição entrará no núcleo do IMS.

Porém se a carga de processamento da CPU tiver excedido o limite pré-estabelecido, isso identificará que o sistema está sendo atacado, e o pedido de *INVITE* será rejeitado.

O cenário de simulação para ataques de inundação *INVITE* é especificado pela Fig. 6.4 abaixo:

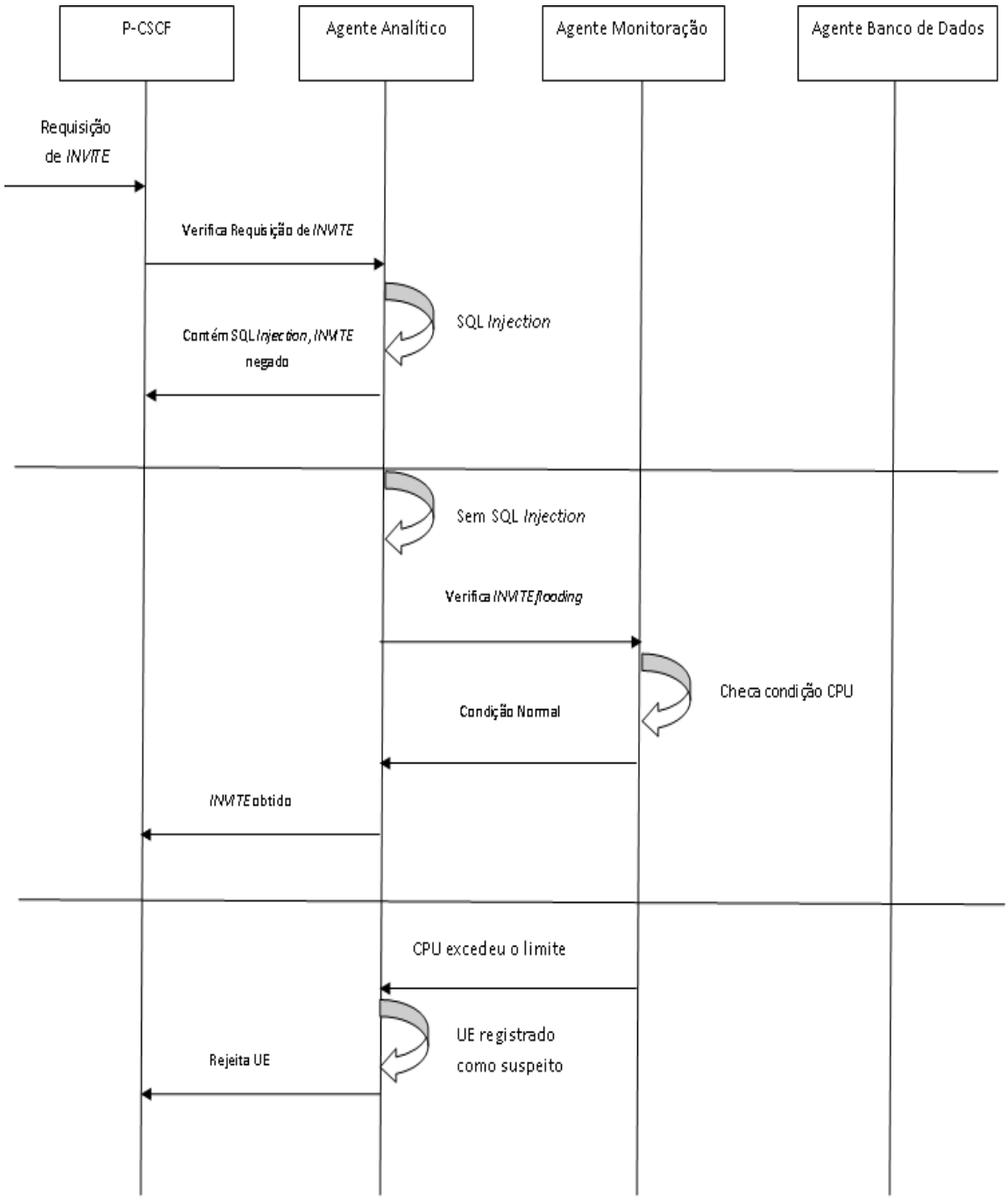

Fig. 6.4 - Especificação de cenário para *INVITE flooding*.

CAPÍTULO 7

CONCLUSÃO

O IMS é uma arquitetura para a entrega de serviços multimídia baseado em IP, a arquitetura da 3GPP integra serviços de rede IP com dispositivos 3G, como telefone celular 3G.

No decorrer do trabalho apresentamos a arquitetura IMS, os motivadores da existência, os benefícios, a história e os protocolos usados na arquitetura, especificamos também detalhadamente todos os componentes da arquitetura.

Tal abordagem foi realizada no intuito de detalhar a estrutura da arquitetura, dessa forma, é possível analisar detalhadamente o mecanismo de segurança da arquitetura. No trabalho também foi especificado com detalhes o protocolo SIP, que é o principal protocolo da arquitetura.

Assim, entramos na arquitetura de segurança do IMS, mostrando com detalhes o mecanismo de segurança proposto pelo 3GPP.

Essa abordagem foi realizada no intuito de provar que o mecanismo de segurança proposta pela 3GPP não é satisfatório, especialmente para proteger a rede IMS de ataques de *flooding*.

Esses ataques derrubam os serviços da rede e esgotam os recursos, os ataques *flood DoS* e *DDoS* é quando um usuário malicioso envia uma quantidade muito grande de mensagens aleatórias para o núcleo da rede IMS de uma única localização (DoS) ou de várias localizações (DDoS).

Na arquitetura de segurança do IMS vimos que o cliente IMS precisa estabelecer associação com o P-CSCF para comunicação, esse é o ponto principal da arquitetura de segurança proposta.

O 3GPP adotou o protocolo AKA (*Authentication and Key Agreement*), como sendo o protocolo de segurança para o processo de autenticação na rede IMS.

Todavia como vimos esse protocolo juntamente com o protocolo de acordo de chaves são vulneráveis a diversos tipos de ataques, fazendo com que a arquitetura fique sujeita a ataques de inundação de mensagens SIP, ataques fuzzing e SQL *injection*, no mecanismo de autenticação.

O projeto de pesquisa prosseguiu realizando uma análise profunda e detalhada nas falhas de segurança da arquitetura IMS, mostrando assim, os principais tipos de ataques que a arquitetura está sujeita.

Realizando uma análise em como esses tipos de ataques e falhas da arquitetura poderiam afetar as operadoras, e os provedores de serviço que utilizam o IMS e também realizou uma análise em como esses tipos de ataques e falhas da arquitetura poderiam afetar os usuários da rede.

Assim, foi feita uma proposta de uma metodologia para eliminar o SPIT no IMS, essa metodologia foi feita baseada na arquitetura lógica de segurança do IMS.

Assim conhecendo a fundo a arquitetura do IMS e o mecanismo de segurança do IMS foi possível criar uma proposta lógica para eliminar o SPIT da arquitetura IMS.

Dessa forma, o projeto de pesquisa partiu para incorporar as idéias de sistema imunológico e arquitetura de multiagentes para a segurança computacional.

Assim, foi proposto um módulo de segurança baseado no sistema imunológico que é capaz de detectar e identificar um ataque, e assim se recuperar e guardar informações sobre o ataque sofrido.

Portanto o módulo proposto deveria ter as mesmas propriedades mencionadas acima, já que simula o sistema imunológico humano.

Foi introduzido também a idéia de agente móveis, que serão responsáveis no módulo proposto pela análise determinística da rede, tomando as devidas ações quando os ataques forem realizados.

Portanto, para proteger o núcleo do IMS dos ataques identificados todas as mensagens de entrada e saída passaram pelo módulo proposto.

Reconhece-se, entretanto que apesar de todos os esforços e análise de segurança apresentados nesse trabalho e em diversos trabalhos que estão por vir, a questão de segurança é um ponto que sempre causará preocupação e demandará esforços de empresas e provedores de serviços.

Porque idependente de quanto uma solução de segurança seja testada, estressada e tenha requisitos e implementações de segurança forte e complexo, sempre haverá a possibilidade de usuários maliciosos passarem e eliminarem essas implementações de segurança.

Porque na mesma medida que empresas e pesquisadores ao redor do mundo trabalham em soluções de segurança, *hackers* e usuários maliciosos também trabalham igualmente para coromperem e eliminarem tais requisitos, principalmente quando fatores econômicos estejam envolvidos, como roubo e venda de informações confidenciais, sejam comerciais ou de usuários.

Sendo assim, o trabalho de segurança e proteção de informações é um trabalho árduo e contínuo que sempre estará sujeito a novo e sofisticados tipos de ataques e ameaças.

O que abre uma brecha para que futuros trabalhos como esse possam ser realizados trazendo novas informações e acrescentando mais um capítulo na história da segurança das redes.

Assim, a arquitetura IMS apesar de promissora apresenta inúmeras questões de segurança que precisam ser bem endereçadas e trabalhadas no intuito de desenvolver uma implementação para o uso seguro do IMS.

Viabilizando dessa forma a adoção e do desenvolvimento dessa arquitetura em escala global.

7.1. Sugestão para Trabalhos Futuros

Como já mencionado assim como evoluem os requisitos e as implementações de segurança das redes, assim também evoluem os tipos de ataques e as ameaças que as redes estão sujeitas.

Com a evolução das redes para LTE o IMS deve ganhar importância e ser implementado e adotado em um número maior de redes e operadoras.

Com essa maior exposições da arquitetura em um ambiente de produção existiram mais dados e relatos sobre tipos de ataques e ameaças que a arquitetura pode vir a sofrer.

Sendo assim uma sugestão de trabalho futuro seria realizar uma análise detalhada sobre relatos de operadoras, provedores de serviço e usuários da rede IMS.

Extraindo depoimentos e informações sobre tipos de ataques, realizando assim uma análise de como esses ataques prejudicaram tanto operadoras quanto usuários da rede.

E assim propor novas soluções de segurança seja para falhas e ataques específicos que a arquitetura possa estar susceptível ou até mesmo criar propostas para um novo módulo de segurança que seja mais moderna e possa eliminar esses futuros ataques e falhas que a arquitetura possa vir a sofrer.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] 3GPP. IP Multimedia Subsystem (IMS). Technical Specification (TS 23.228 version 10.6.0 Release 10), October 2011.

[2] Ericsson's whitepaper, "IMS: IP Multimedia Subsystem" outlines how IMS enables a secure service-driven approach to moving all traffic to the packet switched domain and Session Initiation Protocol (SIP) logic, October 2004.

[3] 3G America's whitepaper, "IP Multimedia Subsystem IMS Overview and Applications" outlines the benefits and multiple applications of IMS, July 2004.

[4] 3GPP. Security architecture. Technical Specification (TS 33.102 version 10.0.0 Release 10), May 2011.

[5] 3GPP. Access security for IP-based services. Technical Specification (TS 33.203 version 10.2.0 Release 10), May 2011.

[6] 3GPP. Security aspects of early IP multimedia subsystem (IMS). Technical Report (TR 33.978 version 7.0.0 Release 7), June 2007.

[7] Bob Bellman. Exploring IMS security mechanisms. Business Communications Review, January 2006.

[8] ITU-T Recommendation Y.2001: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks. Genebra, 2004.

[9] D. Endler and M. Collier. Hacking Exposed VoIP: Voice over IP Security Secrets and Solutions. McGraw-Hill, 2007.

[10] D. Kuhn, T. Walsh, and S. Fries. Security considerations for voice over IP systems. Technical Report 800-58, January 2005.

[11] Alberti, A. Redes Convergentes Unidade VI Arquiteturas de Redes de Próxima Geração. Instituto Nacional de Telecomunicações, 2006.

[12] J. Rosenberg. RFC 3856: A Presence Event Package for the Session Initiation Protocol (SIP), August 2004.

[13] Magedanz, T. Overview of the IP Multimedia System (IMS) Principles, Architecture and Applications. Berlin, 2006.

[14] Camarillo, Gonzalo. The 3G IP multimedia subsystem (IMS): merging the internet and the cellular worlds / Gonzalo Camarillo, Miguel A. Garcia-Martin.-2nd ed. John Wiley & Sons, Ltd, 2006.

[15] 3GPP. Quality of Service (QoS) - Concept and Architecture. Technical Specification (TS 23.107 version 10.1.0 Release 10), June 2011.

[16] 3GPP. Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS). Technical Specification (TS 22.228 version 10.4.1 Release 10), April 2011.

[17] 3GPP. Network architecture. Technical Specification (TS 23.002 version 10.3.0 Release 10), October 2011.

[18] Muhammad Sher, Thomas Magedanz, “Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks”, IEEE computer society, 2007.

[19] M. Sher, S. Wu, T. Magedanz, “Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS)”, IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation.

[20] Hayzelden and Bigham, “Agents for Future Communication Systems”, Springer; 1 edition, June 11, 1999.

[21] A. Niemi, J. Arkko, V. Torvinen, "HTTP Digest Authentication Using AKA", IETF RFC 3310 , 2002.

[22] A.somayali, S.Hofmeyr. and S.forrest, Principles of computer immune system . In proceedings of second new security paradigms workshop, 1997.

[23] R.L.King, A.B. Lambert, S.H Russ, and D.S Reese, “The biological basis of the immune system as amodel for intelligent agents”. Second workshop on Bio-Inspired Solutions to parallel Processing Problems., 1999.

[24] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, “Self-nonself discrimination in a computer”, In Proceedings of the IEEE Symposium on Research in Security and Privacy, Los Alamos, 1994.

[25] J. O. Kephart, R. A. Brooks and P. Maes “A biologically inspired immune system for computers”, Proceedings of the Fourth International Workshop on the Synthesis and Simulation of Living Systems, Cambridge, MA, 1994.

[26] Leandro N. de Castro and Jonathan Timmis, “Artificial Immune Systems: A New Computational Intelligence Approach”, Springer, 2002.

[27] S. Forrest, S. Hofmeyr, and A. Somayaji, “Computer immunology.” Communications of the ACM, Dec. 1996.

[28] AvTravis Russell, “The IP Multimedia Subsystem (IMS): Session Control and Other Network Operations”, McGraw-Hill Professional.

[29] Henning Schulzrinne, Jonathan Rosenberg, “The Session Initiation protocol: Internet-centric signaling”, IEEE Communications magazine, 0ct 2000.

[30] Muxiang Zhang; Yuguang Fang; “Security analysis and enhancements of 3GPP authentication and key agreement protocol”, Volume 4, IEEE Communications magazine, March 2005.

[31] Yauhui Lei, Samuel Pierre and Alejandro Quintero,”Enhancing UMTS Authentication and Key Agreement with Vector Combination”, UbiCC Journal, Volume 3April 2008.

[32] D. Sisalem et Al, “Denial of Service Attacks Targeting a SIP VoIP Infrastructure”, to appear in IEEE Networks Magazine: Securing Voice over IP.

[33] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambbrinoudakis, S. Gritizalis, S. Ehlert, D. Sisalem, “Survey of Security Vulnerabilities in SIP Protocol”, IEEE Communication Surveys Volume 8, No.3 ISBN 1553-877X, 2006.

[34] M. Poikselkae, G. Mayer, H. Khartabil, A. Niemi, “The IMS, IPMultimedia Concepts and Services in the Mobile Domain”, 2nd Edition, John Willey & Sons Ltd, West Sussex, England, 2006.

[35] Dimitris geneiatakis, Tasos dagiuklas, Georgios kambourakis, Costas lambrinoudakis, and Stefanos gritzalis, “Survey of SecurityVulnerabilities in Session Initiation Protocol”, IEEE Communications Surveys & Tutorials, 2006.

[36] Sipera Systems,”Protecting IMS networks from attack”, February 2007 http://www.sipera.com.

[37] Erik E.Anderland, David W.Faucher, Eric H.Grosse, Daniel N. Heer, Andrew R. McGee, David P.Strand, and Robert Thornberry Jr, “IMS Security” , Wiley, 2006.

[38] 3GPP vision, Ashok chatterjee, Eriksson INC. chairman, 3GPP project coordination group, ITU seminar, Ottawa, May 2002, http://www.itu.int/osg/imtproject/docs/2.2_Chatterjee.pdf.

[39] S. Forrest, S. Hofmeyr, A. Somayaji, and T. Longstaff, “A sense of self for UNIX processes”, In Proceedings of the IEEE Symposium on Computer Security and Privacy, IEEE Press, 1996.

[40] M. Handley and V. Jacobson. SDP: Session Description Protocol. RFC 2327, Internet Engineering Task Force, April 1998.

[41] R. Chen, E. Su, V. Shen, Y. Wang, Introduction to IP Multimedia Subsystem (IMS), Part 1: SOA Parlay X Web services, Sep. 2006.

[42] J. Rosenberg and H. Schulzrinne. An Offer/Answer Model with Session Description Protocol (SDP). RFC 3264, Internet Engineering Task Force, June 2002.

[43] Third Generation Partnership Project, (2012), www.3gpp.org

[44] 3GPP Specifications, (2012), www.3gpp.org/specs/specs.htm

[45] 3GPP IMS, (2012), www.3gpp.org/article/ims

[46] www.teleco.com.br, Vinicius Barreiro Funicelli

[47] Fixed Mobile Convergence Alliance – Product Requirement Definitions, Release 2.0. 2006.

PUBLICAÇÕES

NOBÔA, FRANCISCO; IANO, YUZO. Visão Geral sobre as Falhas de Segurança da Arquitetura IMS. Revista Ciência e Tecnologia, Vol. 13, No 22/23 (2010).

NOBÔA, FRANCISCO; IANO, YUZO. Analysis on the Security Mechanism of the IMS Architecture. Subjected to: 37th Annual IEEE Conference on Local Computer Networks, 2012, Clearwater, Florida, USA.

NORMAS 3GPP

Lista de normas 3GPP que mencionam ou estão relacionadas com o IMS:

[TR 21.905] Vocabulary for 3GPP Specifications
[TS 22.066] Support of Mobile Number Portability (MNP); Stage 1
[TS 22.101] Service Aspects; Service Principles
[TS 22.141] Presence Service; Stage 1
[TS 22.228] Service requirements for the IP multimedia core network subsystem; Stage 1
[TS 22.250] IMS Group Management; Stage 1
[TS 22.340] IMS Messaging; Stage 1
[TR 22.800] IMS Subscription and access scenarios
[TS 23.002] Network Architecture
[TS 23.003] Numbering, Addressing and Identification
[TS 23.008] Organization of Subscriber Data
[TS 23.107] Quality of Service (QoS) principles
[TS 23.125] Overall high level functionality and architecture impacts of flow based charging; Stage 2
[TS 23.141] Presence Service; Architecture and functional description; Stage 2
[TS 23.167] IMS emergency sessions
[TS 23.207] End-to-end QoS concept and architecture
[TS 23.218] IMS session handling; IM call model; Stage 2
[TS 23.221] Architectural Requirements
[TS 23.228] IP Multimedia Subsystem (IMS); stage 2
[TS 23.234] WLAN interworking
[TS 23.271] Location Services (LCS); Functional description; Stage 2
[TS 23.278] Customized Applications for Mobile network Enhanced Logic (CAMEL) - IMS interworking; Stage 2
[TR 23.864] Commonality and interoperability between IMS core networks
[TR 23.867] IMS emergency sessions
[TR 23.917] Dynamic policy control enhancements for end-to-end QoS, Feasibility study
[TR 23.979] 3GPP enablers for Push-to-Talk over Cellular (PoC) services; Stage 2
[TR 23.981] Interworking aspects and migration scenarios for IPv4-based IMS implementations (early IMS)

[TS 24.141] Presence Service using the IMS Core Network subsystem; Stage 3

[TS 24.147] Conferencing using the IMS Core Network subsystem

[TS 24.228] Signalling flows for the IMS call control based on SIP and SDP; Stage 3

[TS 24.229] IMS call control protocol based on SIP and SDP; Stage 3

[TS 24.247] Messaging using the IMS Core Network subsystem; Stage 3

[TS 26.235] Packet switched conversational multimedia applications; Default codecs

[TS 29.207] Policy control over Go interface

[TS 29.208] End-to-end QoS signalling flows

[TS 29.209] Policy control over Gq interface

[TS 29.228] IMS Cx and Dx interfaces: signalling flows and message contents

[TS 29.229] IMS Cx and Dx interfaces based on the Diameter protocol; Protocol details

[TS 29.278] CAMEL Application Part (CAP) specification for IMS

[TS 29.328] IMS Sh interface: signalling flows and message content

[TS 29.329] IMS Sh interface based on the Diameter protocol; Protocol details

[TR 29.962] Signalling interworking between the 3GPP SIP profile and non-3GPP SIP usage

[TS 31.103] Characteristics of the IMS Identity Module (ISIM) application

[TS 32.240] Telecommunication management; Charging management; Charging architecture and Principles

[TS 32.260] Telecommunication management; Charging management; IMS charging

[TS 32.299] Telecommunication management; Charging management; Diameter charging applications

[TS 32.421] Telecommunication management; Subscriber and equipment trace: Trace concepts and requirements

[TS 33.102] 3G security; Security architecture

[TS 33.108] 3G security; Handover interface for Lawful Interception (LI)

[TS 33.141] Presence service; security

[TS 33.203] 3G security; Access security for IP-based services

[TS 33.210] 3G security; Network Domain Security (NDS); IP network layer security

[TR 33.978] Security aspects of early IP Multimedia Subsystem (IMS)

NORMAS IETF

Lista de normas IETF que mencionam ou estão relacionadas com o IMS:

[RFC 2327] Session Description Protocol (SDP)

[RFC 2748] Common Open Policy Server protocol (COPS)

[RFC 2782] A DNS RR for specifying the location of services (SRV)

[RFC 2806] URLs for telephone calls (TEL)

[RFC 2915] The naming authority pointer DNS resource record (NAPTR)

[RFC 2916] E.164 number and DNS

[RFC 3087] Control of Service Context using SIP Request-URI

[RFC 3261] Session Initiation Protocol (SIP)

[RFC 3262] Reliability of provisional responses (PRACK)

[RFC 3263] Locating SIP servers

[RFC 3264] An offer/answer model with the Session Description Protocol

[RFC 3265] SIP-Specific Event Notification

[RFC 3310] HTTP Digest Authentication using Authentication and Key Agreement (AKA)

[RFC 3311] Update method

[RFC 3312] Integration of resource management and SIP

[RFC 3319] DHCPv6 options for SIP servers

[RFC 3320] Signalling compression (SigComp)

[RFC 3323] A privacy mechanism for SIP

[RFC 3324] Short term requirements for network asserted identity

[RFC 3325] Private extensions to SIP for asserted identity within trusted networks

[RFC 3326] The reason header field

[RFC 3327] Extension header field for registering non-adjacent contacts (path header)

[RFC 3329] Security mechanism agreement

[RFC 3420] Internet Media Type message/sipfrag

[RFC 3428] SIP Extension for Instant Messaging

[RFC 3455] Private header extensions to SIP for 3GPP

[RFC 3485] SIP and SDP static dictionary for signaling compression

[RFC 3515] The SIP REFER method

[RFC 3550] Real-time Transport Protocol (RTP)

[RFC 3574] Transition Scenarios for 3GPP Networks

[RFC 3588] Diameter base protocol

[RFC 3589] Diameter command codes for 3GPP release 5 (informational)

[RFC 3608] Extension header field for service route discovery during registration

[RFC 3665] SIP Basic Call Flow Examples

[RFC 3680] SIP event package for registrations

[RFC 3725] Best current practices for Third Party Call Control (3pcc) in SIP

[RFC 3824] Using E164 numbers with SIP

[RFC 3840] Indicating user Agent Capabilities in SIP

[RFC 3841] Caller preferences for SIP

[RFC 3842] SIP event package for message waiting indication and summary

[RFC 3856] SIP event package for presence

[RFC 3857] SIP event template-package for watcher info

[RFC 3858] XML based format for watcher information

[RFC 3891] The SIP Replaces Header

[RFC 3903] SIP Extension for Event State Publication

[RFC 3911] The SIP Join Header

[RFC 4028] Session timers in SIP

[RFC 4235] An INVITE-Initiated dialog event package for SIP

[RFC 4475] Session Initiation Protocol (SIP) Torture Test Messages