UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

SEGURANÇA EM SISTEMAS DE COMUNICAÇÃO PESSOAL

Um modelo de arquitetura
de protocolos para a interconexão
de sistemas heterogêneos

por

HERBERT LUNA GALIANO

Dissertação submetida à avaliação, como requisito parcial
para a obtenção do grau de
Mestre em Ciência da Computação

Prof. Juergen Rochol
Orientador

Porto Alegre, agosto de 1997

CIP - CATALOGAÇÃO NA PUBLICAÇÃO

Luna Galiano, Herbert

Segurança em Sistemas de Comunicação Pessoal - Um modelo de arquitetura de protocolos para a interconexão de sistemas heterogêneos / por Herbert Luna Galiano. - Porto Alegre : CPGCC da UFRGS,1997.

75 f. :il.

Dissertação (mestrado) - Universidade Federal do Rio Grande do Sul. Curso de Pós-Graduação em Ciência da Computação, Porto Alegre, BR-RS, 1997. Orientador : Rochol, Juergen.

1. Segurança em Sistemas de Comunicação Pessoal. 2. Sinalização em Sistemas de Comunicação Pessoal. 3. Sistemas de Telefonia Celular. 4. Sistemas de Comunicação sem fio. I. Rochol, Juergen. II. Título.

MOD. 2.

Agradecimentos

A mis Padres, por su amor y sacrificio para lograr conseguir la superación de cada unos de sus hijos, a ellos mis más sinceros agradecimientos.

A mis hermanas, por el inmenso apoyo que me proporcionaron, aquí en el Brasil, en especial a Elfi, por su generosa ayuda, en los momentos mas críticos que me toco vivir .

Al CPGCC de la UFRGS por brindarme la oportunidad de realizar mi maestría, en especial a sus profesores y funcionarios por la excelente calidad de trabajo y dedicación puesta, no haciendo envidiar en nada a los cursos de post-grado en los paises de primer mundo.

A mi Orientador y Profesor Juergen Rochol, por su constante disponibilidad a responder todas mis inquietudes acádemicas, así como su incentivo y estímulo para concluir mi maestría.

Al Conselho Nacional de Pesquisa CNPq, por el auxilio financiero concedido durante toda la maestría.

Finalmente, a Flor de Qantu, mi esposa, por su comprensión, paciencia, y cariño dedicado durante el tiempo que demandó mi maestría. También a ella las gracias por su esfuerzo y sacrificio, luchando para estar a mi lado junto con nuestro pequeño hijo Sebastian, el mismo que ahora se convierte en nuestra fuente de estímulo y superación.

Sumário

Lista de Abreviaturas 7

Lista de Figuras 11

Lista de Tabelas 12

Resumo 13

Abstract 14

1 Introdução 15

2 Segurança em Redes de Comunicação de Dados 17

2.1 Sistemas de Criptografia 17

2.1.1 Criptografia de chave secreta 18

2.1.2 Criptografia de chave pública 20

2.1.3 Sistema de criptografia híbrida 21

2.1.4 Segurança dos sistemas de criptografia 21

2.2 Autenticação 22

2.3 Segurança em Sistemas de Comunicação Sem Fio 24

3 Evolução dos Sistemas de Comunicação Sem Fio 25

3.1 Conceitos de Telefonia Celular 25

3.2 A Primeira Geração dos Sistemas de Comunicação Sem Fio 29

3.2.1 Telefonia celular analógica. 30

3.2.2 Sistemas de telefonia celular analógico AMPS 30

3.3 A Segunda Geração dos Sistemas de Comunicação Sem Fio 32

3.3.1 Sistemas de telefonia celular digital americano USCD 32

3.3.2 Sistema de telefonia celular digital européio GSM 34

3.4 Análise comparativa dos Sistemas de Telefonia Celular AMPS, USCD e GSM 35

3.5 A Terceira Geracão dos Sistemas de Comunicação Sem Fio 36

3.5.1 Sistemas UMTS 36

3.5.2 Sistemas FPLMTS 37

3.5.3 Sistemas PCS 37

4 Estudo Comparativo dos Aspectos de Segurança em Redes de Telefonia Celular 40

4.1 Segurança no Sistema de Telefonia Celular AMPS 40

4.1.1 Autenticação no AMPS 40

4.1.2 Privacidade no AMPS 42

4.1.3 Fraudes em sistemas AMPS 42

4.2 Segurança em Sistemas de Telefonia Celular Digital USCD 43

4.2.1 Autenticação em sistemas USCD 43

4.2.2 Privacidade em sistemas USCD 44

4.3 Segurança em Sistemas de Telefonia Celular Digital GSM 45

4.3.1 O processo de autenticação no GSM 45

4.3.2 O processo de confidencialidade dos dados no GSM 46

4.3.3 Confidencialidade da identidade e localização do assinante no GSM 47

4.4 Análise Comparativa entre os Sistemas AMPS, USCD e GSM, quanto aos aspectos de segurança 48

5 Segurança em Sistemas PCS 50

5.1 Características de Autenticação e Privacidade desejadas em Sistemas PCS 50

5.2 Requisitos dos Mecanismos de Criptografia para Sistemas PCS 51

5.3 Modelo AKA para Autenticação e Privacidade em Sistemas PCS 52

5.4 Padronização dos aspectos Segurança em Sistemas PCS 53

6 A Interconexão com Redes PCS 54

6.1 Segurança na interconexão de redes heterogêneas com Sistemas PCS 55

7 Protocolos de Sinalização 56

7.1 O Modelo RM-OSI 56

7.2 Sistemas de Sinalização Número 7 58

7.2.1 Protocolos da rede SS7 60

7.2.2 O subsistema de serviço de rede NSP 61

7.2.3 O nível 4 do protocolo SS7 61

8 Sinalização em Telefonia Celular e PCS 63

8.1 Sinalização IS-41 MAP em redes de telefonia celular 64

8.2 Sinalização em redes GSM 65

8.3 Sinalização em redes PCS 66

8.4 Os Planos de Sinalização e Transporte para Redes de Telefonia Celular 66

8.5 Uma Arquitetura de Protocolos de Sinalização para a Interconexão de Redes Heterogêneas com Sistemas PCS 68

9 Conclusões 70

Bibliografia 72

Lista de Abreviaturas

AMPS	*Advanced Mobile Phone Service*
AIN	*Advanced Intelligent Networks*
AKA	*Authentication Key Agreement*
ANSI	*American Nationa Standard Institute*
ASE	*Application Service Element*
ATIS	*Alliance for Telecommunications Industry Solutions*
AUC	*Authentication Center*
A&P	*Autenticação e Privacidade*
BPSK	*Binary Phase Shift Keying*
BS	*Base Station*
BSC	*Base Station Controller*
BSS	*Base Station Subsystem*
BTS	*Base Transciver Station*
CCC	*Centro de Controle e Comutação*
CDMA	*Code Division Multiple Acces*
CEPT	*Conférence Européenne des Postes et Telécommunications*
CM	*Connection Management*
DECT	*Digital European Cordless Telefone*
DES	*Data Encryption Standard*
DQPSK	*Differential Quadrature Phase Shift*
EIA	*Electronic Industries Association*
EIR	*Equipment Identity Register*
ERB	*Estação Rádio Base*
ESN	*Electronic Serial Number*
ETSI	*European Telecommunications Standards Institute*
FCC	*Federal Communications Commission*
FDMA	*Frequency Division Multiple Access*
FM	*Frequency Modulation*
FPLMTS	*Future Public Land Mobile Telecommunications Systems*
FSK	*Frequency Shift Keying*

GSM	*Global Systems for Mobile Communications*
HLR	*Home Location Register*
IEEE	*Institute of Electrical and Electronic Engeneering*
IDEA	*International Data Encryption Algorithm*
IIF	*Interworking Interoperability Function*
IMSI	*International Mobile Subscriber Identity*
IMT-2000	*International Mobile Telecommunications-2000*
IN	*Intelligent Network*
IS	*Interim Standars*
ISDN	*Integrated Services Digital network*
ISO	*International Standards Organization*
ISUP	*ISDN User Part*
ITU	*International Telecommunications Union*
IWF	*Interworking Function*
JTC	*Join Technical Committee*
LAI	*Location Area Identity*
LEC	*Local Exchange Carrier*
LMR	*Land Mobile Radio*
MAP	*Mobile Application Part*
MCS	*Mobile Communication System*
MF	*Multi - Frequency*
MFR	*Manufacturer Code*
MIN	*Mobile Identification Number*
MIT	*Massachusetts Institute of Technology*
MM	*Mobilty Management*
MS	*Mobile Station*
MSC	*Mobile Switching Center*
MSS	*Mobile Satellite Services*
MTP	*Message Transfer Part*
NMT	*Nordic Mobile Telephone*
NSA	*National Segurity Agency*
NSS	*Network Subsystem*

NTT	*Nippon Telephone and Telegraph*
OSI	*Open Systems Interconnection*
OMAP	*Operation Maintenance and Administration Part*
PACS	*Personal Access Communications Services*
PBX	*Private Branch Exchange*
PCS	*Personal Communications Systems ou Services*
PIN	*Personal Identification Number*
PKC	*Public Key Cryptography*
PS	*Ponto de Sinalização*
PSTN	*Public Swithed Telephone Network*
QPSK	*Quadrature phase-shift keying*
RAND	*Random Number*
RDSI	*Rede Digital de Serviços Integrados*
RF	*Radio Frequency*
RM-OSI	*Reference Model - Open Systems Interconection*
RR	*Radio Resurces*
RSA	*Rivest, Shamir e Adleman Algorithm*
RX	*Receive ou Reception*
SCM	*Station Class Mark*
SCP	*Service Control Point*
SCCP	*Signaling Connection Control Part*
SDL	*Specification and Description Language*
SDT	*SDL Desing Tool*
SID	*Systems Identification*
SIM	*Subscriber Identity Module*
SMS	*Service Managment System*
SPC	*Signaling Point Code*
SRES	*Signed Response*
SS	*Spread Spectrum*
SSD	*Shared Secret Data*
SSP	*Service Switching Point*
SS7	*Signaling System Number 7*

STP	*Signaling Transfer Point*
TACS	*Total Access Communications Systems*
TAG	*Technical Ad-hoc Gropus*
TCAP	*Transaction Capabilities Application Part*
TDM	*Time Division Multiplexing*
TDMA	*Time Division Multiple Acess*
TIA	*Telecommunications Industry Association*
TMSI	*Temporal Mobile Subscriber Identity*
TUP	*Telephone User Part*
USCD	*United States Cellular Digital*
TX	*Transmit ou Trasmission*
UMTS	*Universal Mobile Telecommunications Systems*
UPT	*Universal Personal Telecommunications*
VLR	*Visited Location Register*
WARC	*World Administrative Radio Conference*
WLAN	*Wireless Local Area Network*

Lista de Figuras

FIGURA 2.1- Sistema de Criptografia..... 18
FIGURA 3.1- Evolução dos Sistemas de Comunicação Sem Fio..... 25
FIGURA 3.2 - Arquitetura e elementos da Rede AMPS..... 31
FIGURA 3.3 - Arquitetura da Rede USCD com a sinalização do IS-41..... 33
FIGURA 3.4 - Arquitetura da Rede GSM..... 35
FIGURA 4.1- Estrutura do MIN - *Mobile Identification Number*..... 40
FIGURA 4.2 - Estrutura do ESN - *Electronic Serial Number*.....41
FIGURA 4.3 - Processo de *Cloning* em Sistemas AMPS 42
FIGURA 4.4 - Processo de Autenticação em Sistemas USCD..... 43
FIGURA 4.5 - Estrutura do SSD - *Shared Secret Data*..... 44
FIGURA 4.6 - Distribuição dos parâmetros de segurança na rede GSM 45
FIGURA 4.7 - Processo de Autenticação no GSM 46
FIGURA 4.8 - Processo do cálculo da chave Kc no GSM..... 47
FIGURA 4.9 - Início do modo de comunicação cifrada no GSM 47
FIGURA 5.1 - Os três processos do modelo AKA 53
FIGURA 6.1 - Interconexão de redes heterogêneas com Sistemas PCS 54
FIGURA 7.1 - Modelo de Referência ISO..... 57
FIGURA 7.2 - O SS7 e sua relação com as camadas do modelo OSI. 61
FIGURA 8.1 - O MAP no SS7 63
FIGURA 8.2 - Sinalização IS-41 MAP entre duas centrais 64
FIGURA 8.3 - Arquitetura de Protocolos do GSM-MAP..... 65
FIGURA 8.4 - Arquitetura de protocolos para o plano de sinalização numa rede de telefonia celular 67
FIGURA 8.5 - Arquitetura de protocolos para uma rede de telefonia celular mostrando o plano de transporte 67
FIGURA 8.6 - Interconexão de redes PCS usando a interface IIF 68
FIGURA 8.7 - Arquitetura de protocolos de sinalização representando a interconexão de uma rede PCS com uma rede de telefonia celular 69
FIGURA 9.1 - Processo de Simulação da Interface IIF usando SDL 71

Lista de Tabelas

TABELA 2.1 - Tempo que levaria para quebrar um algoritmo de *n* bits através ataque da força bruta 21

TABELA 2.2 - Número de máquinas requeridas para quebrar um algoritmo de *n* bits através ataque da força bruta.....22

TABELA 3.1 - Panorama Mundial da Telefonia Celular Analógica 30

TABELA 3.2 - Quadro Comparativo entre os sistemas AMPS, USCD e GSM....36

TABELA 3.3 - Propostas em estudo para padrões de Sistemas PCS 38

TABELA 4.1 - Comparação dos aspectos de segurança em sistemas de telefonia celular..... 49

TABELA 5.1 - Padrões de segurança propostos para Sistemas PCS pelo JTC 53

TABELA 6.1- Analise comparativa da segurança na interconexão de redes PCS com redes heterogêneas 55

Resumo

A evolução dos sistemas de comunicação sem fio ou *wireless* apresentam até agora três gerações em menos de duas décadas. Fazendo parte desta evolução estão os sistemas de telefonia celular e os emergentes Sistemas de Comunicação Pessoal ou PCS (*Personal Communications Systems*). Este trabalho visa apresentar duas questões importantes na evolução destes sistemas, primeiro a questão da segurança e segundo a questão da interconexão com redes heterogêneas.

No trabalho, abordando a questão de segurança, são estudados, analisados e comparados os mecanismos de autenticação e privacidade implementados nos atuais padrões de telefonia celular digital e analógico, como sistemas AMPS (celular analógico americano), USCD (celular digital americano) e GSM (celular digital europeu). São identificadas a vulnerabilidade e os fraudes mais comuns nestes sistemas. Também são analisados as propostas das recentes pesquisas e o *state of art* em termos de segurança, para os sistemas PCS emergentes. Como conclusão é apresentado um quadro comparativo resumindo as principais caraterísticas de segurança adotados pelos sistemas abordados neste estudo.

Uma vez apresentado os aspectos de segurança em forma isolada para cada um dos sistemas acima mencionados, é apresentado a questão segurança no contexto da interconexão com redes heterogêneas. A interconexão com redes heterogêneas é outro problema a ser resolvido na implementação da terceira geração de sistemas *wireless*, para fornecer o *roaming* automático e a mobilidade pessoal e de terminal. Neste trabalho são revisados os protocolos de sinalização SS7 (*Signaling System Number 7*) e MAP (*Mobile Application Part*), como requisitos importantes na solução da interconexão e interoperabilidade entre as redes fixas atuais com as futuras redes móveis. Como conclusão deste estudo é apresentado a proposta de uma arquitetura de protocolos de sinalização, representando a interconexão de um sistema PCS baseado no padrão J-STD-007, com a rede de telefonia celular IS-95. Esta interconexão é realizada através de uma interface de rede denominada IIF (*Interworking and Interoperability Function*) usando protocolos de sinalização por canal comum SS7 e MAP.

Finalmente são apresentados as conclusões quanto aos objetivos alcançados, e é proposto um trabalho futuro, tomando como base o desenvolvido neste trabalho.

Palavras-Chave : Segurança em Sistemas de Comunicação Pessoal, Sinalização em Sistemas de Comunicação Pessoal, Sistemas de Telefonia Celular, Sistemas de comunicação sem fio.

Title : Security in Personal Communications Systems. One model of protocol architecture for the interworking of heterogeneous systems.

Abstract

The evolution of wireless communications systems has developed into the third generation which is mainly represented by the Telephone Cellular Systems and PCS (Personal Communication systems). This work presents an overview about two importante issues in the evolution of the Wireless Communication Systems: Security and Interworking.

Initially we carry out our study on the wireless communication security issue by analyzing and comparing some major authentication features and privacy characteristics implemented in the currently standardized cellular phone systems such as AMPS (American Analog Cellular), USCD (American Digital Cellular) and GSM (Euroupean Digital Cellular). For this end, we tentatively determine how vulnerable to the fraudulent attacks these systems are and what are those frauds commonly occurring in these systems. Also we analyze the state of art and some proposals for security problems in PCS systems found in the literature. We conclude our preliminary study with a table summarizing some principal systems´ characteristics in the security issue.

Next, we extend our discussion to the case of heterogeneous networks. In fact, the interconnection of heterogeneous networks is another important issue that needs to be deeply investigated in order to develop a rebust third generation of wireless communication systems, special those capable of providing automatic "roaming" and personal as well as terminal mobility. In this work we particularly discuss the protocols employed in the signaling system SS7 (Signaling Systems Number 7) and MAP (Mobile Application Part) which are important issues in terms of the interworking and interoperability of wireless and wireline networks. As a conclusion of this discussion, we propose a protocol architecture based on the RM-OSI model relating to the interconnection of a PCS system, J-STD-007, with the IS-95 cellular phone networks. Note that the proposed model uses the signaling systems SS7 and MAP.

Finally we present some importante conclusion with respect to the objetives achieved in this work, and propose some future research activities based on this work.

Keywords: Security in Personal Communications Systems, Signaling in Personal Communications Systems, Cellular Systems, Wireless Communications.

1 Introdução

Atualmente, está acontecendo uma explosiva evolução nos sistemas de comunicação sem fio ou w*ireless*. Dos antigos sistemas de telefonia celular analógicos, estamos passando para novos conceitos de comunicações pessoais, móveis e universais. Os sistemas *wireless* é um dos segmentos que apresentou o maior crescimento nestes últimos anos, com taxas de crescimento que são surpreendentes para a área das Telecomunicações. Na América Latina, por exemplo, com o término do monopólio estatal e a abertura do setor aos investimentos privados, o crescimento da telefonia celular e dos sistemas *paging* estão alcançando taxas de expansão próximo de 100% ao ano [LUX95]. O número total de telefones celulares no mundo está estimado em torno de 110 milhões [SIQ96], número maior que o número de pessoas ligadas, atualmente, à *Internet*.

É certo também, que são cada vez mais exigentes os requisitos de segurança em comunicação de dados, em vista da globalização das comunicações e dos serviços suportados. Infelizmente, pela sua estrutura e pela utilização de canais de comunicação compartilhados, os sistemas *wireless* tornam-se muito mais vulneráveis a ataques. Por exemplo, as fraudes de autenticação (mais conhecido como *cloning*) em sistemas de telefonia celular representam a cada ano um prejuízo cada vez maior para as operadoras. Só nos EUA foi contabilizado em 1995, com fraudes de autenticação, um prejuízo que ultrapassou US$2 bilhões. No Brasil, em quatro meses, de junho a setembro de 1996, a operadora de São Paulo, TELESP, acusou um prejuízo de R$1.6 milhões no seu faturamento devido a fraudes de autenticação [LOB96].

Problemas de segurança em sistemas de telefonia celular não são somente relacionados a autenticação, também existem os relacionados a privacidade e sigilo da localização do usuário. Por exemplo, são conhecidos os casos de escuta clandestina de celulares comprometendo a personalidades da política, do esporte etc. Também são conhecidos os casos da captura do popular *hacker* Kevin Minick e da morte do líder separatista chechênio Dudayev, acontecidos pela frágil segurança relativa a localização do celular [MAR95].

Problemas da segurança em sistemas *wireless* acontecem freqüentemente e, a menos que sejam tomadas medidas específicas para prevení-los, os prejuízos poderão tornar-se cada vez maiores. Este trabalho visa estudar a questão da segurança em sistemas *wireless*, representados principalmente pelos sistemas de telefonia celular e os sistemas PCS emergentes. Uma vez apresentado os aspectos de segurança em forma isolada para cada um dos sistemas acima mencionados, é apresentado a questão segurança no contexto da interconexão com redes heterogêneas. A interconexão e interoperabilidade dos sistemas PCS com redes heterogêneas fixas e móveis é outro problema a ser abordado neste trabalho

No Capítulo 2 é realizado uma revisão dos aspectos de segurança em comunicação de dados, são estudados os sistemas de criptografia pública e privada. Neste capítulo também é abordado a questão de autenticação em redes de comunicação *wireline* e *wireless*.

No Capítulo 3 é apresentado a evolução dos sistemas de comunicação sem fio. São mostrados os conceitos e as caraterísticas básicas dos sistemas de telefonia celular. Como parte da evolução *wireless*, é revisada e analisada cada uma das três gerações, em especial é feito um estudo comparativo entre os principais padrões de telefonia celular analógica, digital e sistemas PCS.

No Capítulo 4 são abordados as características de segurança nos sistemas de telefonia celular analógica AMPS, telefonia celular digital USCD e GSM. O resultado deste estudo é mostrado numa tabela comparativa.

No Capítulo 5 estão descritos as características que os sistemas PCS deverão ter em relação a autenticação e privacidade. Por exemplo, são analisados os requisitos dos algoritmos de criptografia para implementar processos de autenticação eficientes e seguros. É descrito o modelo e o protocolo AKA para autenticação e privacidade em sistemas PCS.

A rápida evolução tecnológica nos campos da informática e telecomunicações permitiu que acontecesse uma verdadeira revolução nas aplicações de telefonia. A telefonia, através de um processo de transformação, se misturou à informática, não sendo mais possível fazer uma separação clara entre elementos como computação, comunicações e telefonia. Uma dessas misturas, entre a informática e as telecomunicações, é a sinalização na rede inteligente pública (IN-*Intelligent Network).*

No Capítulo 6 é abordada a questão da segurança na interconexão de redes heterogêneas, onde é mostrada a importância do uso da rede inteligente baseado em mecanismos de sinalização por canal comum SS7, para a construção de interfaces confiáveis de interconexão e interoperabilidade.

O assunto da interconexão com redes heterogêneas é o outro aspecto a ser resolvido na implementação da terceira geração de sistemas *wireless*. O principal objetivo dos sistemas PCS é oferecer a mobilidade pessoal e do terminal, portanto, além de permitir a interconexão das redes PCS com redes similares, (redes homogêneas) também será necessário que os sistemas PCS interajam de forma compatível com as diversas redes de telecomunicações fixas e móveis (redes heterogêneas), atualmente existentes, razão pela qual será necessário o uso de uma interface de interconexão e interoperabilidade adequada. A questão é abordada no Capítulo 7, onde são revisados e estudados os protocolos de sinalização SS7 (*Signaling System Number 7*) e MAP (*Mobile Application Part*), como requisitos importantes na solução deste problema. Como conclusão deste estudo é apresentado uma proposta de uma arquitetura de protocolos de sinalização, representando a interconexão de um sistema PCS baseado no padrão J-STD-007 com a rede de telefonia celular IS-95. Esta interconexão é realizada através de uma interface de rede, denominada IIF (*Interworking and Interoperability Function*), usando protocolos de sinalização por canal comum SS7 e MAP.

No Capítulo 8 são apresentadas algumas conclusões deste trabalho e é sugerido uma continuidade, como trabalho futuro, a especificação e modelagem de uma interface IIF tomando como base o trabalho desenvolvido.

2 Segurança em Redes de Comunicação de Dados

Os avanços tecnológicos têm facilitado e tornado cada vez mais eficiente a transferência de informações através dos meios de comunicação. Nesta década, a ampla utilização das redes telecomunicações e as exigências próprias de um mundo globalizado impulsa a necessidade de fornecer sistemas e redes confiáveis e seguros. A segurança é um aspecto importante em qualquer sistema de comunicação, os princípios básicos de segurança nestes sistemas compreendem :

- Confidencialidade. Tem por objetivo proteger a informação intercambiada prevenindo-a de acessos não autorizados.

- Integridade. Deve garantir a veracidade da informação protegendo-a de modificações não autorizadas.

- Autenticidade. Visa garantir a identidade dos parceiros do intercâmbio através da autenticação dos usuários.

- Disponibilidade. Objetiva prever interrupções na operação da rede garantindo a disponibilidade do uso da informação.

As técnicas para a proteção da comunicação de dados têm evoluído muito mais no sentido do desenvolvimento de artifícios, como a criptografia para tornar ininteligível, a um intruso, os dados que são transmitidos, do que no sentido de proteger fisicamente os meios de comunicação para evitar o acesso indevido a eles. Em outras palavras, não há maiores preocupações em impedir que um estranho "ouça" o que passa por um canal, mas são tomadas providencias para que ele não consiga "entender" o que pudesse ouvir. Não poderia ser diferente, já que os modernos canais de telecomunicações envolvem meios cuja proteção física em alto grau seria impraticável, por exemplo, longos cabos passando por vias públicas, enlaces de rádio em diferentes espectros de freqüência.

Foi, justamente, pelo reconhecimento desses fatos que as técnicas de criptografia foram desenvolvidas, tornando sem importância o fato de que um intruso conseguir acesso ao que estiver sendo transmitido [TAN96].

2.1 Sistemas de Criptografia.

A finalidade básica de um sistema de criptografia é cifrar (codificar ou criptografar) uma mensagem através de um método de cifragem, que recebe como entrada a própria mensagem e uma chave de cifragem, produzindo como resultado uma mensagem cifrada. Esta mensagem cifrada é então, armazenada em um meio qualquer ou transmitida até um receptor. Para decifrar a mensagem (decodificar ou decriptografar) utiliza-se um método de decifragem, que recebe como entrada a mensagem cifrada e uma chave de decifragem, e fornece como saída a mensagem original. A Figura 2.1 mostra os componentes de um sistema de criptografia.

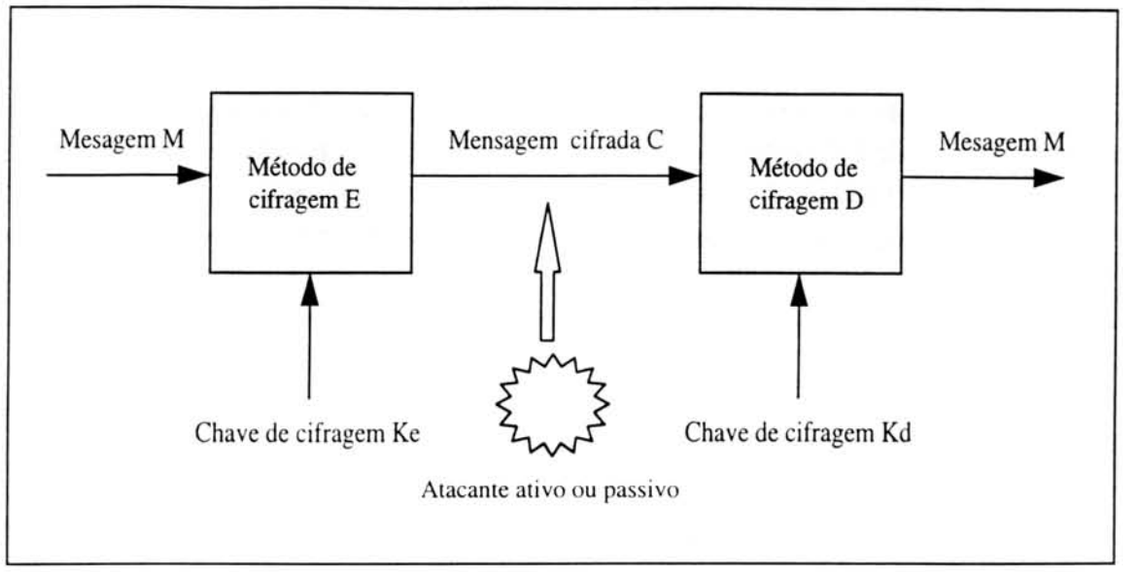

FIGURA 2.1 - Sistema de Criptografia

A criptografia é usada para garantir :

- Sigilo ou privacidade, de forma que somente os usuários autorizados tenham acesso à informação ou consigam torná-la inteligível.

- Integridade, permitindo verificar que as informações originais não foram alteradas, nem acidental nem intencionalmente.

- Autenticidade, fornecendo meios de verificar a identidade do remetente ou autor da mensagem. A assinatura digital é uma aplicação especializada da criptografia utilizada para assegurar a origem da mensagem e também a identidade do emissor.

A Criptoanalise, é a arte ou ciência de descobrir a chave ou decifrar mensagens criptografados sem utilizar a chave; uma tentativa de criptoanálise é chamada de ataque.

Algoritmos da criptografia tradicional utilizam técnicas de substituição e de transposição, já os modernos sistemas criptográficos podem ser classificados em duas categorias de acordo com o tipo de chave que utilizam : criptografia de chave secreta ou simétrica e criptografia de chave pública ou assimétrica [WEB95].

2.1.1 Criptografia de chave secreta.

Os sistemas simétricos utilizam apenas uma única chave, que deverá ser mantida sob sigilo e será usada tanto para criptografar como para decriptografar.

Algumas vantagens dos algoritmos de chave secreta são :

- Rapidez de execução em relação com algoritmos de chave pública.

- Bom desempenho em implementações de *hardware*. Ideal para aplicações de grandes volumes de dados como nos canais de comunicação.

Por outro lado as desvantagens dos algoritmos de chave secreta são :

- Gerenciamento da chave. Como a criptografia simétrica está baseada no compartilhamento de uma mesma chave entre o emissor e o destinatário da mensagem, o principal problema deste método é o gerenciamento das chaves: a chave secreta tem que ser gerada, transmitida e armazenada de uma maneira segura e confidencial para garantir que apenas o usuário origem e o usuário destino tenham acesso a essa informação; para tal, o intercâmbio da chave deverá ser feita usando um meio ou método distinto.
- Diretamente não fornece mecanismos de autenticidade, por exemplo a assinatura digital.

Os algoritmos de chave secreta mais conhecidos são :

a) DES (*Data Encryption Standard*). É um algoritmo de criptografia simétrico desenvolvido pela IBM, adotado pelo governo norte-americano em 1977 e padronizado pelo ANSI (*American National Standard Institute*) em 1981. A chave criptográfica do DES possui 56 bits e durante a criptografia o algoritmo divide a mensagem em blocos de 64 bits e realiza 19 estágios de execução contendo uma transposição de bits inicial, uma transformação de produto realizado em varias etapas de interação (16 ciclos) e uma transposição final. A quebra do DES pelo ataque da força bruta ou por um "*backdoor*", é um assunto bastante discutido pela comunidade cientifica mundial. No evento *Crypto Conference 1993,* por exemplo, foi apresentado a arquitetura de uma máquina baseada em um chip capaz de testar 50 milhões de chaves DES por segundo; ao preço unitário de cerca de 10 dólares por chip. Este chip possibilitaria a construção de uma máquina de 1 milhão de dólares que levaria, em média, 3.5 horas para quebrar qualquer mensagem DES.

b) Triple DES. É um método onde o DES é aplicado três vezes. Nesta técnica cada mensagem passa por três processos criptográficos que irão reduzir a possibilidade de que a segurança seja quebrada através de ataques de força bruta (busca exaustiva). Isto eqüivale a, no mínimo, dobrar o tamanho da chave DES para 112 bits.

c) IDEA (*International Data Encryption Algorithm*).Trabalha sobre blocos de 64 bits com uma chave de 128 bits. Não utiliza transposições, mas, somente operações de ou-exclusivo, soma e multiplicação em módulo de 2^16 (ou seja, ignorando qualquer *overflow*). Todas as operações são realizadas sobre sub-blocos de 16 bits. Não existe ainda um método de ataque efetivo contra o algoritmo, apesar de ele ter sido desenvolvido em 1990. Até o momento, ele tem resistido bem contra os métodos aplicados com êxito sobre outros algoritmos.

d) *Skip Jack.* Usa uma chave de 80 bits e trabalha com blocos de 64 bits. O Algoritmo foi desenvolvido pela NSA (*National Security Agency*) em 1990, maiores detalhes

e informações deste algoritmo são classificadas como secretas pelo governo norte-americano. Este algoritmo está destinado para ser implementado no *Chip Clipper* para tornar as redes de telecomunicações americanas mais seguras.

e) RC2 e RC4. São algoritmos de "exportação" com 40 bits de chave. O governo norte-americano já aprovou a exportação de algoritmos de chave pública de até 56 bits.

2.1.2 Criptografia de chave pública.

A criptografia de chave pública ou assimétrica utiliza duas chaves: uma chave privada e uma chave pública; o usuário deverá divulgar sua chave pública e manter em sigilo sua chave privada. As chaves são complementares no processo criptográfico, sendo assim, que uma delas é usada para criptografar a mensagem e a outra para decriptografar. Os algoritmos assimétricos tiveram inicio a partir de um estudo elaborado por Daffie e Hellman, dois jovens pesquisadores da Universidades de Stanford na Califórnia, em 1976, eles definiram o *Public Key Cryptography* (PKC) cujo objetivo básico seria solucionar o problema de gerenciamento de chaves dos algoritmos simétricos.

Vantagens dos algoritmos de chave pública :

- A principal vantagem da criptografia assimétrica é não necessitar do gerenciamento de chaves: ela possibilita uma maior segurança por não precisar compartilhar uma mesma chave criptográfica. A chave privada deve ser conhecida apenas pelo usuário proprietário, a chave pública correspondente (necessária para fazer o processo criptográfico inverso) poderá ser conhecida por todos.
- Pode ser usado em processos de autenticação, como a assinatura digital.

Desvantagens dos algoritmos de chave pública :

- A pesar da criptografia assimétrica ser bem mais segura que a simétrica, ela possui uma grande desvantagem: para permitir a propriedade de utilizar duas chaves distintas, a sua execução está baseada em protocolos complexos que exigem mais recursos computacionais, isto se reflete na lentidão da execução do algoritmo.
- Algoritmos de chave assimétrica não são apropriados para a crifragem e decifragem de grandes volumes de dados.

O RSA *(Rivest, Shamir e Adleman Algorithm)* é o mais popular algoritmo de chave pública, bem como o mais fácil de compreender e de implementar e ao mesmo tempo um dos mais robustos. Este algoritmo foi desenvolvido por um grupo de pesquisadores : Ronald Rivest, Adi Shamir e Leonard Adleman, sendo patenteado pelo MIT (*Massachusetts Institute of Technology*) em 1978.

A segurança do RSA está baseada na dificuldade de fatorar grandes números: as chaves são calculadas matematicamente combinando dois números primos de grande tamanho. Mesmo se conhecendo o produto desses números primos (que faz

parte da chave pública divulgada), a segurança do algoritmo é garantida pela complexidade de fatorar esse produto e se obter os valores secretos.

Um outro fator que determinou a popularidade do RSA é o fato de ele também poder ser usado para assinatura digital no processo de autenticação. O RSA está patenteado somente nos EUA e está disponível em *hardware* e *software.*

2.1.3 Sistemas de criptografia híbrida.

Os sistemas híbridos são bastante utilizados em criptografia de dados. Este método se apresenta como a combinação das duas técnicas de criptografia apresentados, de tal forma que se aproveita a vantagem de segurança do algoritmo assimétrico e a vantagem de rapidez de execução do algoritmo simétrico. O método usa a criptografia assimétrica para a troca de uma chave secreta temporária; como essa etapa será única e fundamental para a confidencialidade total do intercâmbio, o tempo adicional gasto na criptografia será compensado pela segurança do sigilo oferecido. A criptografia simétrica é usada para proteger as outras mensagens, essa etapa será repetida inúmeras vezes devendo, necessariamente, usar um método rápido de criptografia; como a chave de criptografia foi intercambiada de uma maneira sigilosa e é temporária, o algoritmo simétrico fornecerá uma boa segurança.

2.1.4 Segurança dos sistemas de criptografia.

Os distintos sistemas de criptografia possuem diferentes graus de segurança, mas todos os métodos desenvolvidos e em uso atualmente são quebráveis, desde que sejam fornecidos tempo e recursos computacionais suficientes. Para muitos deles, entretanto, o tempo e o custo necessários para quebrá-los é muito grande (alguns se aproximam de infinito). Se o custo requerido para quebrar um sistema (ou decifrar uma mensagem) é maior que o valor da informação que será obtida, então, para todos os fins práticos, o sistema é seguro. Deve-se observar, entretanto, que o poder de processamento dos computadores está sempre crescendo, e que o valor da informação armazenada diminui com o passar do tempo. Se para um determinado sistema estas duas linhas se cruzarem, o sistema torna-se inseguro.

Na Tabela 2.1 são mostrados os resultados do método de ataque através da força bruta com uma máquina que seja capaz de realizar um milhão de encriptações por segundo, tentando-se todas as combinações possíveis para a chave. Na Tabela 2.2 é mostrado o número de máquinas que será necessário para quebrar um algoritmo de criptografia, assumindo que cada máquina seja capaz de testar um milhão de chaves por segundos.

TABELA 2.1 Tempo que levaria para quebrar um algoritmo de *n* bits através do ataque da força bruta [MAR95]

Tamanho da Chave	32 bits	40bits	56bits	64bits	128bits
Tempo requerido para testar todas as possíveis chaves	1.19 horas	12.7 dias	2.291 anos	584,542 anos	10.8 x10^24 anos

TABELA 2.2 Número de máquinas requeridas para quebrar um algoritmo de *n* bits através do ataque da forca bruta. [MAR95]

Tamanho da chave	1 dia	1 Semana	1 ano
40bits	13	2	
56bits	836,788	119,132	2,291
64bits	2.14x10^8	3.04x10^6	584,542
128bits	3.9x10^27	5.6x10^26	10.8x10^24

2.2 Autenticação.

O processo de Autenticação de usuários é bastante prejudicado pelas possibilidades de interceptação decorrentes pelo fato de que as informações confidenciais que são necessárias para autenticar o cliente (ou o usuário origem) junto a rede (ou usuário destino), poderão ser manipuladas por outros usuários ao trafegarem pela rede.

Devido a esses problemas de vulnerabilidade da comunicação que possibilita ameaças à segurança do sistema, um sistema de autenticação propício a esse ambiente requer:

- Uma autenticação forte (*strong authentication*). Cujo objetivo é fazer com que as informações necessárias para autenticar um usuário não sejam divulgadas durante a comunicação.

- Uma autenticação mútua. A autenticação deve ocorrer nos dois sentidos, ou seja, tanto a origem deve ser autenticada no destino para que este tenha a garantia de onde a mensagem foi originada; como o destino deve ser autenticado na origem para garantir que realmente é ele que irá receber e interpretar a mensagem enviada.

- Uma autenticação contínua. A freqüência do processo de autenticação deverá ser periódica ; apenas uma autenticação inicial não é suficiente, pois, um intruso poderá se fazer passar por um usuário já autenticado e deturpar o intercâmbio.

As ameaças de segurança, em um ambiente distribuído, poderão ser controladas usando criptografia para fornecer uma autenticação forte, mútua e contínua. Independentemente de qual técnica de criptografia (simétrica ou assimétrica) seja utilizada, é necessário que os parceiros de comunicação tenham conhecimento da chave criptográfica. Se a chave de criptografia é compartilhada apenas entre os dois parceiros, denominamos esse processo de protocolo de autenticação.

Na criptografia simétrica, cada dupla de parceiros deverá compartilhar, entre si, uma única informação confidencial; a cada novo parceiro de comunicação uma nova informação deverá ser intercambiada entre eles. Dependendo do número de parceiros que estão envolvidos no processo de comunicação, poderá ficar bastante complexo a etapa de autenticação devido a quantidade de chaves confidenciais que irão ser necessárias para autenticar cada parceiro isoladamente.

Na criptografia assimétrica, teremos um problema semelhante com o gerenciamento das chaves públicas que, apesar de não ser uma informação confidencial como no caso anterior, continuará existindo uma diversidade de chaves (cada parceiro possui a sua própria chave pública).

Os usuários estão interconectados com as suas aplicações distribuídas através de redes abertas, não confiáveis, que podem ser compartilhadas por outros usuários, os quais não estão autorizados a acessar determinados sistemas. Assim torna-se necessário identificar e autenticar o usuário que solicitar conexão ao sistema bem como verificar se ele possui autorização para acessar os recursos solicitados.

A identificação é o processo inicial para verificar se esse usuário está cadastrado no sistema; normalmente, essa identificação é realizada através de um *user-identification,* ou de um PIN (*Personal Identification Number*) [PIN95].

A autenticação é a etapa seguinte na qual o usuário deverá provar sua identidade. Antigamente, este processo era sinônimo de *password*, porém, atualmente podemos classificar os métodos de autenticação do usuário em três categorias:

a) Algo que o usuário conheça. O sistema indaga por uma informação que o usuário tenha conhecimento, sendo o caso típico do *password*. Este é o método mais simples de ser utilizado porém o mais fácil de ser quebrado.

b) Algo que o usuário possua. O sistema solicita a apresentação de algum objeto físico que o usuário tenha, podendo ser desde um simple cartão magnético até sofisticados dispositivos eletrônicos. Esses dispositivos podem ser classificados em :

- *Smart Cards.* São dispositivos semelhantes a um cartão de crédito contendo *microchips* que consistem de um processador, uma memória para armazenar programas e dados e uma interface com o usuário.
- *Tokens.* São dispositivos eletrônicos semelhantes a uma calculadora de mão, normalmente contendo um algoritmo criptografador e uma chave secreta do usuário que serão usados para calcular uma senha de acesso *one time*, senhas válidas apenas uma única vez, ou seja, a cada nova conexão é gerado uma nova senha. A desvantagem deste tipo de autenticação é o custo adicional do hardware e a possibilidade da perda ou esquecimento do *token*.
- Desafio/Resposta. Neste outro tipo de técnica, o servidor de autenticação solicita ao usuário que envie uma "resposta" a um determinado "desafio"; é a técnica usada pela maioria dos fabricantes de *tokens*, possuindo diferentes *hardwares* e formas de implementação. A idea básica desta técnica inicia com o usuário enviando o seu PIN ao servidor de autenticação; o servidor gera um número randómico e envia ao usuário; o *token* do usuário deverá criptografar este número com sua chave secreta (podendo ser usado o algoritmo DES ou RSA, conforme a implementação) e o resultado obtido deve ser encaminhado ao servidor; finalmente, o servidor localiza a chave do usuário e decriptografa o número recebido, verificando se é igual ao número enviado inicialmente. A maior desvantagem desta técnica é número de mensagens intercambiadas entre o usuário e o servidor.

c) Algo que o usuário seja. Esta categoria está relacionada como os sistemas biométricos que são métodos automatizados para verificar a identidade de uma pessoa baseando-se em alguma característica fisiológica ou comportamental. A vantagem desta técnica é que garante uma maior confiablilidade por ser difícil de ser forçada, bem como não poder ser esquecida. Porém tem varias desvantagens: o desconforto de utilizar alguns desses dispositivos, o custo dos equipamentos necessários até a quantidade de dados que devem ser armazenadas e transmitidas. Os tipos de dispositivos biométricos podem ser classificados de acordo com as características utilizadas [PIN95]:

- Caraterísticas fisiológicas. Normalmente, são caraterísticas físicas estáveis (embora possam variar um pouco de tempos em tempos) porém requerem equipamentos mais sofisticados. Exemplo são a impressão digital, formato de mão, padrão de retina, padrão de íris, reconhecimento da face.
- Caraterísticas comportamentais. Essas caraterísticas são favorável à mundanças devido às influencias que sofrem relacionadas a stress, estado emocional, estado de saúde, etc, porém elas são mais simples a serem implementadas e capturadas. Exemplos são a assinatura, padrão de voz, ritmo de teclar, etc.

2.3 Segurança em Sistemas de Comunicação Sem Fio.

As exigências quanto a segurança, em qualquer sistema de comunicação, são cada vez maiores. Infelizmente os sistemas sem fio, pela sua natureza, utilizam como meio de comunicação um canal de RF (rádio freqüência) partilhado, que são muito mais vulneráveis a ataques do que os sistemas com fio. Em sistemas de comunicação por rádio, as mensagens podem ser interceptadas sem necessidade de um "grampo" físico [YAC95]. Basicamente, na comunicações sem fio, a segurança é comprometida em três aspectos principais:

- Privacidade. Em comunicações *wireless* é perdida a privacidade, pois é relativamente fácil interceptar os sinais emitidos por sistemas de rádio. Pode-se fazer isto, por exemplo, utilizando-se um simples sistema de rádio com facilidades de varredura (*scanner)*, como é o caso dos receptores utilizados por radioamadores. Por outro lado, o sigilo da identidade e a localização do usuário também são ameaçadas.
- Autenticação. Não há garantia da identidade de quem está acessando a rede de comunicação. É possível alguém ter escutado e copiado as características de identificação de um usuário legítimo e usar estas credenciais para invadir o sistema. Por exemplo, é muito comum este tipo de fraude em sistemas da telefonia celular analógica, o qual é denominado de fraude do telefone clone.
- Integridade. Em sistemas de comunicações, os dados transmitidos podem ser escutados e, posteriormente, alterados em benefício do intruso. Este tipo de fraude torna-se mais grave em comunicações de dados de alto valor como, por exemplo, os que estão relacionados a serviços de *banking* remoto.

3 Evolução dos Sistemas de Comunicação Sem Fio.

As comunicações móveis ou sem fio, passaram por uma evolução explosiva, que fica evidenciada através de três gerações tecnológicas em menos de duas décadas (Ver Figura 3.1) [LI95]. Esta evolução acelerada é motivada, em parte, por uma vertiginosa demanda da mobilidade e portabilidade nas comunicações por parte dos usuários, que não foi prevista no seu início [LUN95]. Apoiando esta evolução, está também a revolução digital, pela qual estão passando atualmente todos os sistemas de telecomunicações.

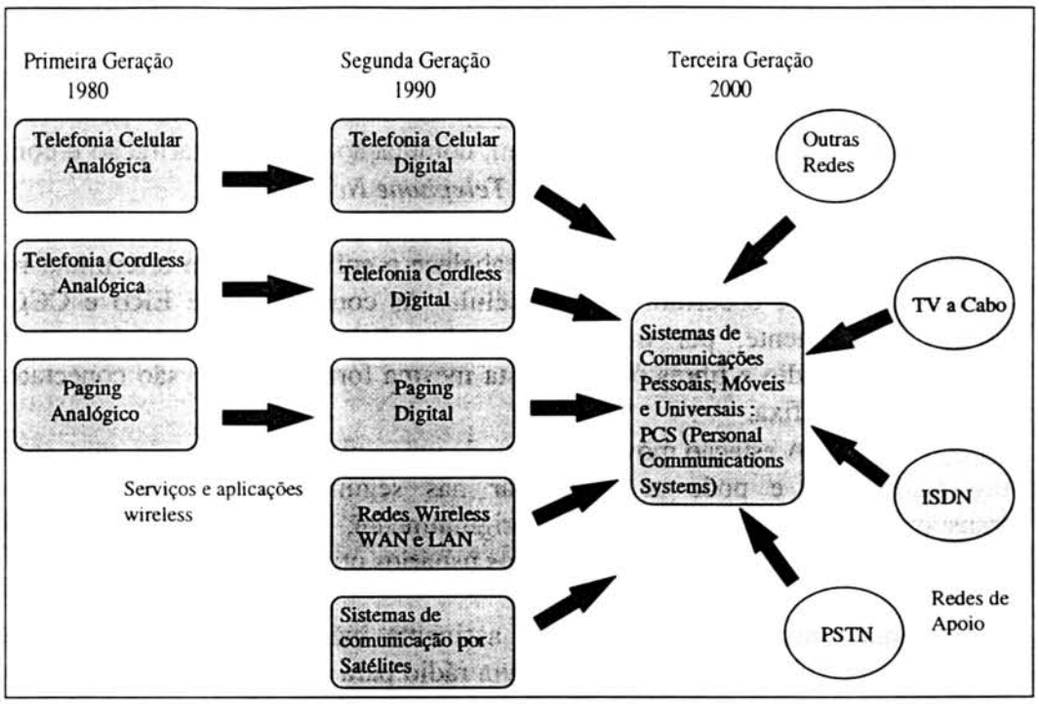

FIGURA 3.1 - Evolução dos Sistemas de Comunicação Sem Fio [LUN96].

3.1 Conceitos de Telefonia Celular.

Os primeiros telefones móveis ou LMR (*Land Mobile Radio*) foram usados em décadas anteriores, mas não tiveram ampla aceitação devido a sua limitada capacidade de usuários e o curto alcance da estação base. Uma solução para estes problemas veio com o conceito de telefonia celular, um sistema de comunicação de radio *full duplex*, baseado na reutilização de freqüências, e que constituem o primeiro passo na revolução das comunicações sem fio [LUN95].

Basicamente, a telefonia celular está estruturada sobre um conjunto de canais de Radio Freqüência (RF) definidos para uma área chamada de célula. As células são definidas como áreas de serviço individuais, onde cada uma delas possui um grupo de canais designados de acordo com o espectro disponível. Cada célula possui a sua estação base, permitindo assim o uso de transmissores de baixa potência [ROC95].

Quando se pensa em uma célula, a primeira idéia é a de uma estrutura circular, pois em condições ideais de propagação e utilizando uma antena omnidirecional,

temos uma zona de cobertura uniforme. Entretanto, quando se monta um aglomerado de células, o modelo de irradiação circular nos traz certos problemas, como áreas de superposição e de sombra. Estas células são, então, usualmente, representadas por hexágonos, cujas formas as possibilitam ser colocadas lado a lado, sem os inconvenientes citados anteriormente. Obviamente, este recurso é somente para uso em modelos teóricos, pois na prática é impossível conseguir condições tão favoráveis de propagação, porque uma região coberta por um sinal de RF está sujeita a vários fenômenos da natureza, causando variações consideráveis em seu percurso.

Um sistema celular típico é constituído de três componentes básicos, além das conexões entre estes elementos, que são [TEL94] :

- Centro de Comutação e Controle (CCC). O CCC é responsável pelas funções operacionais da rede móvel, quais sejam, comutação, controle, tarifação e conexão com a rede fixa PSTN (*Public Swithed Telephone Network*).
- Estação Radiobase (ERB). A ERB fornece a interface entre a central de comutação e controle e as estações móveis; ela estabelece o enlace RF com o terminal móvel dentro da área de cobertura de uma célula. As conexões entre ERB e CCC são feitas, normalmente, por troncos de linhas físicas, sendo também possíveis conexões por rádio e fibras óticas. Desta mesma forma as CCC são conectadas às centrais da rede fixa.
- Estação móvel. A estação móvel consiste de uma unidade de controle, uma antena e um transceptor e pode se apresentar nas seguintes configurações: veicular, transportável ou portátil. Embora, originalmente, desenvolvida para terminais móveis em viaturas, atualmente, 98% dos usuários utilizam unidades portáteis.

Quando uma chamada entre um assinante móvel e um assinante fixo for estabelecida, os dados serão transmitidos via rádio para a estação de rádiobase situada mais próxima desta estação móvel. Em seguida, estes dados são encaminhados a uma central de comutação e controle do serviço móvel, e daí comutada para a rede telefônica pública onde o assinante fixo está conectado.

Da mesma forma, um assinante da rede fixa, pode acessar automaticamente qualquer estação móvel, através de busca (*paging*) e comutação automática processadas pela central de comutação do serviço móvel.

Enlaces de rádio e enlaces de dados a alta velocidade conectam os três subsistemas mencionados anteriormente. São realizadas conexões via rádio entre as estações móveis e a estação de rádiobase, onde cada unidade móvel utiliza apenas um canal por vez para o seu enlace de comunicação. Este canal não é fixo, podendo ser qualquer um, dentro da faixa de freqüência aloucada pela área de serviço.

A técnica de reutilização de freqüência é uma forma de economizar banda e aumentar a capacidade de assinantes. O reuso de freqüência permite que canais distintos designados para uma determinada célula possam ser usados novamente em qualquer outra célula diferente da anterior, desde que estejam separadas por uma distância suficientemente grande para se evitar o surgimento da interferência co-canal, que deteriora a qualidade do serviço. À medida que o sistema se expande, os canais

podem ser continuamente reutilizados, permitindo que este nunca esgote o número de canais disponibilizados ao público.

A extensão geográfica de uma rede de telefonia celular é constituída por células de tal forma que células adjacentes contenham conjuntos de canais de freqüências distintas para evitar interferência mútua.

Devido à grande flexibilidade do sistema celular, a expansão do sistema não é uma tarefa complicada. Quando a demanda, em uma determinada célula, cresce, o problema pode ser contornado das seguintes maneiras:

- Adição de novas células.
- Setorização das células existentes.

No caso da adição de novas células, duas filosofias podem ser adotadas:

1. Baixar a potência dos transmissores das células existentes para cobrir metade da área original, fazendo uma reordenação do plano de freqüências. Assim a distância de reuso das freqüências diminui, possibilitando que na mesma área anterior ocorra um número muito maior de ligações simultâneas.

2. Criação de células menores dentro de uma determinada célula já congestionada, utilizando alguns canais da célula hospedeira (que continua a cobrir a mesma área de antes) até que toda a região tenha sido coberta pelas células menores.

Qualquer dos dois modelos é válido, sendo que no primeiro caso (baixar a potência do transmissor e incluir novas células) o custo é muito elevado, pois é necessário a reordenação total de todo o sistema de uma só vez, o que nem sempre é possível. Já na segunda hipótese (criação de células menores dentro das antigas) o custo é menos elevado, já que o aumento de células pode ser programado, criando pequenas células nos locais de maior tráfego.

No caso da setorização da célula o custo é bem menos expressivo, pois não há necessidade de criação de novas células. A setorização se dá da seguinte forma:

Inicialmente, a célula possui uma antena omnidirecional posicionada em seu centro, e à medida que o tráfego cresce a célula é dividida em setores usando antenas direcionais de 120 ou 60 graus. Esta configuração permite o melhor uso dos canais de freqüência em uma determinada área, aumentando também a sensibilidade da ERB, permitindo o uso de terminais de menor potência.

A transferência de uma célula a outra conhecido como *handoff*, e o deslocamento entre área de controle *roaming*, são caraterísticas importantes dos sistemas de telefonia celular. O *handoff* é uma função que permite manter a continuidade de uma conversação quando o usuário passa de uma célula para outra, deslocando-se no interior de uma área de controle do sistema. O nível de sinal da portadora é, permanentemente, monitorado pela ERB, e se durante uma ligação ocorrer a degradação de qualquer dos dois sinais, a ERB envia à CCC uma mensagem

de alerta de degradação do nível sinal/ruído. Então, a CCC inicia o seguinte procedimento:

1. A CCC recebe o sinal de alerta e envia a ordem de medição do nível de portadora a todas as células adjacentes. Nesta mensagem a CCC ordena que todas as células adjacentes sintonizem o canal de voz que está sendo usado e efetuem a medição do nível do sinal.

2. As células adjacentes, ao receberem esta mensagem, devem mudar a sintonia de um dos canais livres para efetuar a medição do nível, e enviar à CCC a mensagem de medida do nível de portadora.

3 A CCC compara o nível do sinal de todas as células adjacentes, e escolhe a melhor. Em seguida, a CCC seleciona um canal livre dentre os canais correspondentes àquela determinada célula adjacente e envia os sinais para a inicialização da troca de dados.

O *handoff* pode ocorrer de três formas diferentes: entre setores, entre células, e na mesma célula ou mesmo setor.

O *roaming* é uma função que envolve duas áreas de controle de uma mesma área de serviço, cada uma gerenciada por um CCC diferente. Isto acontece quando a estação móvel se desloca de sua região de habilitação, como por exemplo do Rio de Janeiro para São Paulo. Esta função permite, ao usuário filiado, a uma área de controle a passagem para outra, na condição de visitante, sem a necessidade de notificar manualmente sua localização ao sistema. As informações do usuário são enviadas pelo CCC de origem ao CCC visitado através da interligação existente entre estas unidades.

Dependendo das características da área de cobertura (urbana, suburbana ou rural), os sistemas atuais utilizam células com raios entre 1 e 20 km. As antenas das ERBs são instaladas em pontos dominantes da célula, situados acima dos obstáculos existentes (construções ou relevos do terreno), e a propagação é efetuada através de trajetos que envolvem difração e reflexão da energia.

Embora seja possível analisar a propagação através de métodos determinísticos, em geral, a estimativa da atenuação do sinal é feita com o auxílio de formulações empíricas.

Com a ampliação da telefonia celular em áreas urbanas e aplicações correlatas, a alta densidade de tráfego levou à necessidade de células cada vez menores, gerando os conceitos de microcélulas e picocélulas. Uma microcélula cobre distâncias inferiores a 1 km, com as antenas das ERBs colocadas ao nível das lâmpadas de iluminação pública. A propagação se processa em transversais devido à obstrução causada pelos prédios localizados nas esquinas.

As picocélulas se referem a áreas localizadas no interior de prédios comerciais com a finalidade de atender, sem a utilização de redes cabeadas, aplicações do tipo telefone sem fio, PABX e rede local sem fio WLAN (*Wireless Local Area Network*). As distâncias são inferiores a 100 m e a propagação se processa em visibilidade ao

longo dos corredores, por difração entre corredores transversais e por transmissão através das paredes (mesmo andar) e dos pisos (andares diferentes).

A faixa de freqüência destinada para a telefonia celular está em torno dos 800 MHz e têm uma largura de banda de 50 MHz que é subdividida em duas bandas A e B, cada uma com 25 MHz. A banda A está destinada para o uso das concessionárias da telefonia pública comutada enquanto a banda B está reservada às companhias de telefonia celular privadas.

O acesso à interface rádio pode ser feito com o emprego de 3 técnicas distintas: FDMA, TDMA e CDMA.

No FDMA (*Frequency Division Multiple Access*), a faixa de transmissão é dividida em um determinado número de canais, os quais são atribuídos aos usuários através de um processo de consignação por demanda, ou seja, em uma ERB o usuário pode utilizar qualquer um dos canais que esteja desocupado, no instante, considerado. Esta técnica é a única aplicável aos sistemas analógicos.

No TDMA (*Time Division Multiple Access*), cada usuário dispõe de toda a faixa de freqüência durante um determinado período de tempo denominado janela (*slot*). A tecnologia TDMA divide um simples canal de rádio em um número de *slots* (*time division*) permitindo que estes sejam compartilhados (*Multiple Access*), aumentando a capacidade do canal.

No CDMA (*Code Division Multiple Access*), a freqüência do canal é usada, simultâneamente, por múltiplos usuários. Em uma determinada célula, os sinais são distinguidos pela distribuição deles, segundo diferentes códigos. O CDMA está baseado na tecnologia *spead spectrum*.

O SS (*Spread Spectrum*) foi desenvolvida na década do 40, durante a segunda guerra mundial, para permitir comunicações militares seguras. Um transmissor SS espalha ou difunde o sinal de rádio sobre uma ampla gama de freqüências, segundo uma seqüência determinada. No lado da recepção, o sinal só pode ser detectado por receptores de faixa larga e que conheçam a seqüência de espalhamento.

No caso dos sistemas móveis celulares, o emprego do SS como técnica de acesso da versão CDMA tem base na alta rejeição dos sinais interferentes, tanto no que diz respeito às interferências inerentes ao sistema (co-canal e canal adjacente), como para interferências externas. Neste contexto, o uso de códigos ortogonais e um cuidadoso controle do nível da potência transmitida das ERBs são procedimentos fundamentais.

3.2 A Primeira Geração dos Sistemas de Comunicação Sem Fio.

A Primeira Geração de Sistemas *Wireless* está baseada em tecnologia analógica e foram desenvolvidos na década do 70. São sistemas que estão em um estágio de tecnologia bem maduro e são amplamente usados em todo o mundo. Por exemplo, na atualidade, existem mais de 60 milhões de telefones celulares analógicos a maioria

operando nos EUA. Sistemas típicos desta geração são, além da telefonia celular analógica, os sistemas de mensagens (*paging*) e os sistemas analógicos de telefone sem fio (*cordless*).

3.2.1 Telefonia Celular Analógica.

O primeiro padrão de telefonia celular foi o AMPS (*Advanced Mobile Phone Service*). O AMPS foi desenvolvido pelo Bell Labs e instalado, experimentalmente, em Chicago em 1978, embora, devido a problemas de regulamentação, a exploração comercial do AMPS só tenha sido iniciada em outubro de 1983. Com base no AMPS diversos outros padrões foram desenvolvidos e implementados durante a primeira metade da década de 80. Em 1979, foi desenvolvido o sistema MCS (*Mobile Communication System*) no Japão. Em 1980, o sistema NMT (*Nordic Mobile Telephone*) foi desenvolvido nos países nórdicos. O sistema TACS (*Total Access Communication Systems*) foi desenvolvido em 1982 pelo Reino Unido e o sistema C 450 em 1985 pela Alemanha.

O primeiro sistema de telefonia celular que começou a operar comercialmente foi em 1979 na área metropolitana de Tokyo pela NTT (*Nippon Telephone and Telegraph*). A Tabela 3.1 mostra os principais padrões de telefonia celular analógica e suas caraterísticas.

TABELA 3.1 Panorama Mundial da Telefonia Celular Analógica [PAD95]

Padrão	Região	Método de acesso múltiplo	TX móvel / RX base (MHz)	Canal RF (kHz)	Número de Canais
AMPS	EUA, América, Austrália, e parte de África	FDMA	824-849/869-894	30	832
TACS	Reino Unido e parte de África	FDMA	890-915/935-960	25	1000
NMT 900	Suíça	FDMA	890-915/935-960	12.5	1999
C-450	Alemanha e Portugal	FDMA	450-455.74/460-465.74	10	573
Radiocom 2000	França	FDMA	192.5-199.5/200.5-207.5 215.5-233/207.5-215.5	12.5	560 / 640
NTT	Japão	FDMA	925-940/870-885	25	600

3.2.2 Sistemas de telefonia celular analógico AMPS.

O AMPS é um padrão de telefonia celular de primeira geração, ainda assim na atualidade é o padrão mais difundido no mundo inteiro. Só nos EUA tem 40 milhões de assinantes, e é atualmente adotado por, praticamente, todos os países da América Latina, inclusive o Brasil. O padrão AMPS foi elaborado pela TIA (*Telecommunications Industries Association*) em conjunto com a EIA (*Electronic Industries Association*) através do documento TIA/EIA-533. O padrão adota modulação FM (*Frequency Modulation*) para a transmissão de voz, e modulação FSK (*Frequency Shift Key*) para a sinalização. A técnica de multiplexação para compartilhar a banda é FDMA. Os aspectos de segurança do sistema AMPS estão especificados na recomendação TIA/EIA 533 e TIA IS-41. A Figura 3.2 apresenta a arquitetura típica de

um sistema de telefonia móvel tipo AMPS, identificando os seus três principais elementos estruturais :

- Estação Móvel, MS (*Mobile Station*). A MS é utilizado para acessar os serviços de telecomunicações oferecidos pelo sistema e nela está contido todo o equipamento necessário para realizar a transmissão pelo canal de rádio. A MS está conectada através de uma interface com a estação base.

- Estação Base, BS (*Base Station*). É responsável pelo atendimento dos usuários dentro de uma determinada célula, possibilitando, o estabelecimento das chamadas e o gerenciamento e controle da sinalização telefônica. A BS é constituída de dois elementos: o sistema de rádio e o sistema de controle. A BS interliga o assinante com o MSC *(Mobile Switching Center).*

- Central de Comutação Móvel, MSC (*Mobile Switching Center*). Realiza as funções de comutação e gerenciamento da rede celular. Entre outras funções, estabelece a interface com a rede de comutação pública PSTN. A Interligação dos MSC de diferentes centrais e operadoras possibilita o deslocamento do usuário de forma transparente *(automatic roaming)*, mediante o protocolo de sinalização IS-41.

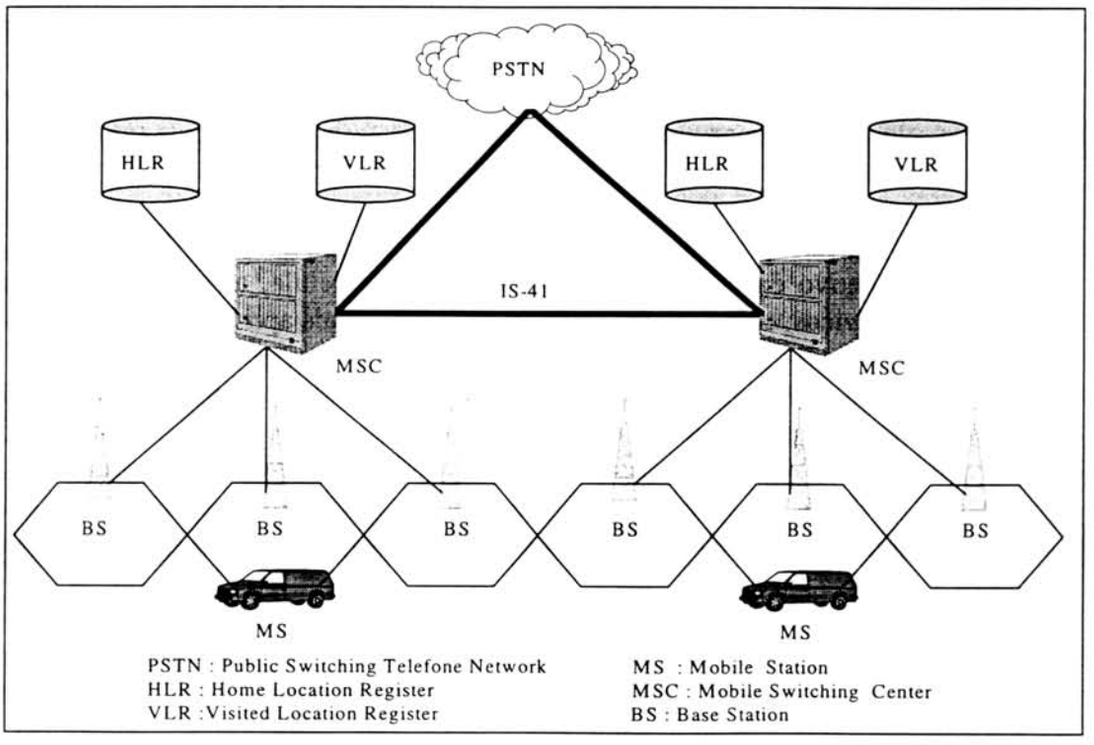

FIGURA 3.2 - Arquitetura e elementos da rede AMPS.

3.3 A Segunda Geração dos Sistemas de Comunicação Sem Fio.

Duas diferentes filosofias orientaram o desenvolvimento dos sistemas digitais que constituem a base da segunda geração da telefonia celular móvel. Na Europa, a necessidade de um sistema que facilitasse o *roaming* internacional levou ao padrão GSM (*Global System Mobile*), incompatível com os sistemas analógicos atuais. Os Estados Unidos e o Japão, ao contrário, optaram pela compatibilidade com os sistemas de primeira geração, de modo a permitir, com o uso de estações móveis duais, uma transição suave para a tecnologia digital.

A Segunda Geração inicia-se com o advento, por volta do final da década de 80, das tecnologias digitais como o SS, as técnicas de acesso múltiplo como o CDMA e o TDMA, entre outras. A técnica de acesso TDMA é usada num dos padrões americanos e nos padrões europeu e japonês. O outro padrão americano adotou a técnica de acesso CDMA.

Entretanto, estes sistemas possuem pontos em comum, embora com modos distintos de implementação. Por exemplo, todos utilizam codificadores, de fonte híbridos, aproveitando o potencial de elevada qualidade dos codificadores de forma de onda com a eficiência de compressão dos codificadores paramétricos (*vocoders*). Por outro lado, com a finalidade de operar com amplificadores de potência não lineares (alto rendimento), são empregadas variações da modulação por desvio de fase de 4 níveis QPSK (*Quadrature Phase Shift Keying*), as quais propiciam também uma satisfatória relação de compromisso entre a largura de faixa do canal de transmissão e a tolerância ao ruído.

Características típicas desta geração são: os serviços de voz e dados digitais, o aumento significativo da capacidade de assinantes por célula, além de uma melhor qualidade dos serviços, como mecanismos de segurança mais aprimorados.

O primeiro padrão de telefonia celular digital, operando comercialmente, foi o GSM, desenvolvido pelos países europeus. Nos EUA surgem os sistemas USCD (*United States Cellular Digital*), sendo o IS-54 o primeiro deles e, posteriormente, o IS-95 e o IS-136. Já na telefonia *cordless*, emergem padrões digitais como DECT (*Digital European Cordless Telephone*) e o PACS (*Personal Access Communications Services*).

Aplicações para transmissão de dados, como os sistemas *paging* de dupla via, e o uso de tecnologias baseadas na modulação SS para redes locais sem fio WLAN também são típicas desta geração.

3.3.1 Sistemas de telefonia celular digital americano USCD.

Sistemas de telefonia celular digital americanos, USCD (*United States Cellular Digital*), são todos aqueles padronizados pela TIA/EIA, ou seja, os *Interim Standard* IS-54, IS-136, e IS-95. A arquitetura de rede dos sistemas USCD e a distribuição de seus elementos estruturais é similar ao padrão AMPS. São agregadas, somente, entidades relacionadas à sinalização do IS-41, como pode ser observado na Figura 3.3.

A seguir será apresentado uma breve descrição das características de cada um dos padrões USCD.

- Padrão IS-54. Foi o primeiro padrão de telefonia celular digital americano, é baseado em técnicas TDMA e FDMA, opera no mesmo espectro usado pelo antigo sistema AMPS conservando os 30 kHz de freqüência portadora. Neste padrão o tipo de modulação digital usado é o π/4 DQPSK (*Diffential Quadrature Phase Shift Keying*). O IS-54 usa a multiplexação TDM *(Time Division Multiplexing)* o que permite 3 usuários por portadora. O quadro tem duração de 20 ms, correspondendo cada janela a 6,67 ms. Este sistema permite obter um ganho maior de 3,5 a 6 vezes maior do que a capacidade do AMPS analógico. IS-54 é chamado, atualmente, por D-AMPS, ou seja AMPS digital. Para facilitar a evolução dos sistemas analógicos, para o digital um fator essencial é o aproveitamento da estrutura já montada e largamente utilizada, por isso o IS-54 é *dualmode*, ou seja, permite a operação em ambos os sistemas.

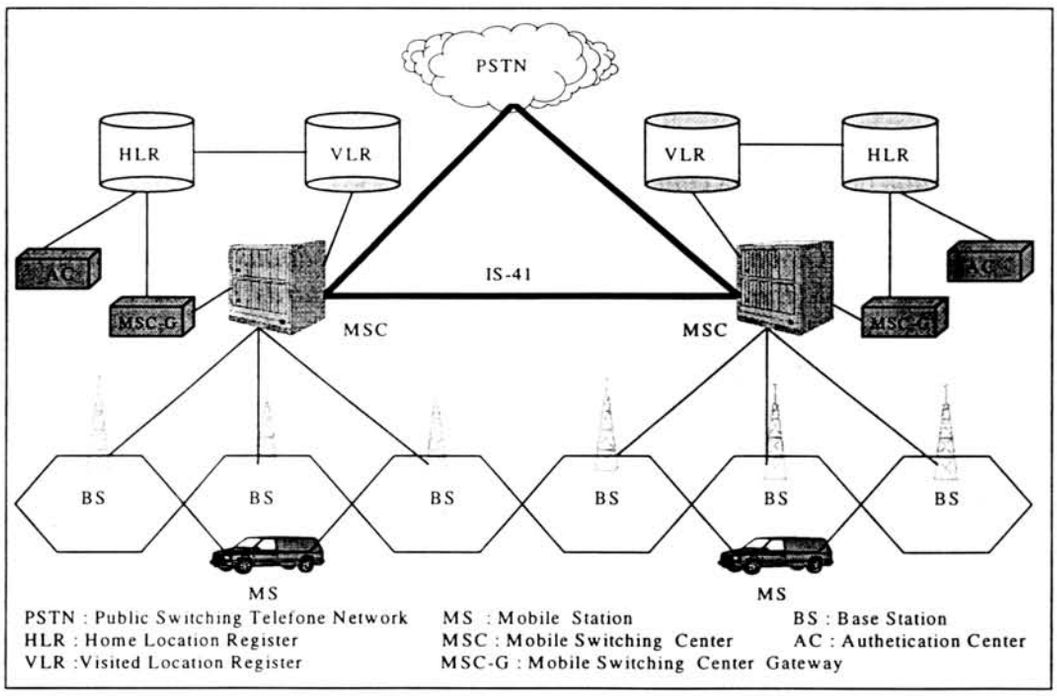

FIGURA 3.3 - Arquitetura da Rede USCD com a sinalização do IS-41

- Padrão IS-95. Em 1992 foi submetido à TIA/EIA uma proposta da *Qualcomm Incorporated*, de um novo sistema de telefonia celular digital, baseado em tecnologia *Spread Spectrum*, chamado CDMA. Em 1994, a TIA /EIA acolheu a proposta da *Qualcomm* como um outro padrão para telefonia celular, através da IS-95. Este padrão também é *dualmode* (AMPS e CDMA). Utiliza uma modulação digital do tipo BPSK/QPSK *(Binary Phase Shift Keying)* e divide a banda de 25 MHz em 10 canais duplex de RF com 1.25 MHz de largura de banda por canal de RF. Cada macro célula pode utilizar a banda celular inteira o que significa um fator de reutilização da freqüência igual a um. Em cada canal de RF são transmitidos, simultáneamente, 64 canais digitais de 9600 bit/s diferenciados através de códigos

de modulação e sequenciação de espalhamento próprios. Sistemas IS-95 tem uma capacidade 10 vezes maior que os sistemas analógicos e oferece uma série de benefícios, incluindo uma alta capacidade de assinantes, excelente desempenho, baixo consumo de potência, eliminação da necessidade de planificar a designação de freqüências para as células e flexibilidade para acomodar as diferentes taxas de transmissão [ROC95a]

- Padrão IS-136. É um padrão de telefonia celular digital baseado no TDMA, na realidade, a revisão C do padrão IS-54. A principal diferença em relação a este é que incorpora um controle totalmente digital do canal, além de aumentar, consideravelmente, a capacidade de assinantes.

- Padrão IS-41. É um padrão de sinalização para as redes de telefonia celular padronizados pela TIA/EIA (inclusive para o AMPS). Neste padrão são definidas as facilidades de operação, capacidade e serviços como *roaming e hand-off:* O IS-41 também especifica os processos de validação e autenticação para assegurar que só legítimos usuários possam acessar o sistema. Os elementos relevantes de uma rede celular, segundo o IS-41, são mostrados também na Figura 3.3 Entre eles está o MSC-G (*Gateway Mobile Switching Center*) e o AC (*Authentication Center*). Uma revisão atualizada, do IS-41-Rev.C, foi publicada em fevereiro de 1996 pela TIA.

3.3.2 Sistema de telefonia celular digital européio GSM.

O GSM (*Global Systems for Mobile Communications*) foi desenvolvido na Europa pelo ETSI (*European Telecommunications Standards Institute*) para fornecer um único padrão de telefonia celular digital para a comunidade Européia. O GSM é um sistema de segunda geração e é baseado no TDMA. Duas bandas de freqüência são definidas para o GSM, uma de 890 até 915 MHz para a transmissão da unidade móvel e outra de 935 até 960 MHz para a transmissão das estações base.

A largura de faixa, por portadora, para este sistema é de 200kHz. Na técnica de acesso TDMA, cada usuário dispõe de toda esta faixa durante 577 microsegundos, ou seja, o período de tempo de uma janela (*slot*). A reunião de 8 usuários distintos corresponde ao quadro (*frame*), cuja duração é de 4,615 milisegundos.

Sistemas GSM operam comercialmente desde 1991, e até dezembro de 1995 havia mais de 10 milhões de usuários, tanto na Europa como em outros países. Nos EUA, por exemplo, algumas operadoras estão estudando o uso de sistemas baseados no GSM, como o PCS-1900 [SCO96].

Como todo sistema de telefonia celular, o GSM tem uma arquitetura semelhante aos demais sistemas de telefonia celular e é composto por três elementos básicos [CAR96] :

- Estação Móvel ou MS (*Mobile Station*). A MS é utilizado para acessar os serviços de telecomunicações oferecidos pelo sistema. O MS contém todos os componentes necessários para realizar a transmissão pelo canal de rádio.

- Subsistema de Estação Base ou BSS (*Base Station Subsystem*). O BSS possui toda a infra-estrutura necessária para operar o sistema de telefonia celular, no que tange a aspectos relacionados com a transmissão via rádio. Funcionalmente, o BSS é subdividido em BTS (*Base Transciver Stations*), encarregada das funções de transmissão, e o BSC (*Base Station Controller*), encarregado das funções de controle.

- Subsistema de Rede ou NSS (*Network Subsystem*). O NSS é responsável pelas principais funções de comutação do GSM e é nele que são encontrados os principais bancos de dados para o armazenamento de informações sobre o usuário e sobre o gerenciamento de sua mobilidade. Seu principal papel, portanto, é gerenciar as comunicações entre os usuários GSM com usuários de outras redes de comunicações. O NSS pode ser subdividido em cinco entidades funcionais; MSC (*Mobile Switching Center*), HLR (*Home Location Register*), VLR (*Visited Location Register*), EIR (*Equipment Identity Register*) e o AUC (*Authentication Center*). Na Figura 3.4 é mostrada a arquitetura da rede GSM com seus principais elementos estruturais

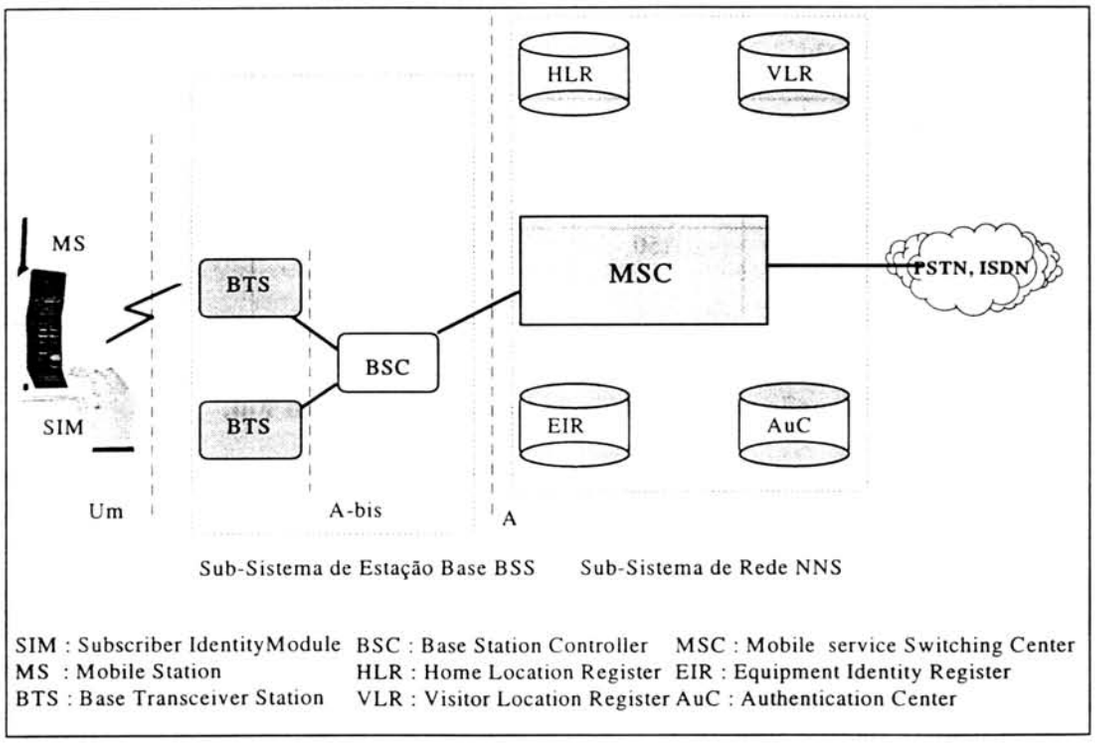

FIGURA 3.4 - Arquitetura da Rede GSM.

3.4 Análise comparativa dos Sistemas de Telefonia Celular AMPS, USCD e GSM.

Atualmente, os sistemas de telefonia celular AMPS, USCD e GSM, estão todos competindo pela supremacia a nível mundial. Além disto, muitas concessionárias, que atualmente estão operando o antigo sistema celular analógico tipo AMPS, estão querendo adotar os novos padrões de telefonia celular digital, o que determinará que terão que oferecer durante algum tempo um sistema *dualmode*, que deverá atender tanto o antigo padrão (analógico) como o novo (digital). Este é o caso

das novas operadoras da banda B no Brasil, que oferecerão a possibilidade de operação dualmode. Outro aspecto que está sendo considerado por estas operadoras, é a capacidade do novo sistema a ser adotado. Na Tabela 3.2 é mostrado os resultados de um estudo comparativo para os sistemas AMPS, USCD e GSM.

TABELA 3.2 Quadro Comparativo entre os sistemas AMPS, USCD e GSM [LUN96].

Caraterísticas	AMPS (FDMA)	IS-54 (TDMA)	IS-136 (TDMA)	IS-95 (CDMA)	GSM (TDMA)
Modos de Operação	Analógico	*Dualmode*	*Dualmode*	*Dulamode*	Digital
Trasmissão Base/Móvel (MHz)	869-894 / 824-849	869-894 / 824-849	869-894 / 824-849	869-894 / 824-849	890-915 / 935-960
Espectro disponível para Telefonia celular (B1)	25 MHz	25 MHz	25 MHz	25 MHz	25 MHz
Modulação	FM/PM/FSK	π/4 DQPSK	π/4DQPSK	BPSK/QPSK SS-DS	GMSK
Canal de RF (B2)	30 kHz	30kHz	30 kHz	1.25 MHz	200 kHz
Número de Canais de voz por canal RF (C)	1	3	6	-	8
Total de número de canais (N) = (B1/B2)*C	833	2499	4998	1200	1000
Fator de sectorização da antena (S)	2.55	2.55	2.55	-	2.55
Fator de reutilização da frequencia (R)	7	7	7	1	7
Canais de voz full-duplex por célula (V) = (N/2)/(R)	59	178	357	-	71
Capacidade de ligações por célula teórico (L) = (V*S)	150	453	910	1200	182

3.5 A Terceira Geração dos Sistemas de Comunicação Sem Fio.

Na década de 90, surgem os sistemas de terceira geração, cuja implantação está prevista para o início do século XXI. São sistemas de comunicação pessoais, segundo um novo conceito de mobilidade e universalidade, em termos de tempo, espaço e serviços conhecidos como sistemas PCS nos EUA, UMTS (*Universal Mobile Telecommunications Systems*) na Europa, e IMT-2000 (*International Mobile Telecommunications at year 2000*) pela ITU (*International Telecommunications Union*). Estes sistemas todos têm características semelhantes, sendo o sistema PCS o mais desenvolvido, no aspecto de padronização e serviços oferecidos comercialmente.

3.5.1 Sistemas UMTS.

Na Europa, a pesquisa e desenvolvimento em tecnologias de terceira geração, estão centrados para os sistemas UMTS (*Universal Mobile Telecommunications Systems*) assumindo pela coordenação das especificações técnicas e padronização à ETSI [SCH95]. Sistemas UMTS estão destinados a integrar todos os serviços da segunda geração, e inclusive uma ampla gama de serviços *broadband* (voz, vídeo, multimídia), coerente e compatível com as redes de telecomunicações fixas.

3.5.2 Sistemas FPLMTS

Em março de 1992, na WARC (*World Administrative Radio Conference*), confereça organizada pela ITU, foram definidas as faixas de RF entre 1885-2025 MHz e 2110-2200 MHz para o Futuro Sistema Público de Telecomunicações Terrestres e Móveis, ou FPLMTS (*Future Public Land Mobile Telecommunications Systems*), incluindo as faixas 1980-2010 MHz e 2170-220 MHz para comunicações pessoais por satélites.

Posicionada dentro de um ambiente de rádio, e usando uma infra-estrutura capaz de oferecer uma ampla gama de serviços, com qualidade semelhante às redes de telecomunicações fixas, o FPLMTS será por volta do ano 2000 a terceira geração global de sistemas de telecomunicações que irão unificar os diversos sistemas que temos atualmente (PSTN e ISDN) [CAL94]. IMT-2000 (*International Mobile Telecommunications at year 2000*) é o outro nome do FPLMTS proposto pelo *Task Group 8/1* do ITU.

3.5.3 Sistemas PCS.

À medida que os usuários vão se acostumando, às comunicações móveis, suas exigências vão aumentando. Eles esperam ser ubíquos, ou seja, que possam ser alcançáveis a qualquer hora, em qualquer lugar e de qualquer forma. Isso é o que pretende ser oferecido pelos novos serviços de comunicação pessoal.

Segundo a definição fornecida pelo FCC (*Federal Communications Commission*), PCS é um sistema pelo qual cada usuário pode trocar informação com alguém, a qualquer hora, em qualquer lugar, através de algum tipo de dispositivo, usando um único número de identificação. Características típicas destes sistemas são [LI95] [PAN95] :

- Mobilidade Pessoal. Diferente dos sistemas de telefonia convencional, os sistemas PCS fornecem mobilidade pessoal, isto é, o assinante terá um número único de acesso à rede PCS, não importa onde esteja ou que tipo de dispositivo ele esteja usando. Um importante passo, nesse sentido, é a padronização do UPT (*Universal Personal Telecommunications*) proposto pela ITU.

- Mobilidade do Terminal. Estes sistemas terão que suportar interfaces de conexão com as redes atuais como: a rede telefônica pública PSTN (*Public Switched Telephone Network*), a rede ISDN (*Integrated Services Digital Network*), as redes de telefonia celular, os sistemas móveis baseados em satélites, entre outras redes. Além disto, os sistemas PCS terão a capacidade de fornecer um *roaming* automático (passagem automática do controle de acesso ao passar de uma célula para outra), inteligente e universal entre redes distintas. Desta forma, o assinante não estará limitado só a um ponto de acesso, ou a uma única rede. Uma questão importante aqui é o terminal PCS, também conhecido como *handset*, o qual será usado para todos os serviços disponíveis. É necessário, portanto, que este seja do tipo *multimode*, com capacidade de operar em ambientes heterogêneos.

- Serviços Multimidia de alta qualidade. Os sistemas *wireless* de terceira geração prometem fornecer uma ampla gama de serviços multimidia, com alta qualidade, como: voz, vídeo *(full motion ou limited)* ou dados, além de altas taxas. O equivalente aos serviços disponíveis na ISDN, também estarão disponíveis nestes sistemas.

- Alta capacidade. A potencial demanda pelos sistemas de comunicação pessoais do futuro está estimada em aproximadamente uma conexão por adulto, por isso, os sistemas da terceira geração terão que ter uma altíssima capacidade.

As atividades de padronização dos sistemas PCS nos EUA estavam sendo feitas de forma desencontrada, até que a TIA (*Telecommunications Industry Association*) e o comitê T1 da ATIS (*Alliance for Telecommunications Industry Solutions*) formaram o JTC (*Joint Technical Committee*), com o objetivo de sugerir recomendações e revisar padrões potenciais para PCS a serem propostos pelos fabricantes. O JTC reconhece que os padrões PCS caem naturalmente em duas categorias: "*high tier* PCS" para macrocélulas com alta velocidade na mobilidade, e "*low tier* PCS", otimizados para baixas potências, pouca mobilidade e microcélulas. Estas duas categorias correspondem, essencialmente, às categorias de "telefonia celular digital" e a "telefonia digital *cordless*", respectivamente [COX95]. Na atualidade, existem sete propostas em estudo pelos TAG (*Technical Ad-hoc Groups*) dentro do JTC, as quais estão resumidas na Tabela 3.3 [COO94].

TABELA 3.3 - Propostas em estudo para padrões de Sistemas PCS [COO94].

Grupo	TAG-1	TAG-2	TAG-3	TAG-4	TAG-5	TAG-6	TAG-7
Padrão	J-STD-017	J-STD-008	J-STD-014	J-STD-011	J-STD-007	-	J-STD-015
Modelo de Referência de Rede	Novo	Baseado no IS-95	Baseado no PACS	Baseado no IS-136	Baseado no GSM	Baseado no DECT	Baseado no IS-665
Sistema	Celular e *Cordless*	Celular	*Cordless*	Celular	Celular	*Cordless*	Celular e *Cordless*
Método de Acesso Múltiplo	CDMA TDMA FDMA	CDMA	TDM TDMA	TDM TDMA	TDMA	TDMA	W-CDMA D-CDMA

Sistemas PCS compreende uma grande variedade de serviços de comunicação móvel e portátil que são fornecidos aos usuários. O espectro é dividido em três categorias distintas, são elas: banda larga *(broadband)*, banda estreita (*narrowband*) e não licenciada (*nonlicenced*).

O FCC alocou um total de 120 MHz do espectro de frequencia ao PCS banda larga no qual oferecerá, inicialmente, serviço de telefonia móvel. O espectro aloucado está na faixa de 1850 a 1990 MHz, e se encontra separado dos outros serviços de comunicação. Sistemas PCS de banda larga é considerado a próxima geração de serviço de telefonia móvel e tem como promessa oferecer também comunicação de dados e vídeo.

Para PCS de banda estreita, o FCC alocou um total de 3 MHz de espectro que será usado para sistemas de *paging* e *menssaging*. Por exemplo, os *pagers* são

equipados com um pequeno teclado, permitindo que o usuário envie mensagens completas através de sinais de RF (e-mail sem fio). Os três MHz que foram aloucados ao PCS de banda estreita estão localizados nas faixas de 901-902, 930-931, 940-941 MHz.

Os PCS não licenciado, acomodará serviços para pequenas áreas dentro de edifícios como redes de área local sem fio, centrais sem fio, telefones *cordless* e outros tipos de comunicação para interiores. Estes sistemas operarão com baixa potência e terão um limite na duração das transmissões. O espectro aloucado para PCS não licenciado compreende a faixa de 1910 a 1930 MHz.

4 Estudo Comparativo dos Aspectos de Segurança em Redes de Telefonia Celular.

Dentro da TIA, segundo o que foi examinado, existem sete propostas de padronização, baseadas na maioria em sistemas de telefonia celular (ver Tabela 3.3). Portanto, está previsto que os sistemas PCS também adotarão, provavelmente, padrões de segurança similares aos que são adotados atualmente na telefonia celular e sistemas *cordless* [BRO95]. Será apresentado, por isso, a seguir, um estudo comparativo dos aspectos de segurança em relação aos principais padrões de telefonia celular, tais como os sistemas AMPS (analógico americano), GSM (digital europeu) e os sistemas USCD (digital americano), representados pelos padrões IS-54, IS-136 e IS-95.

4.1 Segurança no Sistema de Telefonia Celular AMPS.

4.1.1 Autenticação no AMPS.

Em sistemas AMPS, cada unidade móvel é identificada por quatro parâmetros, os quais podem ser armazenados na estação móvel em uma memória permanente, semi-permanente, ou temporária, eles são :

a) MIN (*Mobile Identification Number*). O MIN é um número binário de 34 bits que é derivado a partir do número telefônico do usuário, e normalmente constituído de 10 dígitos. O MIN1 representa os sete últimos dígitos do número de telefone, e o MIN2 e o código de área.

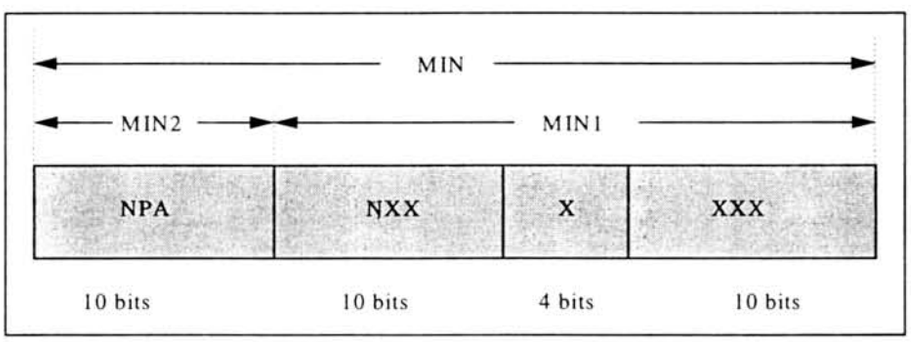

FIGURA 4.1 - Estrutura do MIN - *Mobile Identification Number* .

Por exemplo para o número (617) 637-8687, o MIN respectivo será :

MIN2 : Dez bits mais significativos, obtidos dos 3 primeiros dígitos do Número Telefônico (617) 637-8687 da seguinte forma :

D1=6; D2=1; D3=7
100D1 + 10 D2 + D3 - 111
600+10+7-111=506
506 em binário será : 11111010 = (NPA)

MIN1 : Os dez bits do campo (NXX) são obtidos a partir dos três próximos dígitos (637) como no caso anterior, temos então que, 637 mais transformações resultará em 526, que em binário será, 1000001110.
Os próximos 4 bits do campo (X) são obtidos do digito de mil (8)

transformado em BDC. O algarismo 8 convertido para BCD é igual a 1000. Os dez bits menos significativos de (XXX), são obtidos dos 3 últimos dígitos do número Telefônico, (687) como no primeiro caso :
687 mais as transformações resultará em 576, e em binário será 1001000000

O MIN completo (MIN1 + MIN2) do número telefônico (617) 637-8687 é então :

MIN = 11111010 1000001110100010010000000

b) ESN (*Electronic Serial Number).* O ESN é um número de 32 bits que identifica, de forma unívoca, a estação móvel em qualquer rede celular. Este número é de fabrica, e geralmente está implementado num *chip* ROM soldado na placa. Em algumas ocasiões, o ESN vem embutido no mesmo *chip* do microprocessador ou da RAM ou ROM do telefone celular. O número é constituído de 32 bits divididos em 3 campos conforme mostrado na Figura 4.2. por ocasião da homologação inicial do equipamento será associado um *Manufacturer Code* (MFR), um código do fabricante, constituído de 8 bits. O Campo reservado de 6 bits, por enquanto, estarão todos em zero pois ainda não foi definida nenhuma função para estes bits. Nos bits 0 a 17 será gravado o número serial único do fabricante.

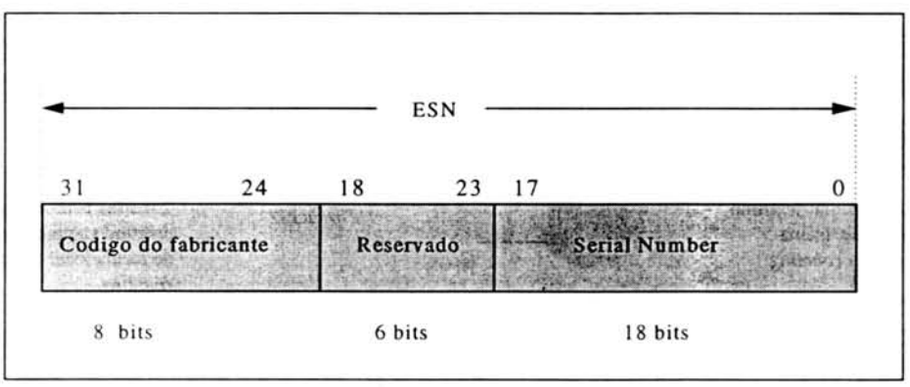

FIGURA. 4.2 - Estrutura do ESN - *Electronic Serial Number.*

c) SCM (*Station Class Mark*). É também usado para a identificação da unidade por parte da estação móvel, onde fornece o tipo de estação e a avaliação de potência de saída. O SCM é um número binário de 8 bits.

d) SID (*Systems Identification*). É um número o qual representa a rede de origem (*home network*) do móvel, este número é de 15 bits.

No processo de autenticação, estes parâmetros são intercambiados entre a MS e o MSC, usando um canal de rádio freqüência. No MSC são consultados e comparados os dados fornecidos pela MS com os dados armazenados no registro de localização de origem HLR quando a MS está na rede de origem, ou no registro de localização de visita VLR quando a MS está em *roaming*. Em ambos os casos, se os dados de identificação coincidirem, o MSC libera o serviço ou então nega a permissão.

4.1.2 Privacidade no AMPS.

Nas especificações originais do documento TIA/EIA-533, não são levados em conta quaisquer aspectos de privacidade, e as informações trafegadas pelos canais de rádio entre a MS, BS e o MSC não tem nenhuma proteção. Isto inclui os parâmetros MIN e ESN, trocados durante o processo de autenticação.

4.1.3 Fraudes em sistemas AMPS.

Analisando os aspectos básicos de segurança do sistema AMPS, conclui-se que os sistemas de telefonia celular, baseados no AMPS, são altamente vulneráveis, pelo fato de que durante o processo de autenticação são trocados os parâmetros críticos de identificação MIN e ESN pelo canal de RF, que não é protegido, podendo ser facilmente capturados e copiados para serem utilizadas em um outro telefone. Este é um tipo de fraude denominada pelas operadoras como *cloning* do telefone celular. Na Figura 4.3 é mostrado o processo *cloning*.

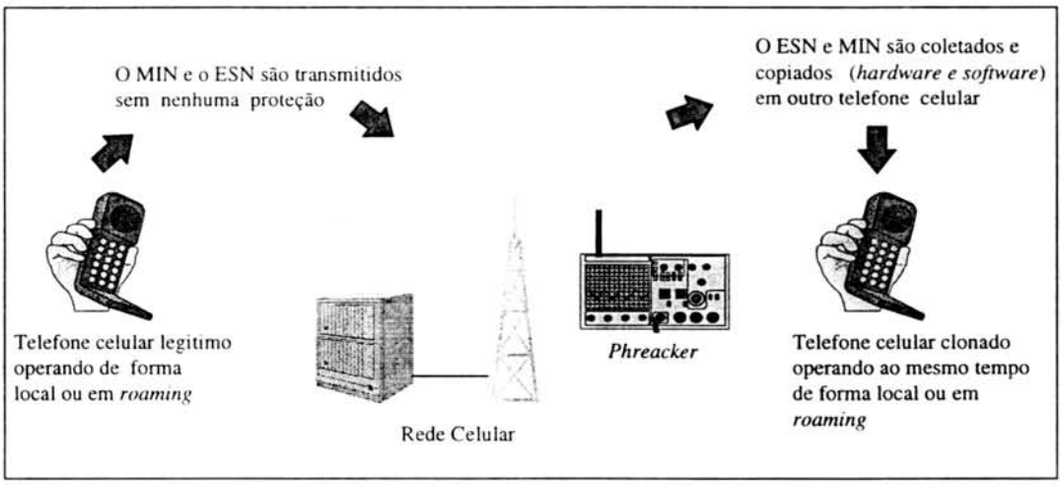

FIGURA 4.3 Processo de *cloning* em sistemas AMPS

Um outro fator, que agrava ainda mais a vulnerabilidade dos sistemas AMPS, está relacionado à tecnologia que o AMPS utiliza, ou seja, a natureza analógica do sistema torna difícil um esquema de defesa contra estes ataques. De outro lado, são amplamente conhecidas as técnicas de *hardware* para a construção amadora de equipamentos de escuta, assim como o *know how* disponível para cometer fraudes em sistemas AMPS. Por exemplo, existem na *Internet* repositórios com abundantes informações referentes às atividades de *phreakers (phone hacker)* [LUN97]. Também se encontram à venda, de forma ilegal, *scanners* de rádio recepção para interceptação de conversação telefônica e até equipamentos para capturar e gravar MIN e ESN de qualquer telefone celular, o que demostra, mais ainda, a vulnerabilidade dos sistemas AMPS [CEC96].

Ultimamente, no entanto, as operadoras desenvolveram mecanismos de segurança adicionais os quais não foram previstos na recomendação original TIA/EIA-533, sendo porém de alto custo. Destacamos, entre eles, os mecanismos de autenticação usando criptografia denominada PIN *(Personal Identification Number)*,

programas de inteligência artificial no gerenciamento da rede para detectar possíveis ataques ou fraudes e, recentemente, o mecanismo de autenticação *RF Fingerprint.* Neste mecanismo, o sistema mantém em um banco de dados as características particulares do sinal de rádio que é emitido por cada telefone celular, semelhante ao processo de impressão digital. Este método é baseado em uma tecnologia de análise digital, assim, a rede celular poderá distinguir o sinal emitido por cada telefone, identificando rapidamente se a ligação é fraudulenta ou não [CEC96].

4.2 Segurança em Sistemas de Telefonia Celular Digital USCD.

No aspecto de segurança em sistemas USCD, todos eles utilizam o padrão IS-41, portanto as características são bem semelhantes entre eles, razão pela qual realizamos um estudo único baseado num só padrão USCD, que neste caso recaiu sobre o TIA/EIA IS-95 pela disponibilidade da documentação completa deste padrão.

4.2.1 Autenticação em Sistemas USCD.

O documento TIA/EIA IS-95 [TIA94] define que "a autenticação é um processo no qual são trocadas informações entre a estação móvel e a estação base com o objetivo de confirmar a identidade da estação móvel". O processo de autenticação em sistemas USCD é mostrado na Figura 4.4. Este processo é baseado num mecanismo desafio/resposta junto ao uso de parâmetros secretos compartilhados e algoritmos de criptografia.

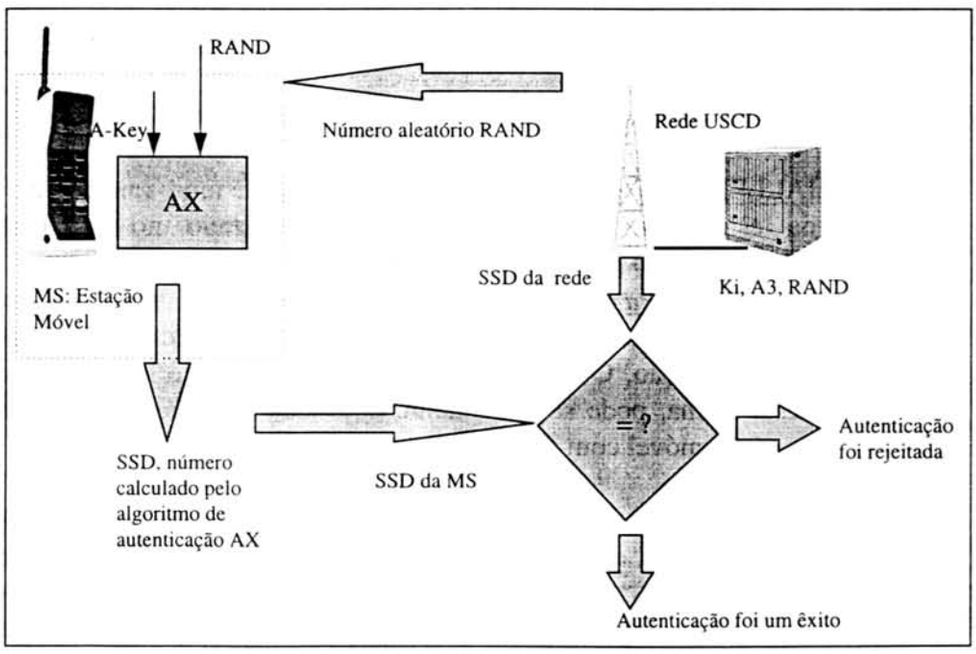

FIGURA 4.4- Processo de Autenticação em Sistemas USCD.

Os principais parâmetros utilizados no processo de autenticação são :

- A-Key. É um número de 64 bits utilizado na identificação da estação móvel. Este número fica armazenado na memória semi-permanente da estação móvel. O A-Key

é enviado pela operadora de telefonia celular ao assinante através do correio convencional e é armazenado na estação móvel de forma manual. O A-Key nunca é transmitido pelo ar e é conhecido pela estação móvel, o registro de localização de origem HLR e o centro de autenticação AC da rede.

- SSD (*Shared Secret Data*). O SSD é um número de 128 bits, guardado pela estação móvel de forma semi-permanente e está disponível para a rede. O SSD é derivado do A-Key durante o processo de autenticação através de um algoritmo criptográfico e um mecanismo desafio/resposta executado neste processo, no qual o SSD da estação móvel é comparado com o SSD, que a rede também guarda, e somente se estes coincidirem, a ligação é liberada (ver Figura 4.4). O SSD pode ser transportado do registro HLR (local) para o registro VLR (remoto) para fornecer autenticação quando a estação móvel está em *roaming*. O registro SSD é dividido em duas partes iguais de 64 bits cada, conformes mostra a Figura 4.5. O SSD_ A é utilizado nos processos de autenticação enquanto o SSD_B é utilizado para suportar privacidade de voz em CDMA e confidencialidade de mensagens em CDMA e no modo analógico.

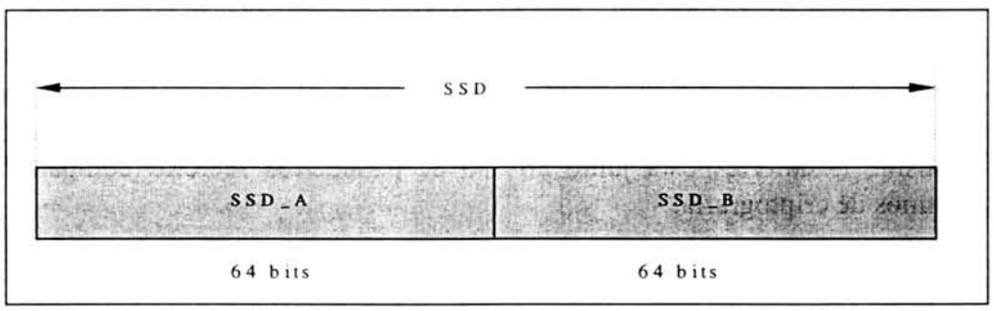

FIGURA 4.5 - Estrutura do SSD - *Shared Secret Data*.

- RAND_CHALLENGE (*Random Challenge Memory*). É uma variável de 32 bits guardada na estação móvel e na rede, e é utilizado no mecanismo de desafio/resposta durante o processo de autenticação.
- COUNT (*Call History Parameter*).Contador de 64 bits mantido na estação móvel em memória semi-permanente, e também na rede, servindo como parâmetro adicional de autenticação. O COUNT armazena o número de ligações que foram efetuadas; desta forma, pode ser facilmente detectada uma fraude ao comparar o COUNT da estação móvel com o COUNT da rede.

Os algoritmos de autenticação são descritos no documento "*Common Cryptographic Algorithms*", enquanto os parâmetros de entrada, utilizados nestes, são descritos no documento "*Interface Specification for Common Cryptographic Algorithms*". Ambos os documentos são de acesso restrito, só tem acceso os fabricantes devidamente credenciados pela CTIA (*Cellular Telecommunications Industry Association*), e não estão disponíveis no documento genérico TIA/EIA IS-95.

4.2.2 Privacidade em Sistemas USCD.

O sigilo dos dados, sejam eles de usuário ou informação de sinalização, é garantido através de processos de criptografia. Em sistemas USCD, isto é feito através

de algoritmos de criptografia também usados no processo de autenticação. Isto significa que, o canal por onde trafegam voz ou dados, sob forma digita é criptografado, garantindo desta forma a privacidade. No documento original do TIA/EIA IS-95 o tamanho da chave o algoritmo de criptografia são de acesso restrito.

4.3 Segurança em Sistemas de Telefonia Celular Digital GSM.

Os aspectos de segurança do GSM são detalhados nas recomendações do ETSI através dos documentos 02.09 *Security Aspects*, 02.*17 Subscriber Identity Modules*, 03.20 *Security Related Network Functions* e 03.21 *Security Related Algorithms* [MAR95]. A segurança no GSM toma em conta os seguintes aspectos: autenticação do usuário, encriptação dos dados e confidencialidade da identidade e localização do assinante. Os parâmetros de segurança são armazenados em três diferentes elementos do sistema: no SIM (*Subscriber Identity Module*), na estação móvel MS e no subsistema de rede NSS. O SIM é um cartão inteligente (*smartcard*), semelhante ao cartão de crédito, que deve ser inserido toda vez que o assinante quiser utilizar uma MS, fornecendo assim a mobilidade pessoal. O SIM fornece ao MS a identidade do usuário, e sem ele o MS não é operável (exceto para ligações de emergência). A Figura 4.6 mostra a distribuição dos parâmetros de segurança na rede GSM.

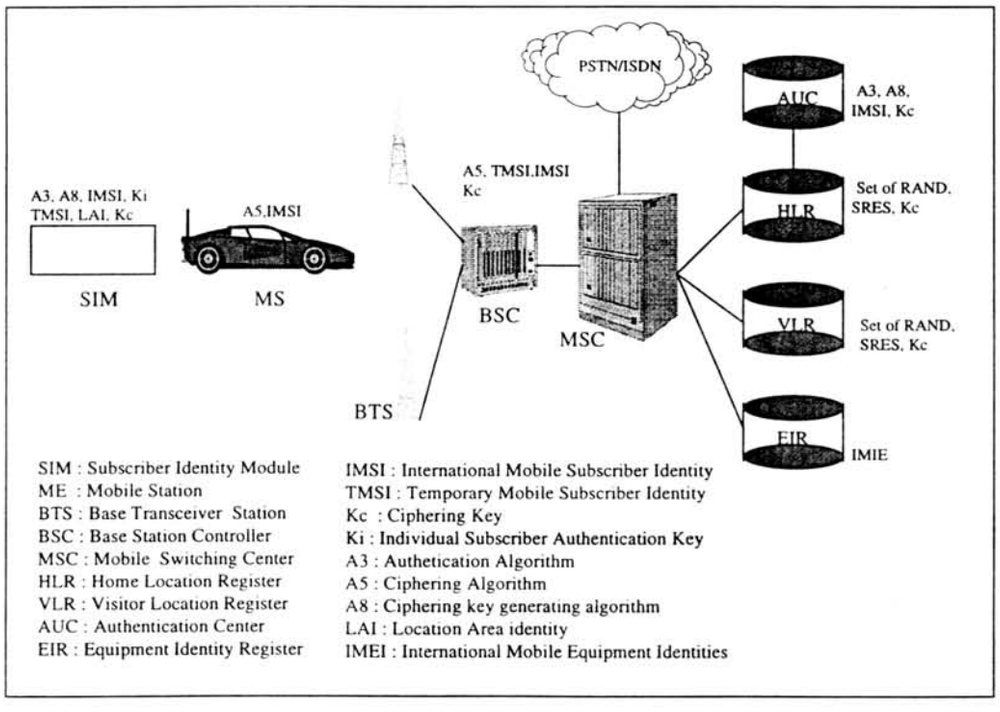

FIGURA 4.6 - Distribuição dos parâmetros de segurança na rede GSM [LUN97].

4.3.1 O processo de autenticação no GSM.

A rede GSM realiza o processo de autenticação do assinante através do SIM usando um mecanismo tipo desafio/resposta. Este processo começa quando um número aleatório RAND (*Random Number*) de 128 bits é transmitido pela NSS para a MS. A chave Ki de 128 bits armazenada no SIM, e o número RAND, são usados como

valores de entrada para o algoritmo de autenticação A3 (também armazenado no SIM), o qual calcula o número SRES (*Signed Response*) de 32 bits. Este número é enviado para a rede GSM, onde se repete o cálculo com os mesmos valores de entrada. O valor SRES recebido é comparado com o valor calculado localmente, se os dois coincidem, então o processo de autenticação teve êxito e a MS continua ligada; se o valor não corresponde, a conexão é interrompida e a falha de autenticação é reportada. Este processo é mostrado num fluxograma resumido na Figura 4.7.

Note-se que o cálculo do SRES é feito, internamente, no SIM. Isto fornece uma segurança adicional, porque as informações críticas, como o Ki e o A3, não são nunca liberadas do SIM durante o processo de autenticação

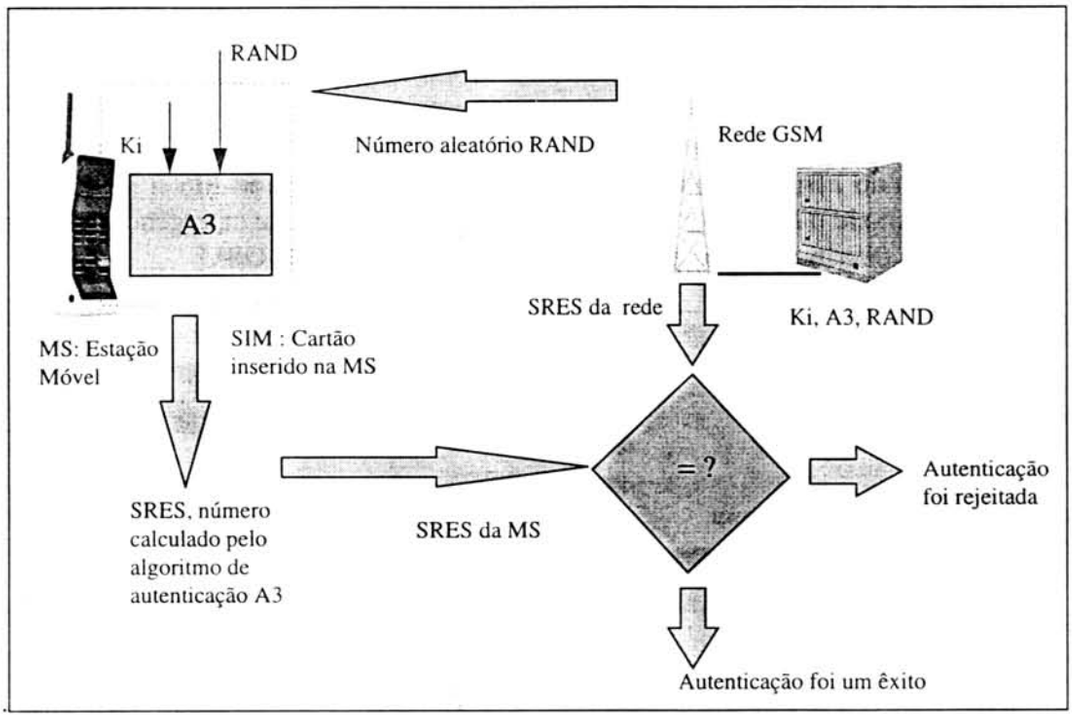

FIGURA 4.7 - Processo de Autenticação no GSM.

4.3.2 O processo de confidencialidade dos dados no GSM.

O SIM contém o algoritmo A8 para produzir a chave de criptografia Kc de 64 bits. No processo para obter a chave Kc também é usado o mesmo número aleatório RAND e a chave Ki usados no processo de autenticação. Assim, Kc é usado para criptografar e decriptografar os dados entre a MS e a rede GSM. Um nível de segurança adicional está previsto pelo fato de que a chave de criptografia é trocada de tempos em tempos, tornando o sistema ainda mais resistente a ataques. A chave Kc pode ser trocada em intervalos regulares ou, quando necessário, por considerações de segurança da rede. A Figura 4.8 mostra como é realizado o cálculo da chave Kc. De forma similar ao processo de autenticação, a chave Kc é processada internamente no SIM, portanto a informação Kc nunca é revelada ou transmitida pelo canal.

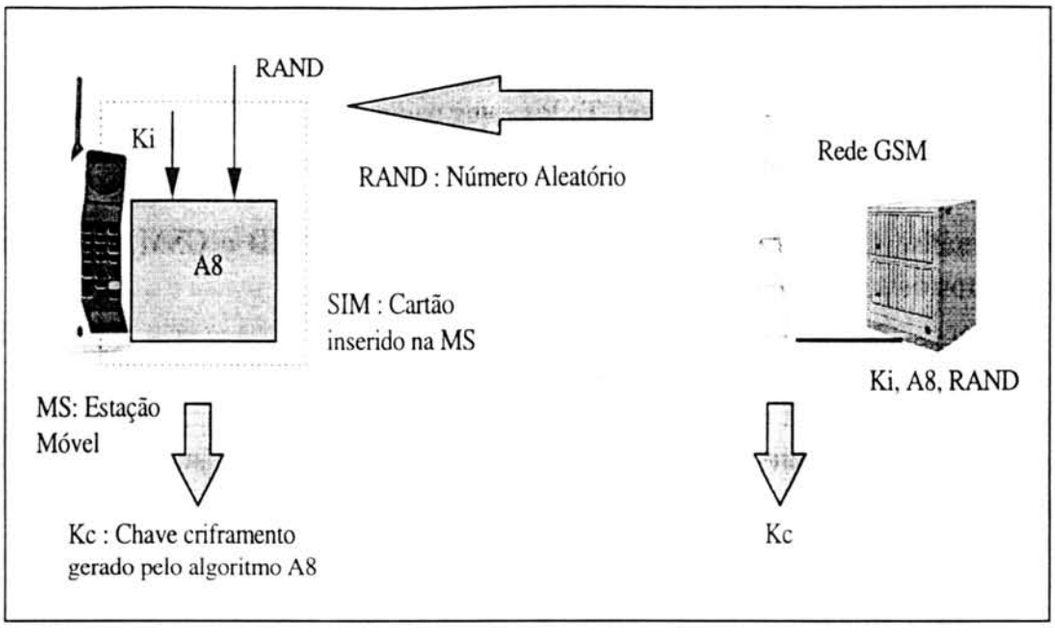

FIGURA 4.8- Processo do cálculo da chave Kc no GSM.

A encriptação da voz e dados entre o MS e a rede é feita através do algoritmo de criptografia A5 (que está armazenado dentro da MS). A comunicação cifrada é iniciada através de um pedido, de modo cifrado, à rede GSM. Uma vez recebido este pedido, a MS começa a criptografar e decriptografar os dados usando o algoritmo A5 e a chave Kc. A Figura 4.9 mostra este processo.

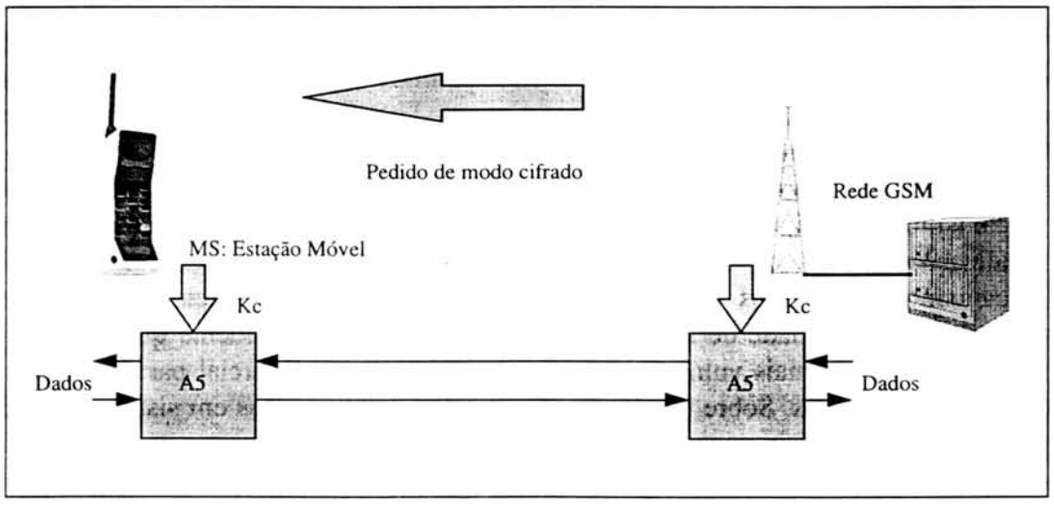

FIGURA 4.9 - Início do modo de comunicação cifrada no GSM.

4.3.3 Confidencialidade da identidade e localização do assinante no GSM.

Para manter em sigilo a identidade do assinante é usado o parâmetro TMSI (*Temporal Mobile Subscriber Identity*). O TMSI é enviado para a MS depois que os procedimentos de autenticação e encriptação estiverem concluídos. O MS confirma a recepção do TMSI, o qual, porém, é valido somente na área de localização em que está sendo usado. Portanto, será trocado cada vez que a MS muda de BSC. Para manter em sigilo a localização do assinante é usado o parâmetro de Identidade Internacional do Assinante ou IMSI (*International Mobile Subscriber Identity*), o qual contém

informações sobre a posição do usuário. Para comunicações fora da área da rede origem, além do TMSI, é necessário o parâmetro de Identificação de Localização de Área LAI *(Location Area Identity)*. Todos estes parâmetros são transmitidos, de forma encriptada, usando o algoritmo A5 e ficam armazenados no SIM e na NSS.

4.4 Análise Comparativa entre os Sistemas AMPS, USCD e GSM, quanto aos aspectos de segurança.

Analisando os aspectos básicos de segurança do sistema AMPS, conclui-se que os sistemas de telefonia celular baseados no AMPS são altamente vulneráveis, pelo fato de que durante o processo de autenticação são trocados os parâmetros críticos de identificação MIN e ESN pelo canal de RF, que não é protegido, podendo ser facilmente capturados e copiados para serem utilizadas em um outro telefone (clone).

Nos sistemas de telefonia celular USCD e GSM, a possibilidade de fraudes e ataques é mais difícil, pelo fato de que possuem poderosos mecanismos de segurança inerentes à própria camada física. Todos estes sistemas, por exemplo, fazem uso de sofisticadas técnicas de modulação do canal digital (GSMK, π/4DQPSK, e BPSK/QPSK) e usam complexos processos de codificação de voz e dados. Qualquer tentativa de ataque sobre os sinais destes sistemas requer equipamentos altamente especializados e, o mais importante, como já foi mencionado, estão previstos nestes sistemas técnicas de autenticação e privacidade que utilizam algoritmos de criptografia, o que garante ainda mais a segurança destes sistemas [WIL95], [MAR95].

Na Tabela 4.1 é apresentado um quadro comparativo resumindo as principais caraterísticas de segurança adotados nos padrões de telefonia celular digital e analógico AMPS (celular analógico americano), USCD (celular digital americano) e GSM (celular digital europeu). São comparados os mecanismos de autenticação e privacidade, resultando que os sistemas digitais são os mais seguros, pois usam mecanismos de criptografia. Na comparação dos mecanismos de identificação e localização, o sistema GSM, é o mais seguro, pelo fato de que são utilizados mecanismos específicos como TMSI e o LAI, abordados no item 3.3. Quando é comparado a facilidade de interceptação do sinal de RF, é evidente que os sistemas analógicos são os mais vulneráveis, pela disponibilidade comercial para amadores de *scanners* analógicos. Sobre os algoritmos de criptografia usados em sistemas digitais, pouco se conhece. São de acesso restrito, ou seja, só disponíveis para os fabricantes de equipamentos centrais, telefones, comutadores, etc, o mesmo acontecendo com as chaves empregadas nestes sistemas. No entanto, recentemente foi filtrada informação sobre as caraterísticas do algoritmo A5 (usado para a criptografar a voz em sistemas GSM) e do tamanho da chave do mesmo, chegando a ser divulgada pela *Internet*. De forma similar, a pouco tempo atras, foi divulgado também na comunidade, que um *hacker* havia conseguido quebrar este mesmo algoritmo. Ainda assim, como já foi mencionado, a quebra de um algoritmo em um sistema como o GSM, não significa a quebra do sigilo do sistema pelo fato de usar vários parâmetros, como por exemplo os parâmetros temporais que são trocados de tempo em tempo.

TABELA 4.1 Comparação dos aspectos de segurança em sistemas de telefonia celular [LUN97].

	AMPS	GSM	USCD (IS-95 e IS-136)
Mecanismos de autenticação.	Baseado no uso de parâmetros armazenados dentro da estação móvel e que são transmitidos pelo ar sem nenhuma proteção. Processo que coloca em risco a segurança do sistema.	Procedimento desafio/ resposta, na qual os parâmetros de identificação não são transmitidos pelo ar, portanto, não coloca em risco a segurança do sistema.	Procedimento desafio/ resposta, na qual os parâmetros de identificação não são transmitidos pelo ar, portanto, não coloca em risco a segurança do sistema.
Mecanismos de privacidade.	Não utiliza.	Usa criptografia para proteção dos dados trafegados entre o assinante e a rede além dos dados de sinalização.	Usa criptografia para proteção dos dados trafegados entre o assinante e a rede além dos dados de sinalização.
Mecanismos de proteção da identidade e localização do assinante.	Não utiliza.	Usa criptografia e procedimentos de identificação temporal.	Não disponível.
Facilidade de Interceptação e decodificação dos sinais de RF.	Fácil. *Scanners* que rastreiam e interceptam sinais analógicos, são fáceis de construir ou comprar.	Difícil. Usa canal digital, difícil de ser demodulado e decodificado por *scanners* simples.	Difícil. Usa canal digital, difícil de ser demodulado e decodificado por *scanners* simples.
Utilização de algoritmos de Criptografia.	Não utiliza.	Usa três algoritmos de chave privada, denominados A3, A8, e A5. Este último é um *stream cipher*, ou seja, é apoiado por mecanismos da camada física. Todos estes algoritmos são de acesso restrito.	Usa algoritmos de chave privada, os quais estão severamente protegidos por leis de *Copyright*, portanto de acesso restrito.
Parâmetros de entrada ou chaves para os algoritmos de criptografia.	Não tem.	Ki, RAND são de 128 bits, e o Kc tem 64 bits. Parte do algoritmo A5 foi pública na *Internet*, o tamanho é 40 bits. Se desconhece o tamanho dos demais algoritmos.	A-Key é de 64 bits. Se desconhece o tamanho de chave dos algoritmos.
Método de disponibilização da chave.	Não tem.	A chave Ki já bem embutido no SIM, e nunca é transmitido pelo ar.	A chave A-Key é enviado pela operadora ao assinante por correio convencional. O qual é armazenado no MS de forma manual, e nunca é transmitido pelo ar.

5 Segurança em Sistemas PCS

Os sistemas PCS deverão oferecer serviços de comunicação de forma ubíqua (a qualquer tempo e de qualquer lugar) e com uma alta capacidade de assinantes. Para alcançar estas metas, os fabricantes e projetistas estão diante de inúmeros desafios. Entre estes se destacam a questão da mobilidade do terminal, a mobilidade pessoal, o *roaming* universal, o controle de acesso e a proteção das informações do assinante. Os últimos dois desafios estão relacionados aos aspectos de segurança, e podem ser resumidos em duas palavras: Autenticação e Privacidade ou A&P [BRO95]. A&P, na realidade, fazem parte de um mesmo processo porque a obtenção de uma chave de sessão para criptografar é, freqüentemente, parte integrante do processo de autenticação.

5.1 Caraterísticas de Autenticação e Privacidade desejadas em Sistemas PCS.

Podemos mencionar como características desejáveis de A&P em Sistemas PCS os seguintes [LUN97]:

a) Estabelecimento de uma chave de sessão. Os sinais de rádio transmitidos por um canal de RF em sistemas *cordless* ou celular podem ser interceptados, facilmente, por *scanners* disponíveis comercialmente. Em sistemas digitais avançados este problema ainda não existe, porém, cedo ou tarde a tecnologia de *scanners* digitais também estará disponível amplamente. Para proteger as mensagens, estas deverão ser transmitidas em forma cifrada. Durante o processo de autenticação uma chave secreta de sessão deverá ser negociada entre a rede e a estação móvel. Esta chave de sessão pode ser utilizada durante um certo tempo, após o qual, por questão de segurança, deverá ser trocada. A tendência é que, os protocolos de segurança em PCS forneçam uma nova chave de sessão de tempos em tempos ou para cada nova sessão.

b) Sigilo da identidade e localização do assinante. Em sistemas de telefonia tradicional, um assinante está conectado a uma central telefônica através de um par de fios, desta forma, o assinante é automaticamente identificado pelo número de telefone associado. No entanto, em ambientes sem fio, não existe esta associação física portanto, o assinante de alguma maneira tem que fornecer sua identificação para sua verificação pela rede. Este processo, também, deverá fornecer informações referentes a sua localização, e deverá ser feito de forma segura, para que tanto a identidade do assinante como a sua localização, não corram o risco de serem alvo de ataques por parte de *phreakers*.

c) Autenticação mútua. Em sistemas celulares da primeira geração, o pedido de uma ligação por parte de um *roamer* é concedido imediatamente, ao mesmo tempo em que o processo de autenticação está em andamento. Devido a isto, muitos pedidos de ligação de telefones fraudulentos são completados antes de serem detectados. Isto provoca retardos no processo de autenticação, causados principalmente por falta de um apropriado protocolo de comunicação entre as operadoras de telefonia celular, acarretando prejuízos incalculáveis. Este problema poderá ser facilmente contornado com o estabelecimento de um acordo entre as operadoras, de modo que

o processo de validação seja concluído antes que a ligação seja completada. Os novos sistemas emergentes utilizam modernas técnicas de criptografia para eliminar este tipo de fraudes.

d) Serviço não rejeitado. Para o provedor de serviços é desejável que o assinante não possa recusar uma conta por serviços prestados. Por outro lado, o assinante não deverá ser onerado por serviços não solicitados, ou não utilizados. Teoricamente, ambos os problemas podem ser resolvidos através do uso de uma assinatura digital, o que pode ser obtido com as técnicas de criptografia assimétricas [LIN95].

5.2 Requisitos dos Mecanismos de Criptografia para Sistemas PCS.

Para proporcionar um apropriado processo de A&P em sistemas PCS será necessário que os algoritmos de criptografia sejam apropriados e compatíveis com a interface de rádio, entre outras considerações [WIL95], [LIN95]. Na escolha dos algoritmos deverão ser levados em conta os seguintes requisitos:

a) Requisitos em relação à privacidade. Os mecanismos de criptografia deverão proporcionar privacidade durante a troca de informações confidenciais, através de um canal não confiável. É necessário que todos os dados sejam enviados de forma segura, tanto da conversação, como da localização e identificação do assinante. Assim sendo, são aceitáveis, somente, algoritmos com chaves superiores a 56 bits.

b) Requisitos em relação à robustez contra roubos e fraudes. A criptografia deverá reduzir ou dificultar o uso de um terminal roubado, assim como, o projeto do terminal deverá ser resistente ao *cloning*. Para evitar o *cloning* é necessário que informações críticas não sejam comprometidas, seja pela troca em canais não confiáveis no processo de roaming, ou, devido a bancos de dados não devidamente protegidos.

c) Requisitos em relação ao canal de rádio. O sistema criptográfico deverá levar em conta o ambiente hostil de rádio, caracterizado por uma alta taxa de erros causados, principalmente, por desvanecimentos do sinal, caminhos múltiplos, ruído eletromagnético, entre outros. Outro aspecto, particularmente crítico, é o processo de *handoff* dos sistemas celulares onde se pode perder facilmente a sincronização.

d) Requisitos em relação à vida do sistema. Em telefonia, a vida média de um sistema é muito alta; por exemplo, o sistema AMPS foi projetado no inicio dos anos 70 e ainda possui uma expectativa de vida útil de muitos anos. Donde se conclui que os mecanismos de criptografia a serem implementados deverão ter uma garantia de não serem quebrados em pelo menos 20 anos.

e) Requisitos em relação ao mercado. O sistema criptográfico a ser adotado deverá ser produzido em larga escala como um produto de consumo, isto é, deverá ser produzido com custos muito baixos. Além do mais, novas regras comerciais de importação e exportação para algoritmos de criptografia deverão ser estabelecidas pelos governantes.

f) Requisitos em relação aos aspectos físicos. Deverão ser levados em conta aspectos como: espaço, tamanho, peso, potência, dissipação de calor, velocidade do

processamento do *chip* e facilidade de ser gravado em memórias permanentes, semi-permanentes ou temporária.

g) Requisitos em relação a aspectos legais. O governo pode autorizar judicialmente o grampeamento de certas ligações e, portanto, os mecanismos criptográficos deverão ser projetados levando em conta também este aspecto. Uma alternativa são os algoritmos fortes administrados por uma entidade confiável do governo que mantenha o controle do repositório das chaves; esta modalidade é conhecida como *key scrow* (guarda chaves) pelo governo dos EUA.

5.3 Modelo AKA para Autenticação e Privacidade em Sistemas PCS.

Do ponto de vista do projetista, o controle de acesso e a obtenção de uma chave de sessão podem ser englobados numa única atividade denominada de AKA (*Authentication Key Agreement*) segundo [BEL93] e [BRO95]. O modelo e protocolo AKA é constituído de três processos seqüenciais:

1. Processo de distribuição e troca dos parâmetros de segurança. Neste processo é feita a distribuição e troca de alguns parâmetros de segurança entre o assinante e a rede (como a chave Ki e os números RAND e SRES no GSM), para que o assinante ou a estação móvel possam executar, posteriormente, os processos de autenticação e, assim, adquirir legitimidade perante à rede.

2. Processo de autenticação. Neste processo é constatada a autenticidade do assinante ou da estação móvel. Uma vez devidamente autenticado, o usuário é registrado na rede, que não, necessariamente, precisa ser a rede de origem (*home network).* Quando em rede visitada *(visited network)*, serão trocados somente subconjuntos restritos de credenciais. Isto é necessário porque a divulgação de dados secretos da estação móvel (como o Ki do GSM e o A-Key do IS-95) pode, eventualmente, comprometer a segurança do sistema. De qualquer modo, continua a necessidade de que a rede visitada seja capaz de distinguir um usuário legítimo, baseada somente nesta informação parcial (no caso do GSM, a chave Kc, e os números RAND e SRES).

3. Processo de obtenção de chaves para troca de dados. Neste processo do protocolo AKA é executada uma negociação, entre a rede e o usuário, para obtenção de uma chave de criptografia (chave Kc no GSM), que permitirá a proteção do processo de comunicação de dados.

Uma das características do protocolo AKA é que ele pode ser implementado segundo um esquema de distribuição das chaves, que pode ser pública ou privada; por exemplo, recentemente métodos de A&P, usando protocolos AKA de chave pública, foram propostos por pesquisadores independentes e pelo padrão PACS [NOE96], [BRO95]. Protocolos AKA de chave privada são adotados, atualmente, pela maioria dos sistemas de telefonia celular de segunda geração, incluindo os sistemas de telefonia celular GSM e USCD. Atualmente, o AKA é um protocolo para A&P que está sendo examinado pelos organismos internacionais de padronização dos sistemas PCS.

A Figura 5.1 apresenta um modelo geral do protocolo AKA com a seqüenciação dos três principais processos executados.

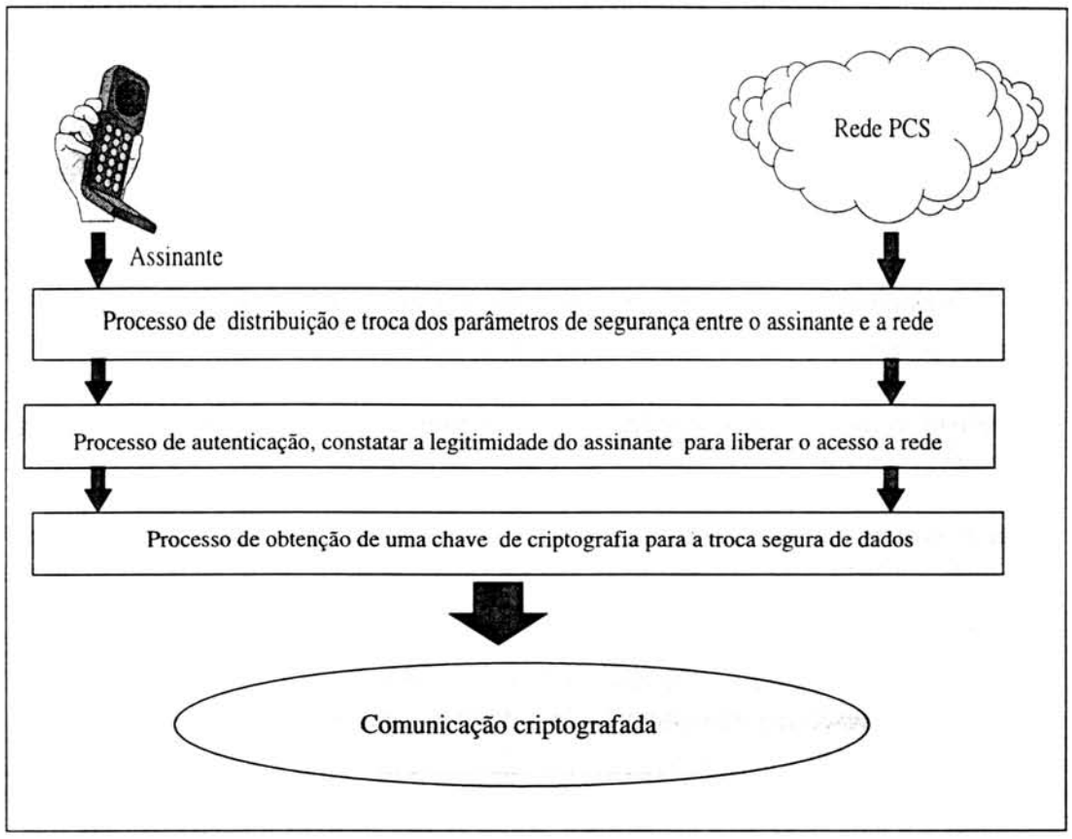

FIGURA 5.1 - Os três processos do modelo AKA [BRO95].

5.4 Padronização dos aspectos de segurança em Sistemas PCS.

Os Sistemas PCS, que estão previstos para operar na banda de 2 GHz, provavelmente, adotarão técnicas de A&P baseadas no modelo AKA, semelhantes aos encontrados nos sistemas de telefonia celular GSM e USCD. Atualmente estão sendo consideradas, também, técnicas baseadas num mecanismo híbrido de chave pública e chave privada, [BRO95], [LIN95]; todos, porém, seguem o modelo AKA descrito anteriormente. Na Tabela 5.1 estão resumidos alguns aspectos de segurança de cada uma das propostas de padronização para sistemas PCS de acordo com o JTC.

TABELA 5.1 - Padrões de segurança propostos para Sistemas PCS pelo JTC.

Padrão	J-STD-017	J-STD-008	J-STD-014	J-STD-011	J-STD-007	DECT	J-STD-015
Modelo de Segurança adotado	AKA GSM e USCD	AKA USCD	AKA USCD e híbrido	AKA USCD	AKA GSM	Propieta-rio	Ainda não definido

6 A Interconexão com Redes PCS

É um fato que os serviços PCS serão fornecidos por múltiplas redes regionais de PCS, cada uma gerenciada por diferentes concessionárias, e, muito provavelmente, usando padrões distintos. Obviamente, estas redes deverão interconectar-se para oferecer o *roaming* automático, o que exigirá a implementação de uma interface para facilitar a interoperabilidade entre elas. Atualmente, a interconexão entre as redes de telefonia celular é feita usando a rede pública comutada (PSTN); em outros casos, como na rede GSM, é feita através de uma interface especial conhecida como IWF *(Interworking Function)* [VAR96].

O principal objetivo dos sistemas PCS é oferecer a mobilidade pessoal e do terminal, portanto, além de permitir a interconexão das redes PCS com redes similares, (redes homogêneas) também será necessário que os sistemas PCS interajam de forma compatível com as diversas redes de telecomunicações fixas e móveis, atualmente existentes, como as redes públicas de telefonia comutada (PSTN), a rede digital de serviços integrados (ISDN), as redes de telefonia celular, a telefonia *cordless*, os sistemas *paging*, as redes WLAN *(Wireless Local Area Network),* entre outras, razão pela qual também será necessário o uso de uma interface de interconexão. Segundo [HUS96] e [GAR96] esta interface esta sendo denominada como IIF (*Interworking Interoperability Function*), e que devera ser projetada obedecendo a os protocolos de sinalização SS7 (*Signaling System #7*) e o MAP (*Mobile Application Part*). Na Figura 6.1 representa a interconexão de redes heterogêneas com redes PCS.

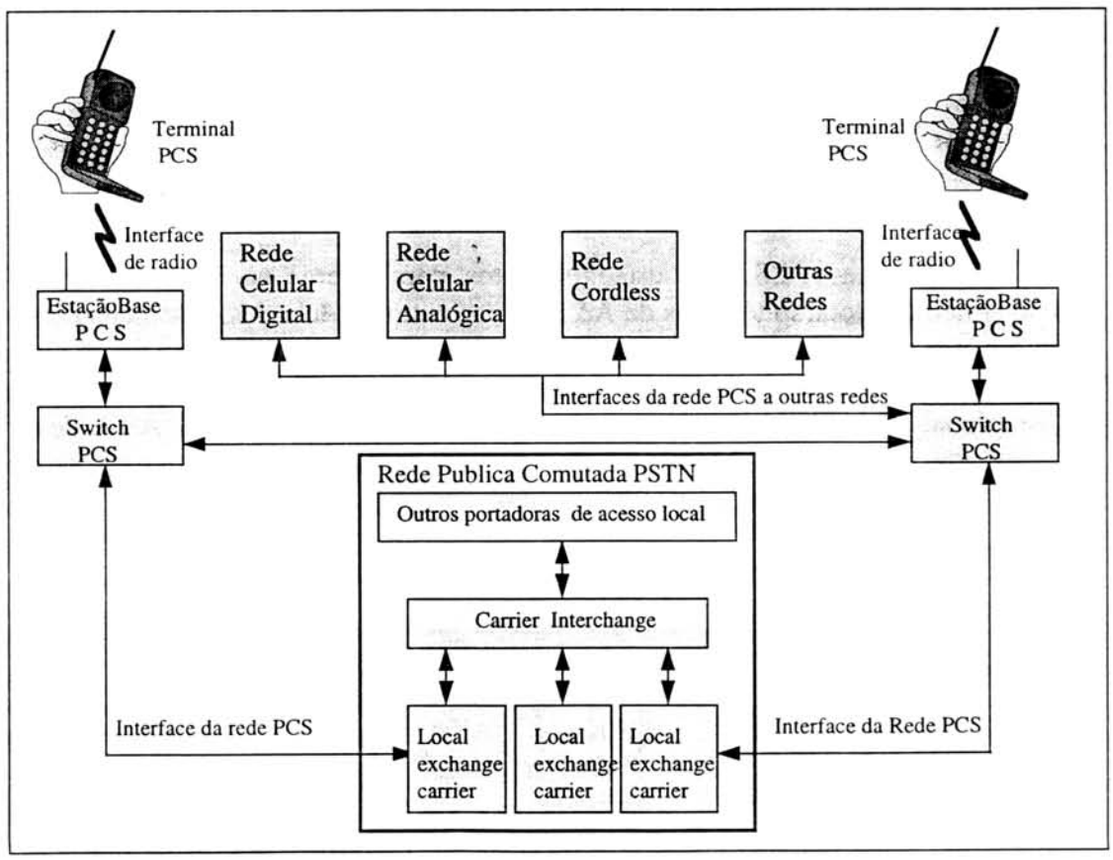

FIGURA 6.1 - Interconexão de redes heterogêneas com sistemas PCS.

Desta forma, os sistemas PCS oferecerão uma espécie de integração de serviços, mesmo que sejam operados por diferentes concessionárias e usem distintos padrões. Aqui há um aspecto importante a considerar: a troca de serviço de uma rede para outra deverá ser transparente para o assinante, o que significa que o sistema será capaz de manter a conexão sem a necessidade de trocar de terminal. Para que isto seja possível, o assinante deverá ter um único *handset* do tipo *multimode*, possibilitando assim a operação em múltiplos ambientes de rede.

6.1 Segurança na interconexão de redes heterogêneas com Sistemas PCS.

As vantagens da interconexão com as redes heterogêneas, ou seja, a mobilidade pessoal e o *roaming* universal, colocam aos sistemas PCS numa situação extremamente vulnerável a fraudes e ataques [LI95]. Na interconexão de Sistemas PCS com redes heterogêneas são considerados diferentes padrões, cada um com níveis de proteção distintos e, portanto, fica evidente que neste esquema o controle de acesso e o gerenciamento da rede ficarão ainda mais complexos [LIN95] e [GAR96].

Na Tabela 6.1 é mostrada uma analise comparativa da segurança na interconexão para o caso de sistemas PCS com redes celulares. Nesta analise é considerado um sistema PCS baseado em protocolos do modelo AKA, e as redes de telefonia celular : AMPS, USCD e GSM. Usando dois tipos de interfaces; a rede PSTN, e uma do tipo IIF, são apresentadas duas situações de interconexão: uma delas; quando o *handset* PCS está operando em *roaming*, e a outra quando o *handset* PCS está numa comunicação ponto a ponto com um usuário de uma rede diferente. Por exemplo, no primeiro caso apresentado (PCS-PSTN-AMPS), um *handset* PCS dualmode (AMPS e PCS AKA) esta operando em *roaming* numa rede AMPS, portanto a autenticação, privacidade e localização sera vulnerável pelo fato de estar trabalhando no modo AMPS, e quando a interconexão seja ponto a ponto, ou seja o *handset* PCS operando na sua rede de origem em comunicação com um usuário da rede AMPS, a privacidade sera perdida, pois num segmento da interconexão é usada a infra-estrutura da rede AMPS, sendo fácil o grampeado. Similarmente são apresentado outros casos, os mesmos que são mostrados na Tabela 6.1. Todo isso nos leva a considerar dois aspectos importantes: primeiro, adotar sistemas PCS com mecanismos de segurança do tipo AKA, e usar as interfaces de interconexão do tipo IIF.

TABELA 6.1. Analise comparativa da segurança na interconexão de redes PCS com redes heterogêneas [LUN97].

Interconexão de Redes Rede-interface-Rede	Autenticação (Usuário em *Roaming*)	Privacidade (Usuário em *Roaming*)	Localização (Usuário em *Roaming*)	Privacidade do usuário na comunicação ponto a ponto
PCS-PSTN-AMPS	Vulnerável	Vulnerável	Vulnerável	Vulnerável
PCS-PSTN-USCD	Segura	Segura	Vulnerável	Vulnerável
PCS-PSTN-GSM	Segura	Segura	Segura	Vulnerável
PCS-PCS (AKA)	Segura	Segura	Segura	Segura
PCS-IIF-AMPS	Vulnerável	Vulnerável	Vulnerável	Vulnerável
PCS-IIF-GSM	Segura	Segura	Segura	Segura
PCS-IIF-USCD	Segura	Segura	Vulnerável	Segura

7 Protocolos de Sinalização

No Capítulo 6 foi revisado a questão da segurança no contexto da interconexão de sistemas PCS com redes heterogêneas. Também foi mostrado a importância do uso da rede inteligente IN (*Intelligent Network)* baseado em mecanismos de sinalização por canal comum SS7 e MAP, para projetar uma interface de interconexão e interoperabilidade.

No capítulo a seguir, dentro do contexto da interconexão e interoperabilidade entre as redes fixas atuais com as futuras redes móveis do tipo PCS, serão revisados as características funcionais dos protocolos de sinalização SS7 e MAP (*Mobile Application Part*), como requisitos importantes na solução deste problema.

As centrais telefônicas são interligadas através de redes de telecomunicações, que utilizam protocolos próprios em funções como estabelecimento de ligações, controle, tarifação, supervisão, gerenciamento e operação da rede, além de troca de informações necessárias para o processamento de aplicações distribuídas. O conjunto destes protocolos são conhecidos como o sistema de sinalização SS7 (*Signaling System #7*) [MOD90].

A sinalização telefônica, que consiste numa forma de comunicação entre as centrais telefônicas, foi inicialmente implementada utilizando os próprios canais de voz para transportar estas informações na forma de tons ou pulsos elétricos de forma rudimentar. A rede de sinalização conhecida como Sinalização por Canal Comum SS7, foi especificada e padronizada mundialmente pela ITU, baseada numa rede de dados de alto desempenho que transporta, entre outras informações, a sinalização telefônica. Atualmente, a maioria dos países esta em fase de implantação desta tecnologia de sinalização por canal comum [CAM96] em suas plantas de telecomunicações.

Os protocolos de sinalização são organizados segundo uma estrutura em níveis de forma análoga ao modelo de arquitetura de protocolos para sistemas abertos RM-OSI, e que será revisado a seguir.

7.1 O Modelo RM-OSI.

A ISO (*International Organization for Standardization*) é uma organização internacional fundada em 1946, que tem por objetivo a elaboração de padrões internacionais. No documento ISO 7498, denominado RM-OSI (*Opem System Interconnection Reference Model*), é fornecido uma base comum que permite o desenvolvimento coordenado de padrões para interconexão de sistemas.

O fato de dois sistemas distintos seguirem o RM-OSI não garante, necessariamente, que eles possam trocar informações entre si, pois o modelo permite que sejam usadas diferentes opções de serviços/protocolos para as várias camadas. Essa flexibilidade, pode levar a situações onde dois sistemas que utilizam opções de

serviços/protocolos em conformidade como o RM-OSI, não conseguem se comunicar, porque as opções adotadas são incompatíveis.

Para que dois sistemas quaisquer possam trocar informações é necessário que escolham opções compatíveis de serviços/protocolos para todas as camadas do modelo. Com o objetivo de definir grupos de opções de serviços/protocolos padronizados, a ISO elaborou o conceito de perfis funcionais. Se dois sistemas seguirem o mesmo perfil funcional eles, garantidamente, irão comunicar-se, pois nesse caso as opções de serviço/protocolo adotadas serão compatíveis.

O Modelo OSI possui sete níveis de protocolos, conforme são mostrados na Figura 7.1. A idéia básica da estruturação em camadas do RM-OSI é de que cada uma das sete camadas fornece serviços de comunicação, com um certo grau de confiabilidade, à camada imediatamente superior. Os serviços pelas camadas inferiores são sucessivamente ampliados e aperfeiçoados, de modo que na camada mais superior seja oferecido um conjunto de serviços adequado para suportar as diversas aplicações.

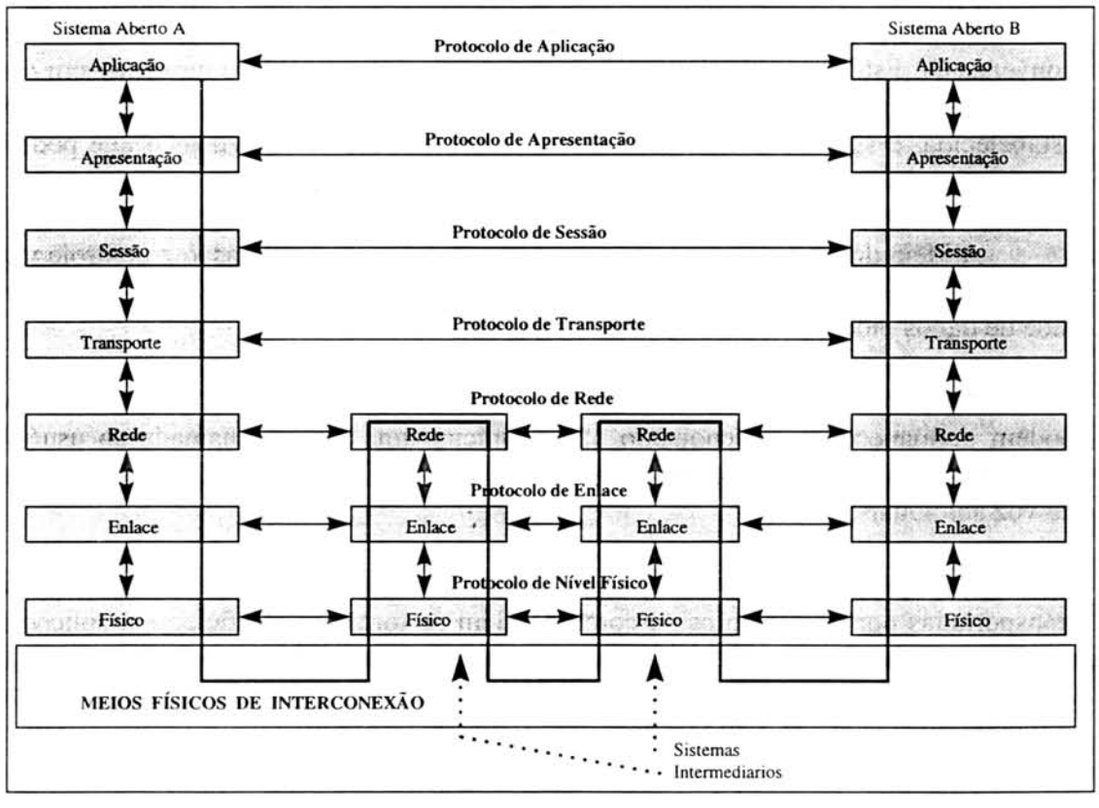

FIGURA 7.1. Modelo de Referência ISO [TAM96].

As entidades de uma camada N, num determinado sistema, "conversam" com as entidades pares na camada N num outro sistema, conforme ilustrado pelas linhas tracejadas na Figura 7.1. As regras e convenções usadas nesta "conversação" são conhecidas coletivamente como protocolos da camada N.

É importante observar que, na realidade, as unidades de dados envolvidos na comunicação entre dois sistemas não são transferidas diretamente de uma camada N num sistema para a camada N no outro, exceto na camada mais inferior. Em vez disso,

cada camada passa dados e informação de controle para a camada imediatamente inferior até chegar à mais baixa. Nesta última camada, existe uma comunicação "física" (através dos meios físicos de transmissão) com a camada equivalente em outro sistema. A conversação do lado do sistema receptor processa-se de maneira inversa, isto é, os dados e a informação de controle passam sucessivamente através de camadas até chegarem ao processo destinatário da camada mais alta. Entre cada par de camadas adjacentes existe uma interface que define as operações das primitivas e os serviços que a camada inferior oferece à camada superior. A comunicação entre dois sistemas pode envolver sistemas intermediários atuando apenas ao nível das camadas inferiores (Física, Enlace e Rede).

7.2 Sistema de Sinalização Número 7.

Os primeiros sistemas de sinalização utilizados nas centrais automatizadas se basearam totalmente na codificação de informações bastante simples em sinais (pulsos) elétricos denominado sinalização SM (*Single-Frequency*), posteriormente, em combinações de tons audíveis denominado sinalização MF (*Multi-Frequency*), onde são transportados pelo próprio canal de voz, ou seja, pelo mesmo caminho da conversação. Estes tipos de sistemas ocupam canais de voz desde o momento em que o originador inicia a discagem, mesmo que a chamada efetiva não chegue a ser estabelecida, e são muito limitados quanto à diversidade de informação que podem representar.

A idéia do SS7, é fazer com que as informações de sinalização e controle não transitem no próprio canal de voz da conexão correspondente, e sim através de uma rede de dados independente, de alto desempenho.

Separando-se em uma rede própria os circuitos de sinalização, os canais de voz podem permanecer livres enquanto não se iniciar uma efetiva chamada ao usuário distante, aumentando a disponibilidade de canais de voz sem a instalação de circuitos de voz adicionais.

Na rede SS7, várias informações distintas podem ser empacotadas e então transportadas por um único canal comum. Além de tornar mais eficiente a aplicação telefônica, a sinalização por canal comum permite novas facilidades e é aberta a novas aplicações, tais como sinalização da rede ISDN, da rede de telefonia celular, o suporte à rede inteligente IN (*Intelligent Network*) e outras [KUH94].

Uma rede de telecomunicações servida por uma sinalização por canal comum é composta por um número de nodos de processamento e comutação interconectados por enlaces de transmissão.

Todo nodo na rede SS7 é chamado genericamente de Ponto de Sinalização (PS). Todo ponto de sinalização tem a capacidade de realizar a discriminação de mensagens (ler o endereço e determinar se a mensagem é para este nodo).

Existem várias classificações de pontos de sinalização, de acordo com sua função na rede de sinalização. Entre elas, podemos destacar:

- STP (*Signaling Transfer Point*). Ponto de sinalização com função de transferência, isto é, capaz de ser "intermediário" (nem a origem nem o destino final da mensagem), podendo receber uma mensagem vinda de outro PS e passá-la adiante.

- SSP (*Service Switching Point*). É uma designação comum para um PS que provê apenas acesso local à rede de sinalização.

Além disso, nas redes AIN (*Advanced Intelligent Networks*), temos o SCP (*Service Control Point*) responsável pelo acesso à base de dados da rede AIN e o SMS (*Service Management System*) que provê a interface humana à base de dados, bem como a capacidade de atualizá-la quando precisar.

Todo ponto de sinalização em uma rede SS7 é identificado por um código de endereçamento único, conhecido como *point code*.

A sinalização por canal comum usa vias bidirecionais de sinalização que transportam mensagens entre dois pontos de sinalização, denominados enlaces de sinalização (*signaling links*). Dois pontos de sinalização (PS) SS7 são ditos adjacentes se são diretamente interconectados por um enlace.

É importante destacar que usa-se o termo enlace de sinalização ou apenas enlace para designar a conexão entre dois pontos de sinalização a nível funcional (lógico) e o termo enlace de dados de sinalização para se referir à conexão física por onde passa o enlace.

Os enlaces são dispostos em conjuntos que interconectam diretamente os mesmos dois PS, chamados conjuntos de enlace (*linksets*). Podem haver até 16 enlaces associados a um só conjunto de enlaces. Embora tipicamente um conjunto de enlaces inclua todos os enlaces paralelos (enlaces entre os mesmos dois PS), é possível haver mais de um conjunto de enlaces entre dois PS.

Um grupo de enlaces dentro de um mesmo conjunto de enlaces que têm características idênticas é chamado grupo de enlaces.

Além de *linksets*, um PS deve definir rotas. Rota é uma seqüência de *linksets* usada para atingir um certo destino. Um *linkset* pode pertencer a mais de uma rota. Uma coleção de rotas é chamada conjunto de rotas (*routeset*) e um conjunto de rotas é associado a um só destino, permitindo que exista mais de uma rota para o destino de forma que, caso uma rota fique indisponível, haja uma rota alternativa.

Um destino é um endereço presente na tabela de roteamento de um PS. Destinos não precisam ser diretamente adjacentes ao PS, mas devem ser um código de endereçamento (*point code*) de um PS que pode ser atingido a partir deste. O PS não precisa conhecer todos os *point codes* entre ele e o destino, apenas seu próprio conjunto de enlaces que levará ao destino.

Para quaisquer dos pontos de sinalização para os quais há possibilidade de comunicação entre seus usuários, diz-se que há uma relação de sinalização entre eles.

O modo de sinalização refere-se à associação entre o caminho tomado por uma mensagem de sinalização e a relação de sinalização a qual a mensagem se refere. Existem dois modos de sinalização possíveis em uma rede SS7:

- Associado: a mensagem referente a uma relação de sinalização em particular entre dois pontos adjacentes é transportada por um conjunto de enlaces que interconecta, diretamente, estes dois pontos.

- Quase-associado: a mensagem de uma certa relação de sinalização é levada por dois ou mais conjuntos de enlace em seqüência, passando por um ou mais PS intermediários (o que caracteriza o modo não-associado), mas há uma limitação: o caminho percorrido por uma mensagem na rede de sinalização é predeterminado e, numa determinada configuração, fixo.

O modo totalmente não-associado não é previsto para redes SS7, uma vez que os protocolos não incluem recursos para evitar chegada de mensagens fora de seqüência ou outros problemas que tipicamente surgem em um modo de sinalização não associado com roteamento de mensagens dinâmico.

7.2.1 Protocolos da rede SS7.

Os protocolos do SS7 são organizados em níveis, de maneira análoga às camadas do modelo RM-OSI. São 4 os níveis no SS7; os três níveis de menor hierarquia compõem o Subsistema de Transferência de Mensagens MTP (*Message Transfer Part*) e correspondem, em essência, aos três primeiros níveis do RM-OSI. No nível 4 do SS7 que corresponde à camada de Aplicação do modelo OSI, podemos ter vários subsistemas de usuário (*User Parts*), como o TUP (*Telephone User Part*) e o ISUP (*ISDN User Part*).

Para suportar outras aplicações na rede, dois componentes foram criados no SS7: o SCCP (*Signaling Connection Control Part*), que complementa os serviços do MTP para torná-lo funcionalmente equivalente ao nível de rede do modelo OSI, e o TCAP (*Transaction Capabilities Application Part*), que fornece um conjunto de protocolos e funções usados por aplicações distribuídas na rede para que essas possam se comunicar. A relação entre os níveis do SS7 e o modelo OSI é ilustrada na Figura 7.2.

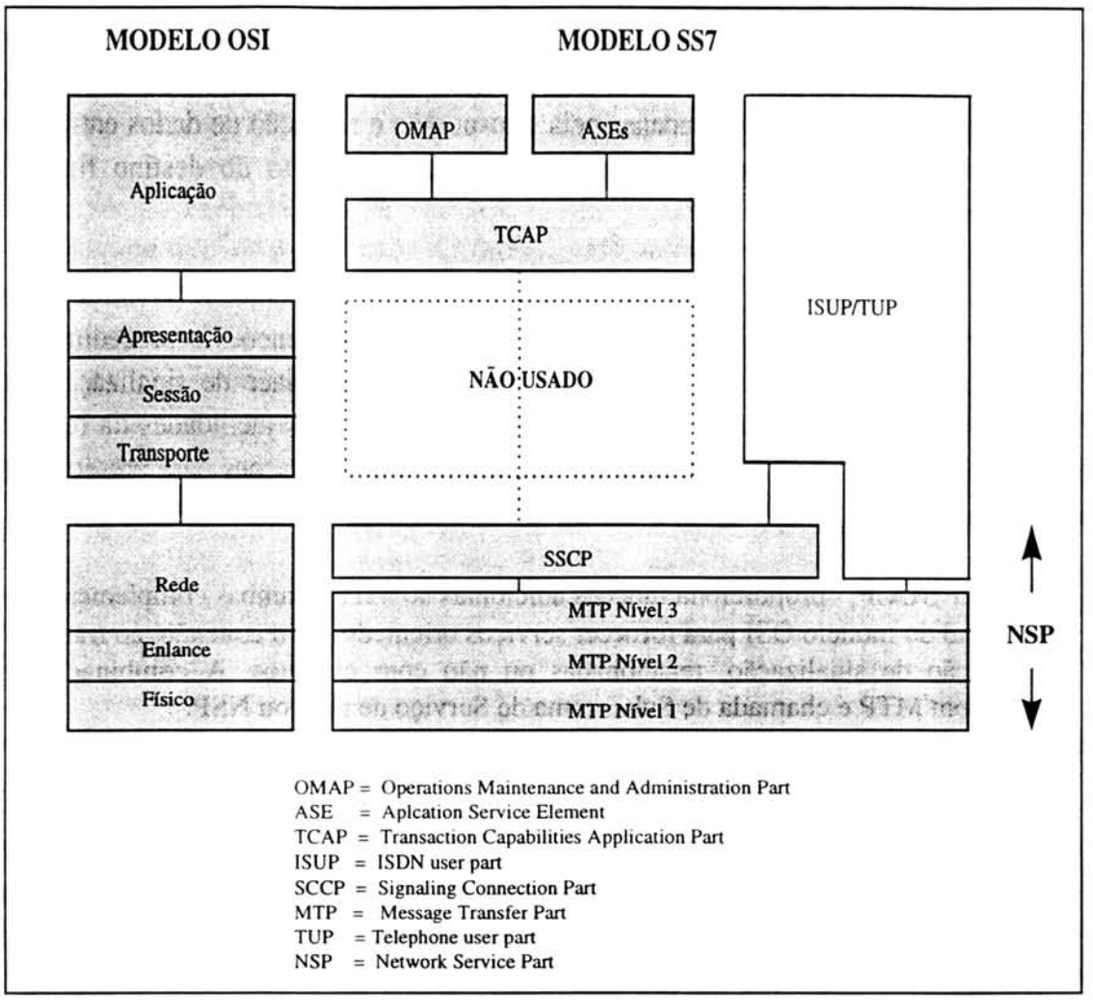

FIGURA 7.2 - O SS7 e sua relação com as camadas do modelo OSI [MOD90].

7.2.2 O Subsistema de serviço de rede NSP.

O Subsistema de Transferência de Mensagens MTP é o protocolo de transporte usado pelos outros protocolos de nível acima no SS7 (ISUP e TUP). O MTP provê às demais camadas do SS7 os seguintes serviços:

- transmissão de dados nodo a nodo;
- esquema de detecção e correção de erros básicos;
- seqüenciamento de mensagens;
- roteamento de mensagens;
- discriminação de mensagens;
- funções de distribuição de mensagens.

O MTP é subdividido em três camadas: níveis 1, 2 e 3, que correspondem, respectivamente, ao níveis físico, enlace e rede do modelo OSI.

O nível físico do **MTP1** é o responsável pela conversão de dados digitais em uma seqüência de bits para transmissão através da rede. O padrão SS7 não especifica qualquer interface ou taxa de transmissão de dados para esse fim. Desta forma, estes parâmetros ficam determinados, principalmente, pelo requerimento de custo/desempenho da rede sobre a qual o sistema será implantado.

O nível do enlace do **MTP2**, provê detecção e correção de erros e seqüenciamento de todos os pacotes de mensagens do SS7. Assim como no modelo OSI, este nível é responsável apenas pela transmissão e recepção de dados entre dois nodos adjacentes na rede. Este nível não tem conhecimento do destino final da mensagem.

O último e mais complexo nível é o **MTP3**. Nesta camada (nível de rede) encontram-se as funções de rede na sinalização; define-se funções e procedimentos para controlar o encaminhamento das mensagens para o enlace de sinalização (ou parte do usuário apropriada); controla-se a configuração das facilidades da rede de sinalização. Em caso de falhas também controla as reconfigurações para preservar ou restabelecer a capacitação normal de transferência de mensagens.

O **SCCP**, proporciona funções adicionais ao MTP, e ambas complementam a camada 3 do modelo OSI para fornecer serviços orientados sem conexão, ao transferir informação de sinalização, relacionadas ou não com circuitos. A combinação de SCCP com MTP é chamada de Subsistema de Serviço de rede ou **NSP**.

7.2.3 O nível 4 do protocolo SS7.

O nível 4 do SS7 é equivalente a camada de Aplicação do OSI. No SS7 não existem as camadas de Transporte, Sessão e Apresentação. Formando parte do nível 4 estão o TUP e ISUP. O **TUP** (*Telephone User Part*) define funções e procedimentos de sinalização necessários ao uso de SS7, no controle das chamadas telefônicas. Em tanto que o **ISUP** (*ISDN User Part*) define funções e procedimentos necessários à oferta de serviços comutados e as facilidades do usuário para aplicação de voz e dados na ISDN. O ISUP pode ser usada em redes telefônicas ou em redes mistas (analógicos e digitais). A pesar de estar no nível 4, possuem uma interface com a SCCP para sinalização de extremo a extremo.

O Elemento do Serviço de Aplicação **ASE** (*Application Service Element*) fornecem a informação específica uma aplicação precisa. O **TCAP** (*Transaction Capabilities Application Part*), fornece todas as ferramentas necessárias pelo ASE para distribuir operação entre as camadas de aplicação.

Usuários do TCAP são o OMAP (*Operation Maintenance and Adminstration Part*) e o MAP (*Mobile Application Part*). **OMAP** fornece protocolos de aplicação e procedimentos para monitorar, coordenar e controlar todos os recursos da rede que fazem possível a comunicação baseada no SS7. Todas as interações entre diferentes nodos da rede SS7 são levadas através dos serviços da TCAP. O **MAP** fornece capacidades de sinalização necessárias para suportar capacidade móvel (por exemplo o *roaming*) numa rede de comunicação móvel.

A especificação mundial do SS7 está na série Q.700 de recomendações da ITU-T (ITU *Telecommunication Standardization Sector*), órgão permanente da ITU, originalmente publicadas no "Livro Azul CCITT" (CCITT *Blue Book*) em Melbourne, novembro de 1988, Fascículos VI.7-9. A maior parte das recomendações da série Q.700 foram revisadas pelo *ITU-T Study Group XI* (1988-1993) e aprovadas em Helsinki, em março de 1993.

8 Sinalização em Telefonia Celular e PCS

Os serviços de sinalização para ambas redes, fixa e móvel, deveram ser definidos independentemente da arquitetura física da rede. Desde o ponto de vista da rede, camadas superiores deveram requerer só serviços fornecidos pelas camadas inferiores e não precisam saber como estes serviços são fornecidos. No modelo de sinalização da rede SS7, a camada de aplicação e os serviços que este pode fornecer foi definido no Capítulo 7. Para segurar a mobilidade em redes de comunicação móvel, o MAP foi agregado para a camada de aplicação do SS7. A implementação do MAP usa o conceito de elemento de serviço de aplicação ASE (*Application Service Element*) do SS7 [JAB92] [KUH94].

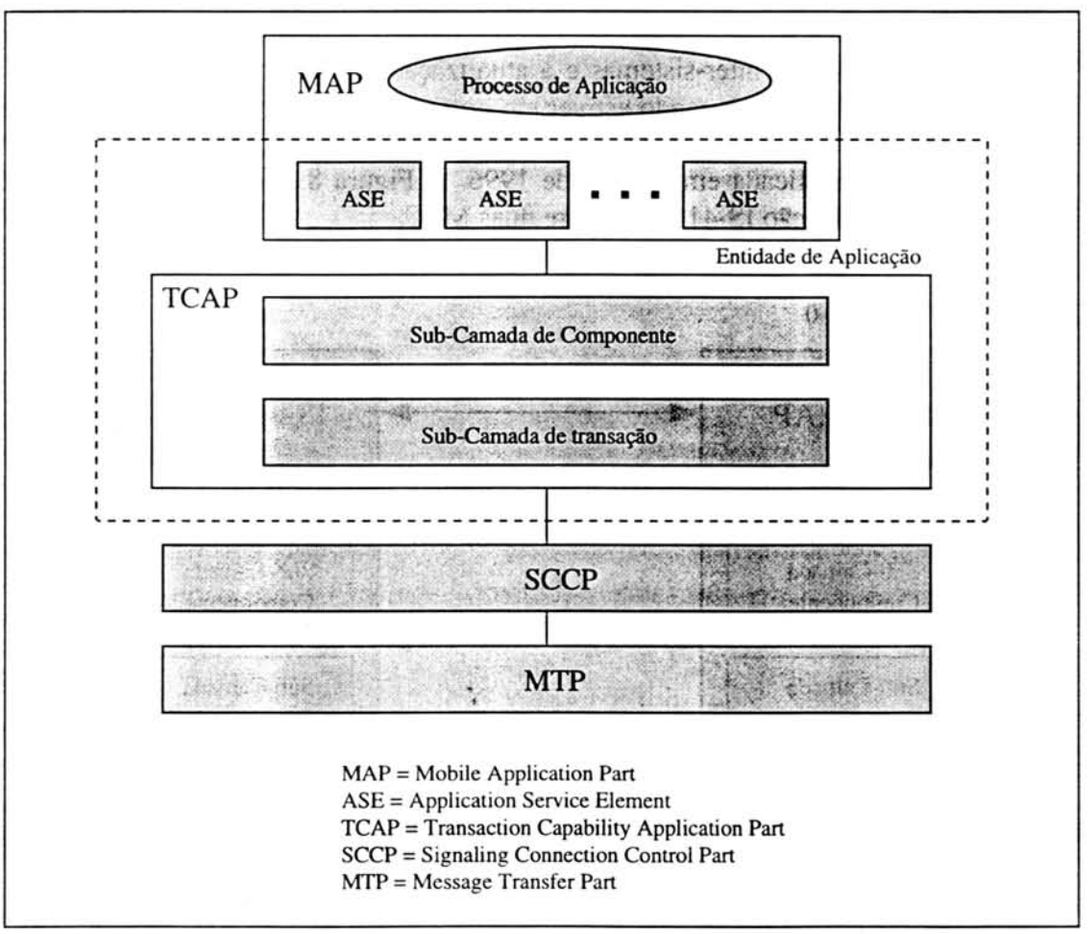

FIGURA 8.1 - O MAP no SS7 [JAB92].

MAP é na realidade um ASE baseado no TCAP do SS7. O TCAP consiste de duas sub-camadas: a sub-camada de componente e a sub-camada de transação, ambas correspondem à camada de aplicação do OSI. O MAP também requer o suporte do SCCP e do MTP do SS7. A localização do MAP no SS7 é mostrado na Figura 8.1. O MAP é só uma entidade funcional e portanto independente da implementação física da rede de sinalização. Muitos procedimentos MAP são definidos para fornecer independência da interface rede/fabricante entre pares de elementos da rede para suportar funções relativas à mobilidade, tal como localização e registro, *handoff*, autenticação, manipulação da informação, etc. Estes procedimentos facilitam o acesso

para serviços fornecidos pelas camadas inferiores só no ponto de serviço de acesso (SAP), o qual isola a camada superior do inferior. Desde que o MAP é uma rede independente, a modificação de procedimentos existentes e a introdução de novos serviços são fácies e rápidos. Isto também permite a camada física para desenvolver sem afetar as aplicações. A sinalização de rede SS7 usado em ambientes móveis estão padronizados nas recomendações da ITU, Q.1061 e Q1062.

8.1 Sinalização IS-41 MAP para redes de telefonia celular.

A comunicação entre dois MSC (*Mobile Switching Center*) numa rede de telefonia celular é automática usando o protocolo de sinalização IS-41 MAP. A sinalização por canal comum, em telefonia móvel, tem sua função voltada para a interligação de centrais de comutação móveis (MSC) para viabiabilizar o *roaming* automático, o *handoff* inter-sistemas e a atualização dos serviços suplementares de um usuário móvel mesmo quando estiver em outra área de cobertura que não é a sua. O IS-41 MAP está baseado no SS7. A atual versão do IS-41 MAP se encontra na revisão C, e foi publicada em Janeiro de 1996. A Figura 8.2 mostra as camadas do protocolo de sinalização IS-41 MAP entre duas MSC.

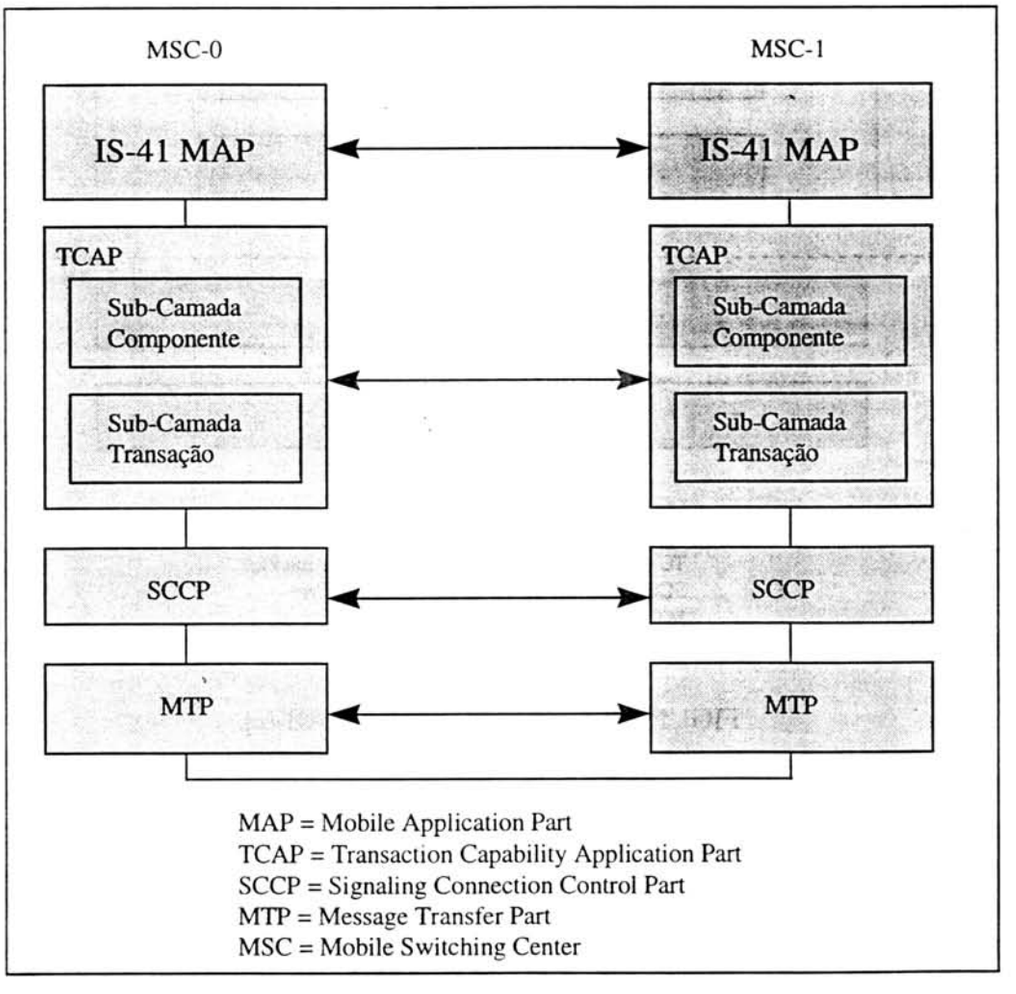

FIGURA 8.2. - Sinalização IS-41 MAP entre duas centrais [TEL94].

8.2 Sinalização em redes GSM.

Na Figura 8.3 é mostrada a arquitetura de protocolos de sinalização da rede GSM, denominado GSM-MAP, entre a estação móvel e a rede GSM . A arquitetura de protocolos para uma rede GSM-MAP está estruturada em três camadas : a camada física, na qual usa canais baseados em TDMA, a camada de enlace de dados na qual são usados os protocolos LAPDm e o MTP2 do SS7, e a camada de rede que está divido em três subníveis :

- *Radio Resurces Management* (RR). Tem como finalidade o gerenciamento dos meios de transmissão (canais físicos e de controle) de modo a estabelecer, manter e terminar conexões que permitam a comunicação da MS com o resto da rede, incluindo os *handoff*.
- *Mobility Management* (MM). Proporciona as informações referentes à mobilidade dos usuários.
- *Connection Management* (CM). O objetivo desta subcamada é o estabelecimento de chamadas entre usuários tanto da rede GSM como entre um usuário da rede móvel e fixa, assim como a sua manutenção e término.

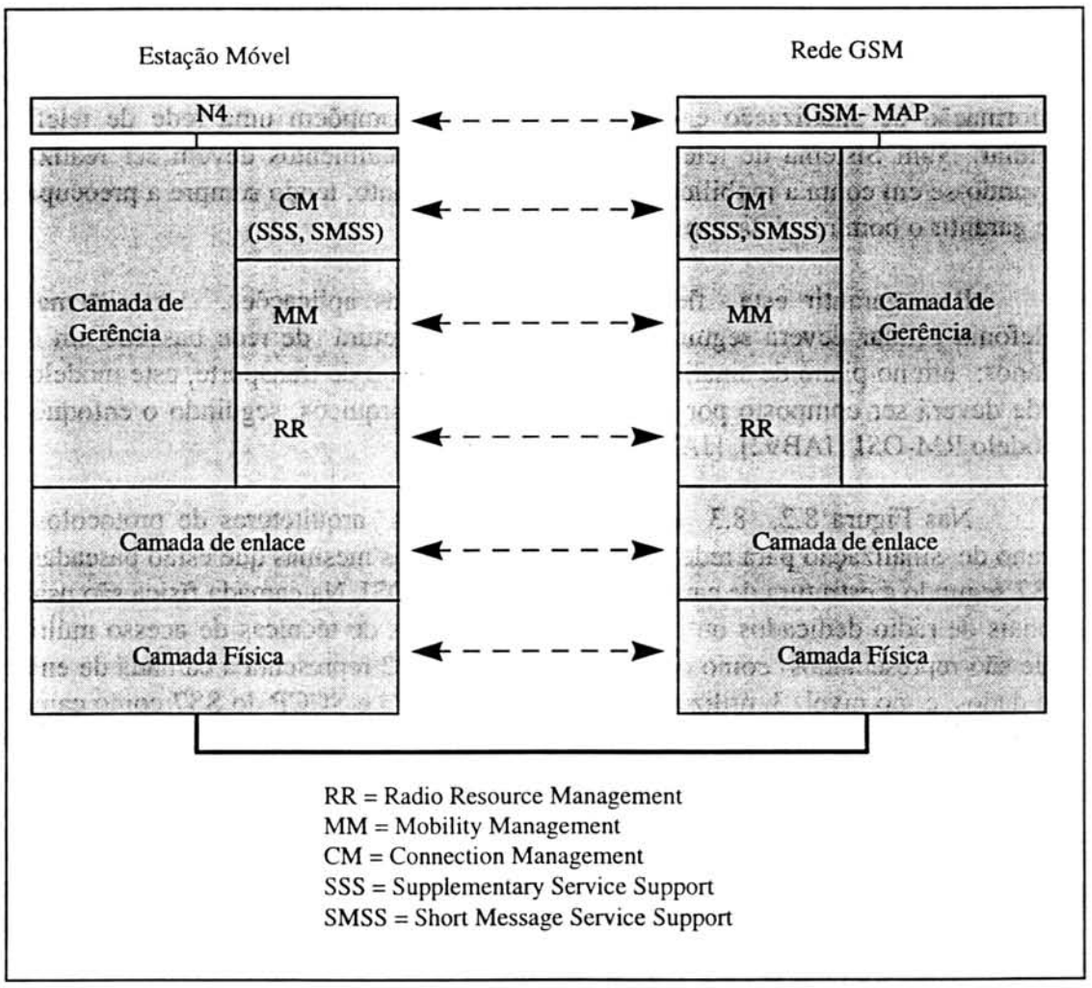

FIGURA 8.3 - Arquitetura de Protocolos do GSM-MAP [SIE95].

8.3 Sinalização em redes PCS.

As principais preocupações do protocolo de sinalização em redes PCS, são a capacidade, a eficiência, flexibilidade para futuros desenvolvimentos, e compatibilidade com o padrão de sinalização da rede ISDN [LI95].

O protocolo de sinalização proposto para sistemas PCS deverá estar baseado no padrão SS7 levando em conta suas caraterísticas específicas de mobilidade. Protocolos de sinalização para sistemas PCS podem ser similares aos usados em sistemas de telefonia celular da segunda geração, mais com a capacidade para suportar adicionais exigências como alta mobilidade, e caraterísticas superiores de serviço de rede.

Assim, na atualidade existem dois protocolos de sinalização já propostos para sistemas PCS; o IS-41 MAP (americano) e o GSM-MAP (européio) [AKY96].

8.4 Os Planos de Sinalização e Transporte para Redes de Telefonia Celular.

Para efetuar procedimentos referentes a: estabelecimento/término de chamadas, monitorização da localização do assinante, implementação de procedimentos de segurança e provisão de serviços avançados, são necessárias diversas trocas de informação de sinalização entre as entidade que compõem uma rede de telefonia celular. Num Sistema de telefonia celular tais procedimentos devem ser realizados levando-se em conta a mobilidade do usuário e, portanto, tendo sempre a preocupação de garantir o bom nível da comunicação.

Para garantir esta flexibilidade nas diversas aplicações, um sistema de telefonia celular deverá seguir um modelo de arquitetura de rede baseado em dois planos: um no plano de sinalização e o outro no plano de transporte, este modelo de rede deverá ser composto por níveis funcionais hierárquicos, seguindo o enfoque do modelo RM-OSI [JAB92], [JAB95], [LEE95].

Nas Figura 8.2, 8.3 e 8.4 são mostradas as arquiteturas de protocolos no plano de sinalização para redes de telefonia celular, as mesmas que estão baseadas no SS7 segundo a estrutura de camadas similar ao RM-OSI. Na camada física são usados canais de rádio dedicados ou canais terrestres através de técnicas de acesso múltiplo que são representados como o nível MTP1. O MTP2 representa a camada de enlace de dados, e no nível 3, utiliza-se os protocolos MTP3 e SCCP do SS7 como camada de rede. Uma das funções realizadas pelo MTP3 é de endereçamento local, tendo relevância apenas dentro de uma rede nacional. O endereço contido nesse protocolo chama-se SPC *(Signaling Point Code)*. Já o SCCP é utilizado para o endereçamento global dos usuários, quando estes se comunicam através de duas redes distintas. Acima dos protocolos MTP3 e SCCP está o TCAP. Embora considerado um protocolo de aplicação, o TCAP cumpre mais o papel de um protocolo de sessão, já que provê os meios para distinguir os diferentes fluxos de mensagens pertencentes a cada diálogo em andamento. Níveis superiores são consideradas como a camada de aplicação e estão especificadas nas normas IS-41 MAP e GSM-MAP.

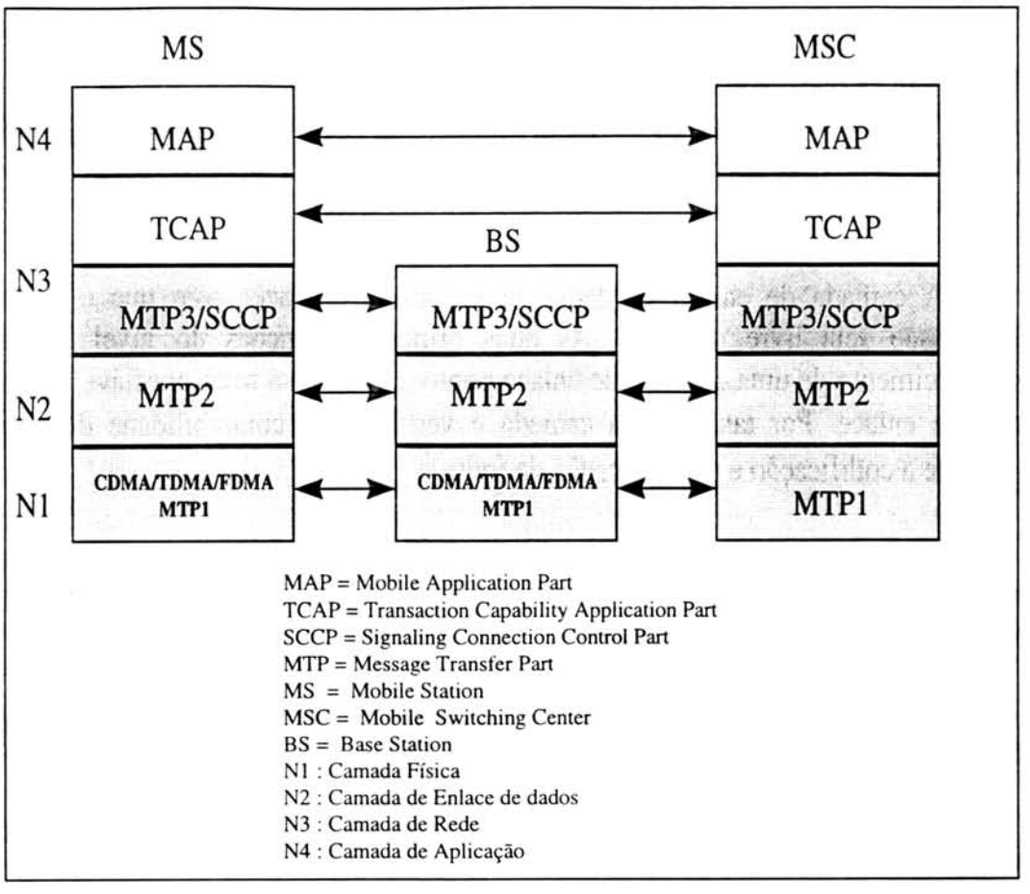

FIGURA 8.4 Arquitetura de protocolos para o plano de sinalização numa rede de telefonia celular.

De forma similar, um modelo de arquitetura de protocolos mostrando o plano de transporte é mostrado na Figura 8.5.

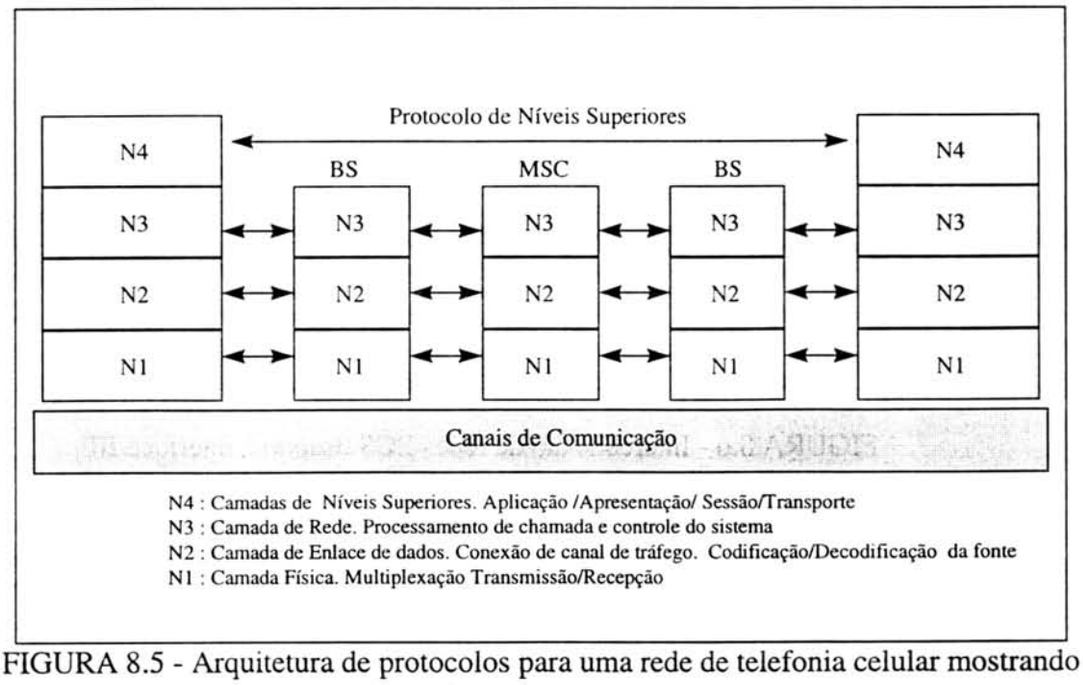

FIGURA 8.5 - Arquitetura de protocolos para uma rede de telefonia celular mostrando o plano de transporte.

Nesta arquitetura a camada física, realiza a transmissão física dos canais e fornece canais lógicos para as camadas superiores, que envolve a implementação dos sistemas de transmissão/recepção, ou seja as funções básicas para transmitir o fluxo de bits como: modulação, temporização, sincronismo e filtragem, além dos mecanismos de multiplexação.

A camada de enlace de dados se encarrega de fazer com que o meio de transmissão seja livre de erros. As duas principais funções do nível 2 são: o estabelecimento de uma conexão de enlace ponto a ponto e a troca confiável de dados por este enlace. Por tanto, nesta camada é verificado a confiabilidade dos dados, mediante a codificação e decodificação da fonte.

Na camada de rede têm como objetivo o encaminhamento das mensagens para ser distribuídas aos destinatários corretos, e define somente as funções próprias da conexão fim a fim da rede, associadas ao serviço de telefonia.

8.5 Uma Arquitetura de Protocolos de Sinalização para a Interconexão de Redes Heterogêneas com Sistemas PCS.

Segundo [HUS96] e [GAR96], para resolver o problema da interconexão e interoperabilidade de uma redes PCS com outra de padrão diferente (rede celular, rede cordless, rede ISDN, etc), será necessária uma unidade funcional de interconexão de rede, que foi denominada de IIF (*Interworking Interoperability Function*), e esta unidade deverá estar baseada numa arquitetura protocolos de sinalização SS7 e MAP.

Por exemplo, na Figura 8.6, representamos graficamente a interconexão de uma rede de telefonia PCS do tipo USCD com uma rede PCS do tipo GSM. Esta interconexão é realizada usando uma IIF baseada em protocolos de sinalização SS7, IS- 41- MAP e GSM-MAP.

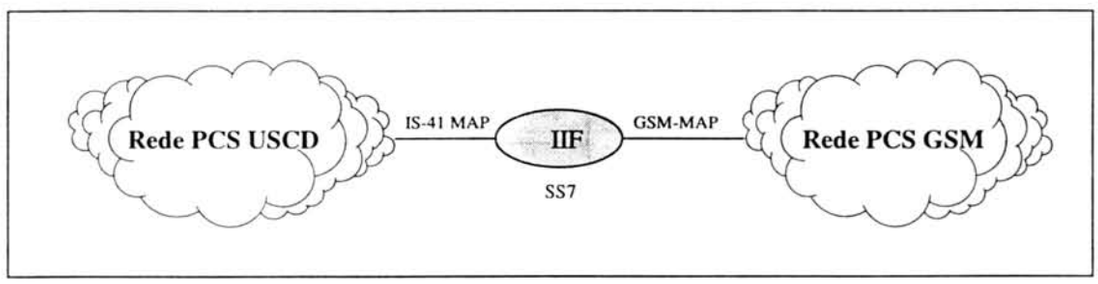

FIGURA 8.6 - Interconexão de redes PCS usando a interface IIF.

O problema da interconexão de uma rede PCS com as diversas redes fixas e móveis ainda não esta resolvido, até agora, nem a própria TIA tem um padrão definido para isso [HUS96], [GAR96]. Só existem soluções particulares para cada tipo de rede, por exemplo, a interconexão da rede GSM com a rede PACS [NOE96], de forma similar GSM-MAP com IS-41 MAP [GAR96], GSM com ISDN [LAI95], etc. Estas soluções são parciais e proprietárias e até o momento, ainda não existe uma solução global, ou seja um padrão que permita a interconexão de uma rede PCS com as

demais redes heterogêneas. Nos congressos e publicações especializadas está havendo uma grande discussão sobre isso, e possivelmente a solução ainda demande mais algum tempo. Pode acontecer também que neste período algum padrão de fato seja adotado para cada uma das redes. Este problema é abordado também no sistema FPLMTS, que é proposto pela ITU, que está sendo projetado considerando uma padronização global em relação a interoperabilidade, assim como foi na rede ISDN.

Devido a diversidade de padrões propostos para PCS pela TIA, (ver Tabela 3.3), e também pela quantidade de redes heterogêneas fixas e móveis que deveram ser inter-conectadas aos sistemas PCS num futuro próximo, a complexidade da inter-conectividade de todas estas redes usando uma só interface fogem do escopo desta dissertação e por isso vamos delimitar nosso objetivo inicial e considerar apenas uma solução particular na interconexão de dois tipos de redes *wireless*.

Neste sentido, vamos considerar a interconexão de uma rede PCS baseada no padrão J-STD-007 (baseado GSM) e uma rede de telefonia celular IS-95 (digital americano), e vamos propor uma arquitetura de protocolos no plano de sinalização e uma interface do tipo IIF (*Interworking Interoperability Function*) que viabilize esta interconexão, conforme é mostrado na Figura 8.7.

A arquitetura proposta representa a interconexão de duas arquiteturas de sinalização, a primeira, baseada no protocolo GSM-MAP, que foi revisado no item 8.3, e a segunda é baseada no protocolo IS-41-MAP, abordado no item 8.2. Entre estas duas arquiteturas está a interface IIF, baseada no protocolo de sinalização SS7, que é compatível com a pilha de protocolos IS-41-MAP e GSM-MAP, conforme foi visto no item 8.1.

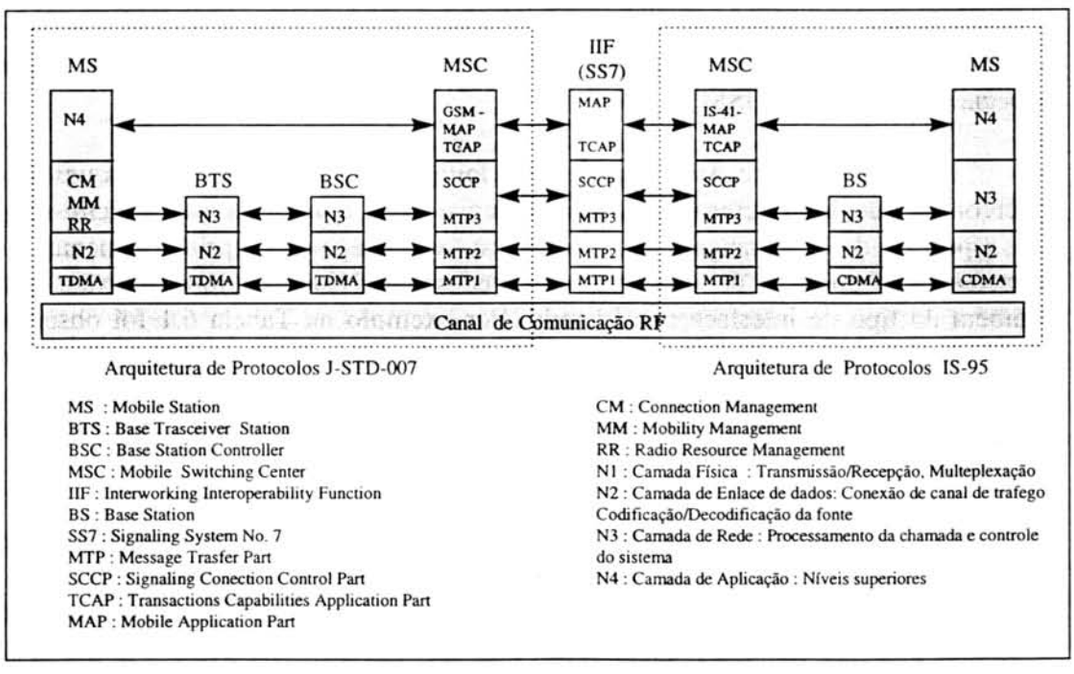

FIGURA 8.7 - Arquitetura de protocolos de sinalização representando a interconexão de uma rede PCS com uma rede de telefonia celular.

9 Conclusões

No Brasil, com a privatização dos serviços de telecomunicações, as novas concessionárias da banda B de telefonia celular, terão que oferecer sistemas com características de operação do tipo *dualmode*, ou seja, deverão atender simultaneamente o antigo sistema analógico AMPS e o novo sistema digital a ser adotado. Neste contexto, os novos sistemas, além de oferecerem uma alta capacidade de assinantes por célula, deverão oferecer, principalmente também, características de segurança altamente confiáveis.

Na primeira parte deste trabalho foram analisados e revisados os aspectos de segurança em sistemas de telefonia celular. O estudo comparativo apresentado no Capítulo 4 mostra as características de segurança dos principais sistemas de telefonia celular, que poderá servir como base para a especificação das características de autenticação e privacidade dos novos sistemas de telefonia celular a serem adotados pelas novas concessionárias. Em particular, a partir de um enquadramento dos diversos sistemas estudados, sugerimos um modelo que é baseado na arquitetura GSM, pois os mecanismos de segurança e autenticação incorporados no GSM tornam este padrão o mais seguro em comunicações móveis, particularmente se comparado aos sistemas analógicos e ao USDC [LUN97].

A partir da análise e discussão dos aspectos de segurança em sistemas de telefonia celular e de alguns sistemas PCS apresentados, conclui-se que os sistemas PCS emergentes, provavelmente deverão adotar soluções baseadas nos novos sistemas de telefonia celular digital. Isto significa que nosso estudo comparativo quanto aos aspectos de autenticação e privacidade dos sistemas de telefonia celular (ver Tabela 4.1), também pode ser estendido aos sistemas PCS emergentes. A partir de um enquadramento dos diversos sistemas estudados, também é sugerido um modelo de segurança para estes novos sistemas PCS que seja baseado no modelo AKA, e em especial na arquitetura GSM.

Na segunda parte deste trabalho foi feita uma análise referente à questão da interconexão de redes heterogêneas com sistemas PCS, a partir da qual conclui-se que os aspectos de segurança neste contexto vão depender, principalmente, das características próprias de cada uma das redes envolvidas na interconexão, como também do tipo de interface considerado. Por exemplo na Tabela 6.1 foi observado que o uso de uma interface do tipo IIF melhora os aspectos de privacidade em relação a uma interconexão usando a rede PSTN, o mesmo não ocorrendo porém no caso de uma interconexão com uma rede analógica, na qual a segurança sempre estará comprometida.

Em continuação, no Capítulo 7 deste trabalho, é aprofundado o estudo referente à questão da interconexão de redes heterogêneas com os sistemas PCS, que é completado com a abordagem dos protocolos de sinalização SS7 e MAP, requisitos importantes na solução dos problemas de interoperabilidade. Do estudo conclui-se que a sinalização jogará um papel decisivo no desenvolvimento dos sistemas PCS nos próximos anos e como os padrões para estes sistemas ainda estão em fase de projeto, uma significativo parcela de trabalho e esforço ainda está por ser feita. Por exemplo, a definição de uma unidade funcional de interconexão IIF, que forneça

interoperabilidade entre a rede fixa e móvel, ainda é uma questão importante a ser resolvida [SOH96], [LI95], [GAR96],[HUS96].

Neste trabalho estamos propondo uma IIF para a interconexão e interoperabilidade de uma rede PCS com uma rede de telefonia celular, em que esta unidade funcional será baseada na arquitetura de protocolos RM-OSI e segue o PRM (Protocol Reference Model) do sistema de sinalização SS7 e MAP. A IIF proposta é mostrada na Figura 8.7.

Finalmente é sugerida uma implementação desta unidade funcional (IIF), ou seja, além de ser especificada formalmente, deverá ser modelada e simulada a seguir para avaliação de seu desempenho. A IIF pode ser especificada usando a linguagem de especificação formal SDL (*Specification and Description Language*) na sua formulação SDL/GR (gráfica) ou SDL/PH (texto). Para fins de avaliação do desempenho da interface proposta, pode ser usado a ferramenta de *software* estática SDT (*SDL Design Tolol*) e a seguir a dinâmica do tipo MSC (*Message Sequence Charts*), que deverão ser adaptadas para comunicações móveis [HED94]. Estas ferramentas SDL deverão rodar sobre alguma plataforma computacional que permita a simulação do comportamento desta IIF. Este processo é mostrado, nos seus aspectos genéricos, através da Figura 9.1.

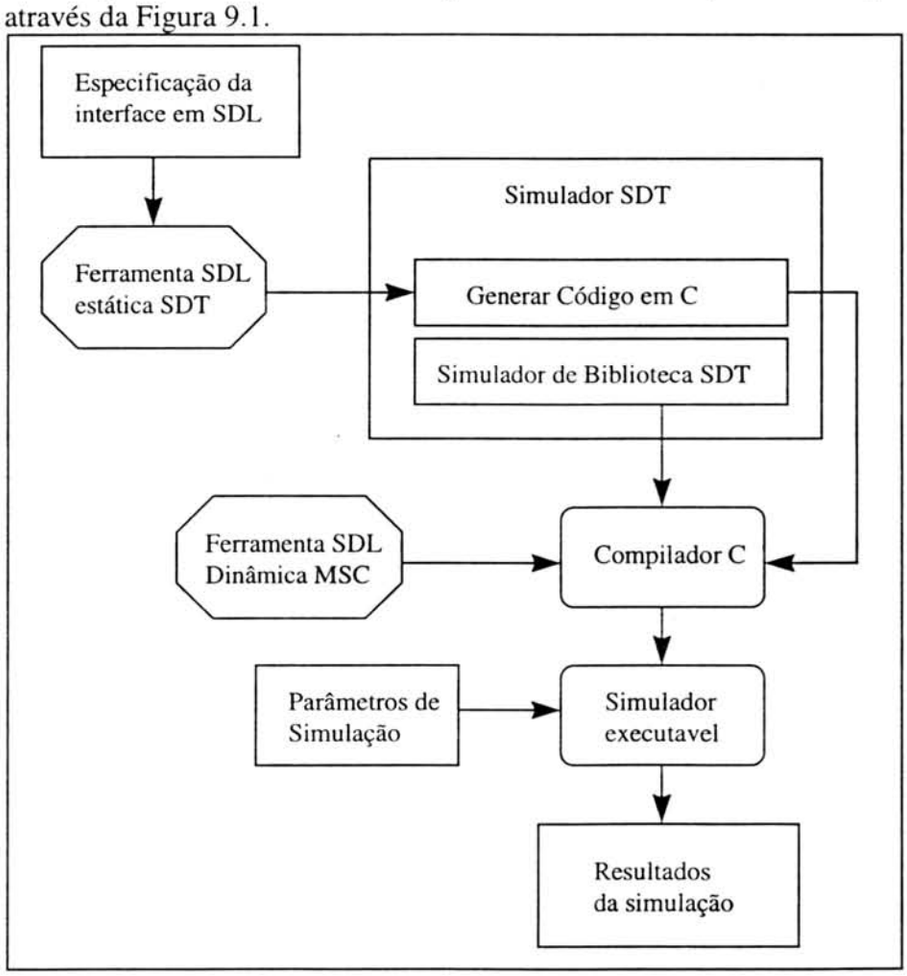

FIGURA 9.1 - Processo de Simulação da Interface IIF usando ferramentas SDL [HED94]

Bibliografia

[AKY96] AKYILDIZ, Ian F. On Location Management for Personal Communications Networks. **IEEE Communications Magazine,** New York, v. 34, n. 9, p. 138-145, Sept.1996.

[BEL93] BELLER, Michel J. Privacy and Authentication on a Portable Communications Systems. **IEEE Journal on Selected Areas in Communications,** New York, v. 11, n. 6, p. 821-829, Aug.1993.

[BIN95] BING, Y. Ling. PCS Network Signaling Using SS7. **IEEE Personal Communications**, New York, p. 44-55, June 1995.

[BRO95] BROWN, Dan. Techniques for Privacy and Authentication in PCS. **IEEE Personal Communications**, New York, p.6-10, Aug. 1995.

[CAL94] CALLENDAR, Michel. Future Public Land Mobile Telecommunications Systems. **IEEE Personal Communications**, New York. p. 10-11, Fourth Quarter 1994.

[CAM96] CAMARGO, Henrique. **Introdução ao Sistema de Sinalização por Canal Comum Numero 7**. Disponível em http://www.dcc.ufmg.br/~marcio/ss7/reltec28.html (30 set. 1996).

[CAR96] CARNEIRO, H.; SANTIVAÑES, J.; BOISSON R. Arquitetura e Sinalização em Redes Celulares. In : SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES, SBT, 14., 1996, Curitiba, **Anais...** [S.l.:s.n.], 1996. p. 773 778.

[CEC96] CECILIO, Nilo. Guerra ao Clone. **Revista Nacional de Telecomunicações RNT**, São Paulo, v. 18, n. 204, p. 13-16, ago. 1996.

[COO94] COOK, I. Charles. Development of Air Interface Standards for PCS. **IEEE Personal Communications**, New York, p.30-34, Fourth Quarter 1994.

[COX95] COX, C. Donald. Wireless Personal Communications : What Is It ? **IEEE Personal Communications**, New York, p. 20-35, Apr. 1995.

[GAR96] GARG, Vijak K., WILKES, Joseph E. Interworking and Interoperability Issues for North American PCS. **IEEE Communications Magazine**, New York, p. 94-99, Mar. 1996.

[HED94] HEDMAN, Eva. Simulation and formal specification of protocols for mobile radio networks - an integrated approach. **IEEE Journal on Selected Areas in Communications,** New York, v.12. n.5, p. 373-377, Mar. 1994.

[HUS96] HUSAIN, Syed. Intelligent Network : A key Plataform for PCS Interworking and Interoperability. **IEEE Communications Magazine**, New York, p. 98-106, Oct. 1996.

[JAB92] JABBARI, Bijan. Intelligent Network Concepts in Mobile Communications. **IEEE Communications Magazine**, New York, p. 64-69, Feb. 1992.

[JAB95] JABBARI, Bijan. Network Issues for Wireles Communications. **IEEE Communications Magazine**, New York, p. 88-98, Jan. 1995.

[KUH94] KUHN, Paul. Common Chanel Signaling Networks: Past, Present, Future. **IEEE Journal on Selected Areas in Communications,** New York, v.12, n.3, p. 383-393, Apr. 1994.

[LAI95] LAITINEN, Mikko, RANTALA, Jari. Integration of Intelligent Network Services into Future GSM Networks. **IEEE Communications Magazine**, New York, p.76-85, June 1995.

[LEE95] LEE, William C. Y. **Mobile Cellular Telecommunications.** London - UK : McGraw-Hill Inc., 1996.

[LI95] LI, Ok. Victor, XIAOXIN Qiu. Personal Communications Systems (PCS). **Procedings of the IEEE**, New York, p. 1210-1243, Sept. 1995.

[LIN95] LIN, Hung-Yu. Authentication Protocols for Personal Communications Systems. In : ACM SIGCOMM 1995, London - UK. **Proceedings...** [S.l.: s.n], 1995.

[LOB96] LOBO, Ana Paula. Guerra contra o fraude**. Computer World IDG Brasil**, Rio de Janeiro, p. 12, set. 1996.

[LUN95] LUNA, Herbert. **(R)Evolução dos Sistemas de Comunicação Sem Fio**. Porto Alegre : CPGCC-UFRGS, 1995. (TI-520).

[LUN96] LUNA, Herbert. Sistemas de Telefonia Celular Rumbo a la Tercera Generación. **Revista Colombiana de Telecomunicaciones CINTEL**, Santa Fé de Bogotá, p. 35-41, Dic. 1996.

[LUN97] LUNA, Herbert, JUERGEN, Rochol. Segurança em Sistemas de Comunicação Pessoal - Um estudo comparativo e a questão da interconexão com redes heterogêneas. In : SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES - SBRC, 15., 1997, São Carlos - SP. **Anais....** [S.l.:s.n.] , 1997. p.245-261.

[LUX95] LUXNER, Larry. El Fin de La Línea?. **CommunicationsWeek Latinoamérica.** Londres - UK, v. 2, n. 2, p. 16-17, 1995.

[MAR95] MARGRAVE, **David. GSM Security and Encryption**. Disponível em http://www.10pht.com/~drwho/cell/gsm-secur.html (15 Mar. 1995).

[MOD90] MODARRESSI, Abdi. Signaling System Number. 7 : A Tutorial. **IEEE Communications Magazine,** New York, p. 19-35, July 1990.

[NOE96] NOERPEL, Anthony. PACS: An Alternative Technology for PCS. **IEEE Communications Magazine**, New York, p. 138-150 , Oct. 1996.

[PAD95] PADGETT, Jay. Overview of Wireless Personal Communications. **IEEE Communications Magazine**, New York, p. 68-81, Jan. 1995.

[PAN95] PANDYA, Raj. Emerging Mobile and Personal Communications Systems. **IEEE Communications Magazine**, New York, p.34-42, June 1995.

[PIN95] PINTO, Ana Clara. **SEGREDE - mecanismos para Gerência de Segurança em redes**. Porto Alegre : CPGCC-UFRGS, 1995. Dissertação de Mestrado.

[ROC95] ROCHOL, Juergen, BOEIRA, M, PUFAL, H. Comunicação de Dados em Redes Celulares de Telefonia Móvel. In SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES - SBRC, 13., 1995, Curitiba. **Anais....** [S.l.:s.n.], 1995. p. 247-263.

[ROC95a] ROCHOL, Juergen, BOISSON , J. Proposta de um Serviço de Comunicação de Dados no Sistema DS-CDMA de Telefonia Celular Móvel baseado na IS-95 da TIA/EIA. In : SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES SBT, 13., 1995, Aguas de Lindoia-SP, **Anais....** [S.l.:s.n.], 1995. p. 137-142.

[ROC95b] ROCHOL, Juergen. **Disciplina : Tópicos Especiais em Comunicação de Dados**. Porto Alegre : CPGCC- UFRGS, 1995. Notas de aula.

[SCH95] SCHWARTZ, Mischa. Network Management and Control Issues in Multimedia Wireless Netwoks. **IEEE Personal Communications**. New York, p.8-16, June 1995.

[SCO96] SCOURIAS, John. **Overview of the GSM**. Disponível em http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html (2 Jun. 1996).

[SIE95] SIEGMUND, Redl . **An Introduction to GSM.** Noerwood - MA : Artech House Publishers, 1995

[SIQ96] SIQUEIRA, Ethevaldo. Conhecendo o CDMA. **Revista Nacional de Telecomunicações RNT**, São Paulo, v. 18, n. 208-A, p. 4-5, dez. 1996.

[SOH96] SOHRABY, Kazem. Integrated Services and Integration Issues in Wireless Networks. **IEEE Communications Magazine**, New York, p. 88-89, Sept. 1996.

[TAN96] TANEMBAUM, Andrew. **Computers Networks**. London - UK: Printice Hall International, 1996.

[TIA94] TELECOMMUNICATIONS INDUSTRIES ASSOCIATION. **Security And Identification,** TIA/EIA/Interim Standard IS-95. Washington, 1994.

[TEL94] TELEBRAS. **Básico de Telefonia Celular**. Campinas - SP: Centro Nacional de Treinamento, 1994. 60 f.

[VAR96] VARMA, Vijay. Architecture for Interworking Data over PCS. **IEEE Communications Magazine**, New York, v. 34, n.9, p. 124-130, Sept. 1996.

[WEB95] WEBER, Raul. Criptografia Contemporânea. In : SIMPÓSIO DE COMPUTADORES TOLERANTES A FALHAS, 6.,1995, Canela, RS, **Anais...** [S.l.:s.n.], 1995. p 10-23 .

[WIL95] WILKES, Joseph. Privacy and authentications Needs of PCS. **IEEE Personal Communications**, New York, v. 2, n.4, p. 11-16, Aug. 1995.

[YAC95] YACOBI, Yacob. Security for Wireless Systems. **IEEE Personal Communications**, New York, v. 2, n.4, p. 2, Aug. 1995.

Informática  UFRGS

CURSO DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Segurança em Sistemas de Comunicação Pessoal - Um Modelo de Arquitetura de Protocolos para a Interconexão de Sistemas Heterogêneos.

por

Herbert Luna Galiano

Dissertação apresentada aos Senhores:

Prof. Dr. Lee Luan Ling (UNICAMP)

Profa. Dra. Liane Margarida Rockenbach Tarouco

Prof. Dr. Raul Fernando Weber

Vista e permitida a impressão.
Porto Alegre, 12 / 08 / 97 .

Prof. Juergen Rochol
Orientador.

Profa. Carla Maria Dal Sasso Freitas
Coordenadora Substituta do Curso de
Pós-Graduação em Ciência da Computação
Instituto de Informática - UFRGS