Segurança em Sistemas de Comunicação Pessoal
Um estudo comparativo e a questão da interconexão com redes heterogêneas

Herbert Luna Galiano[1] Juergen Rochol[2]

Curso de Pós-Graduação em Ciência da Computação
Instituto de Informática, Universidade Federal de Rio Grande do Sul
Caixa Postal 15064
91501-970 Porto Alegre - RS

Resumo

Este trabalho visa apresentar uma revisão sobre os problemas de segurança em sistemas de comunicação sem fio, representados principalmente pelos sistemas de telefonia celular e os sistemas de comunicação pessoais PCS *(Personal Communications Systems)* emergentes. O trabalho também apresenta os principais aspectos de segurança implementados nos atuais padrões de telefonia celular. São abordados e avaliados, principalmente, os mecanismos de autenticação e privacidade dos sistemas AMPS, IS-95, IS-136 e GSM além das propostas, em termos de segurança, dos sistemas PCS emergentes. Também abordaremos a questão da segurança na interconexão de sistemas PCS com as redes de telefonia celular. Finalmente é apresentado uma proposta de arquitetura de protocolos, baseada no modelo RM-OSI, interconectando um sistema PCS, baseado no padrão J-STD-007, com a rede de telefonia celular IS-95.

Abstract

This work presents an overview of the security characteristics of Wireless Communication Systems, mainly represented by Telephone Cellular Systems and the emerging PCS systems (Personal Communication Systems). This work also presents the main features of security implemented in the current standardized Cellular Phone Systems. Our approach is mainly related to the characteristics of authentication and privacy of the standardized systems like AMPS, IS-95, IS-136 and GSM, apart of the proposals, regarding to the features of security, of PCS systems. Another issue that we present is about the integration of PCS with heterogeneous networks. Finally, we make a proposal of an protocol architecture, based on the RM-OSI model, related to the interconnection of a PCS system, J-STD-007, with the IS-95 cellular phone networks.

Palavras-Chave : Sistemas de Comunicação Pessoal, Telefonia Celular, Autenticação e Privacidade.

1. INTRODUÇÃO.

Atualmente está acontecendo uma explosiva evolução nos sistemas de comunicação sem fio ou *wireless*. Dos antigos sistemas de telefonia celular analógicos, estamos passando para novos conceitos de comunicações pessoais, móveis e universais. Na área das Telecomunicações, os sistemas *wireless* são um dos segmentos que apresentou o maior crescimento nestes últimos anos, com taxas de crescimento que são surpreendentes para a área. 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 sistemas *paging* está 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*.

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 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 da segurança em sistemas *wireless* acontecem freqüentemente e, a menos que sejam tomadas medidas específicas para preveni-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 *(Personal Communication Systems)* emergentes. Também abordaremos

[1] Mestrando do CPGCC da UFRGS e bolsista do CNPQ. Email: luna@inf.ufrgs.br
[2]Professor do Departamento de Informática Aplicada e do CPGCC. Email: juergen@inf.ufrgs.br

estes mesmos problemas, quando da interconexão destes sistemas, sugerindo uma arquitetura de protocolos segundo o modelo RM-OSI.

2. 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 1) [LI95]. Esta evolução acelerada é motivada em parte por uma vertiginosa demanda por mobilidade e portabilidade nas comunicações por parte dos usuários, que não foi prevista em seu início. Apoiando esta evolução, está também a revolução digital, pela qual estão passando atualmente todos os sistemas de telecomunicações.

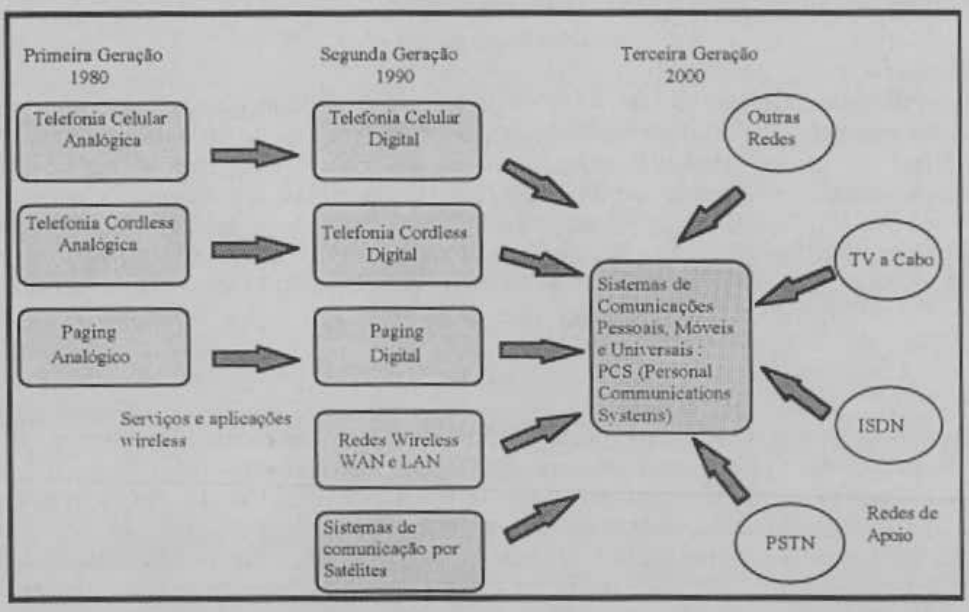

Figura 1 - Evolução dos Sistemas de Comunicação sem fio

A primeira geração de sistemas *wireless* está baseada em tecnologia analógica e foram desenvolvidas na década do 70. Sistemas típicos desta geração são a telefonia celular analógica, os sistemas *paging* e os sistemas analógicos de telefone sem fio *(cordles)*.

A segunda geração inicia com o advento, por volta do final da década de 80, das tecnologias digitais como o *spread spectrum* (espalhamento de espectro), as técnicas de acesso múltiplo como o CDMA *(Code Division Multiple Access)* e o TDMA *(Time Division Multiple Access)*, entre outras. A principal característica 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 *(Global System Mobile)*, desenvolvido pelos países europeus. Nos EUA surgem os sistemas USCD *(Uniited States Cellular Digital)*, sendo o IS-54 o primeiro deles e posteriormente o IS-195 e o IS-136. Já na telefonia *cordless*, emergem padrões digitais como DECT (*Digital European Cordless Telephone*) e o PACS (*Personal Access Communications Systems*).

Finalmente, 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. Entre eles estão os sistemas PCS dos EUA, o UMTS (*Universal Mobile Telecommunications*) da Europa, e o IMT-2000 (*International Mobile Telecommunications*) proposto pela ITU *(International Telecommunications Union)*. Estes sistemas todos têm características semelhantes e serão detalhados a seguir.

3. SISTEMAS 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 Multimídia de alta qualidade. Os sistemas *wireless* de terceira geração prometem fornecer uma ampla gama de serviços multimídia, com alta qualidade, como; voz, vídeo *(full motion ou limited)* e 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 pessoa, 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 1 [COO94].

Tabela 1 - Propostas em estudo para Padrões de Sistemas PCS

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
Arquitetura de rede adotado	Novo	Baseado no IS-95	Baseado no PACS	Baseado no IS-136	Baseado no GSM	Baseado no DECT	Baseado no IS-665
Categoria	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

4. SEGURANÇA EM SISTEMAS DE COMUNICAÇÃO SEM FIO.

As exigências quanto a segurança, em qualquer sistema de comunicações, são cada vez maiores. Infelizmente os sistemas *wireless*, pela sua natureza, utilizam como meio de comunicação um canal de RF (rádio freqüência) compartilhado, 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.
- 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.

5. ESTUDO COMPARATIVO DOS ASPECTOS DE SEGURANÇA EM REDES DE TELEFONIA CELULAR.

Dentro do JTC, como vimos, existem sete propostas de padronização, baseadas na maioria em sistemas de telefonia celular (ver Tabela 1), e está previsto que os sistemas PCS adotarão provavelmente padrões de segurança similares aos que são adotados atualmente na telefonia celular e sistemas *cordless* [BRO95]. Apresentaremos, 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.

5.1 Segurança no sistema de telefonia celular AMPS.

O padrão de telefonia celular AMPS (*Advanced Mobile Phone Systems*) pertence a primeira geração. No entanto, é o padrão mais difundido no mundo inteiro. Só nos EUA tem 40 milhões de assinantes, e é atualmente adotado também em praticamente todos os países da América Latina, inclusive o Brasil. O padrão AMPS foi elaborado pela TIA em conjunto com a EIA (*Electronic Industry Association*) através do documento TIA/EIA-533. O padrão adota modulação FM (*Frequency Modulation*) para a transmissão de voz, e modulação FSK (*Frequency Shift Keying*) para a sinalização. A técnica de multiplexação para compartilhar a banda é FDMA (*Frequency Division Multiple Access*). Os aspectos de segurança do sistema AMPS estão especificados na recomendação TIA/EIA 533 e TIA IS-41. A Figura 2 apresenta a arquitetura de uma rede AMPS, identificando os seus principais elementos estruturais :

- Estação Móvel, MS (*Mobile Station*). O MS é utilizado para o acesso aos serviços de telecomunicações oferecidos pelo sistema e nela está contido todo o equipamento necessário para realizar a transmissão pelo canal de rádio. O 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.
- 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.

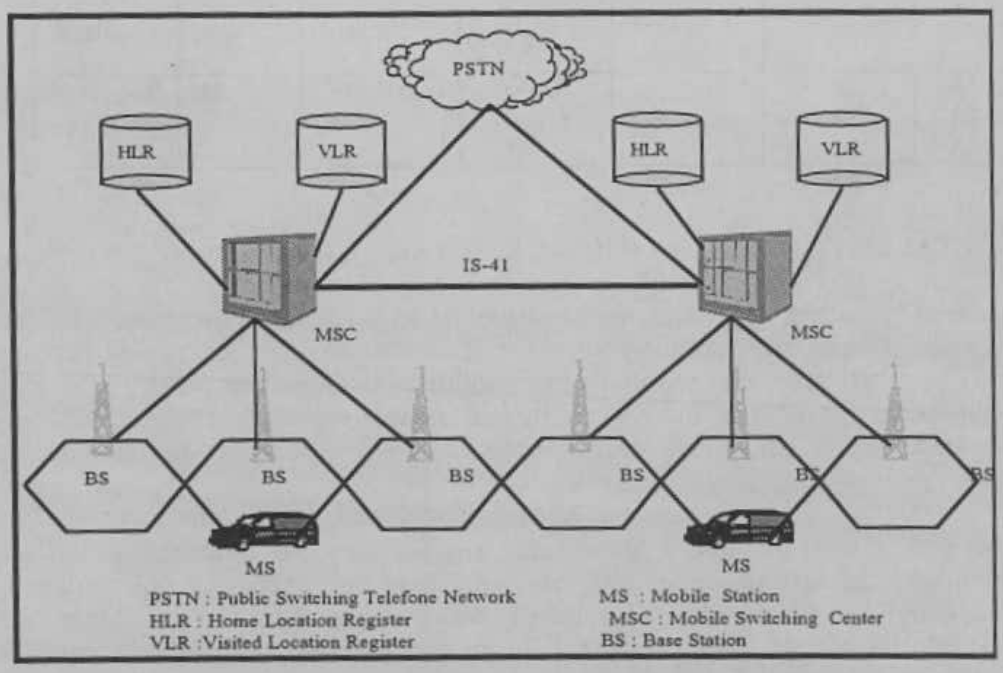

Figura 2 - Arquitetura e elementos da rede AMPS

5.1.1 Autenticação no AMPS.

Em sistemas AMPS, cada unidade móvel é identificada por dois parâmetros: o número de identificação do móvel, MIN (*Mobile Identification Number*), e o número de série eletrônico, ESN (*Electronic Serial Number*), os quais podem ser armazenados na estação móvel em uma memória

permanente, semi-permanente, ou temporária. O MIN é um número binário de 34 bits que é derivado a partir do número telefônico do usuário. Já o ESN é um número de 32 bits que identifica de forma unívoca a estação móvel em qualquer rede celular. No processo de autenticação estes parâmetros são intercambiados entre o 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 (*Home Location Register*), quando o MS está na rede de origem, ou no registro de localização de visita VLR (*Visited Location Register*), quando o MS está em *roaming*. Em ambos os casos, se os dados de identificação coincidirem, o MSC libera o serviço ou então nega a permissão.

5.1.2 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 o MS, BS e o MSC não tem nenhuma proteção. Isto inclui os parâmetros MIN e ESN, trocados durante o processo de autenticação.

5.2 Segurança em Sistemas de Telefonia Celular USCD.

Sistemas de Telefonia Celular Digital Americano, USCD (*United States Cellular Digital*), são todos aqueles padronizados pela TIA/EIA, ou seja, os IS (*Interim Standard*) IS-54, IS-136, e IS-95. No aspecto de segurança, todos estes padrões possuem mecanismos que são apoiados pelo padrão de sinalização IS-41. 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. A seguir apresentaremos uma breve descrição das características de cada um dos padrões USCD.

- Padrão IS-54. Foi o primeiro padrão de USCD, está baseado em técnicas TDMA e FDMA e opera no mesmo espectro usado pelos sistemas AMPS. O tipo de modulação digital usado é o ($\pi/4$ DQPSK). O IS-54 é *dualmode*, ou seja, permite operação em ambos os sistemas, AMPS (analógico) e IS-54 (digital).
- Padrão IS-95. Em 1992 foi submetido a 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, oferece uma alta capacidade de assinantes, excelente desempenho e baixo consumo de potência.
- Padrão IS-136. É um padrão de telefonia celular digital baseado no TDMA, na realidade é 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. Este padrão é conhecido comercialmente como D-AMPS.
- 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 na Figura 3. Entre eles está o MSC-G (*Gateway Mobile Switching Center*) e o AC (*Authentication Center*). Uma revisão atualizada, o IS-41-Rev.C, foi publicada em fevereiro de 1996 pela TIA.

Todos os sistemas USCD são apoiados pelo padrão IS-41, portanto as características de segurança são semelhantes entre eles, razão pela qual faremos um estudo único baseado no TIA/EIA IS-95. Vamos apresentar a seguir as principais características dos processos de autenticação e privacidade de uma rede típica USCD.

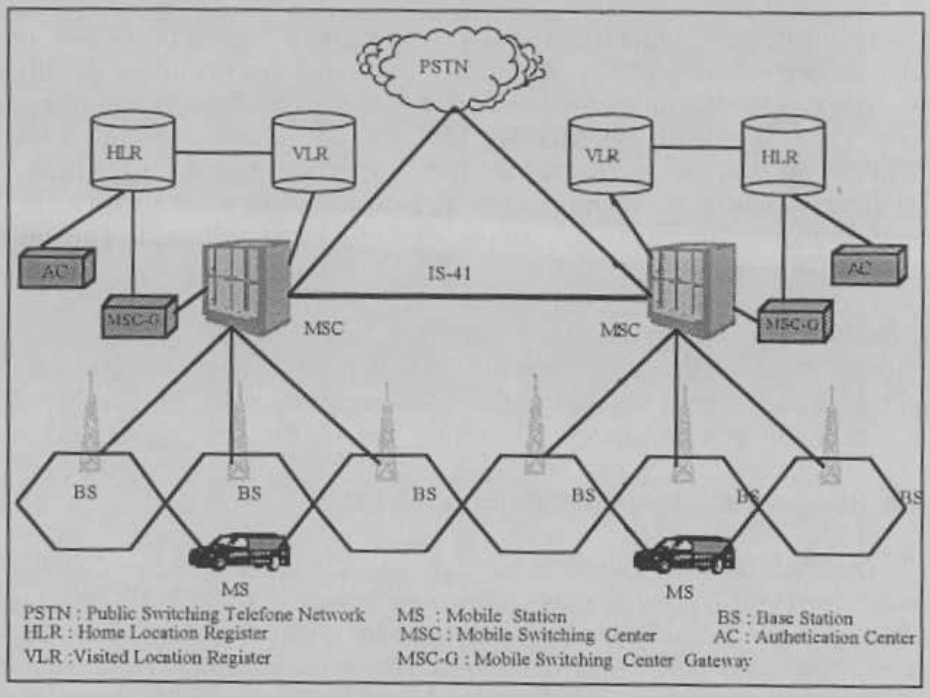

Figura 3 - Arquitetura da Rede USCD e a sinalização IS-41

5.2.1 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". Uma saída com sucesso do processo de identificação ocorre somente quando puder ser demostrado que a estação móvel e a estação base possuem um conjunto idêntico de dados secretos compartilhados. Um fluxograma simplificado deste processo é mostrado na Figura 4.

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 e não estão disponíveis no documento genérico TIA/EIA IS-95. 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). O SSD pode ser transportado do registro HLR (local) para o registro VLR (remoto) para fornecer autenticação quando a estação móvel está em *roaming*.
- 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.
- MIN (*Mobile Identification Number*). Número binário de 34 bits derivado do número Telefônico do Diretório. É Usado quando opera em modo analógico (AMPS).
- ESN (*Electronic Serial Number*). É um número binário de 32 bits que identifica de forma unívoca a estação móvel em qualquer sistema celular. É Usado quando opera em modo analógico.

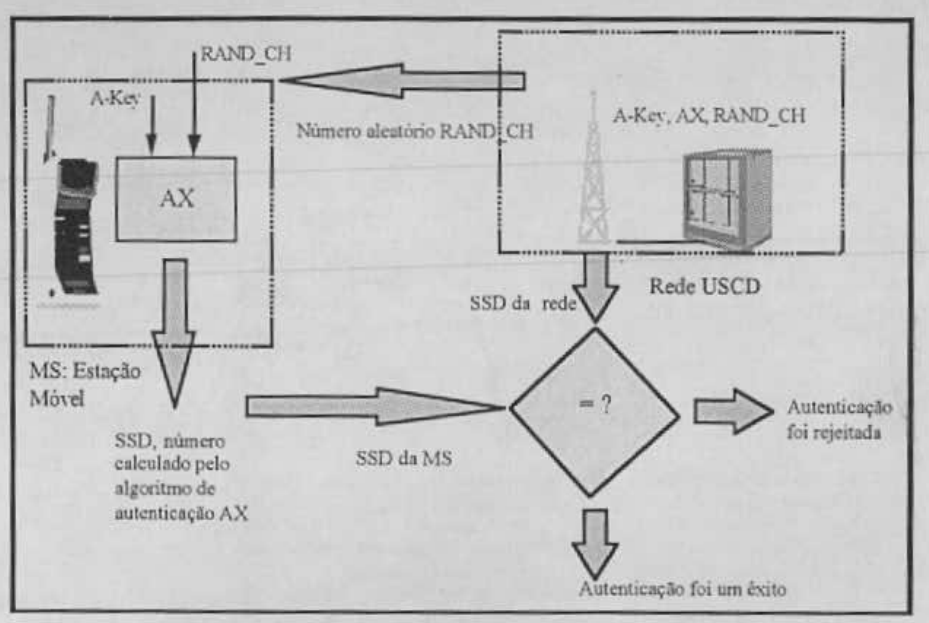

Figura 4 - Processo de autenticação em sistemas USCD

5.2.2 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 mecanismos de criptografia durante o processo de autenticação. Isto significa que o canal por onde trafegam voz ou dados, sob forma digital, também pode ser criptografado, garantindo desta forma privacidade. No documento original do TIA/EIA IS-95 esta informação (tamanho da chave, algoritmo de criptografia) é de acesso restrito.

5.3 Segurança em sistemas 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. 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)*. O 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 Station*), 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*), VRL (*Visited Register Location*), EIR *(Equipment Identity Register*) e o AUC *(Authentication Center).*

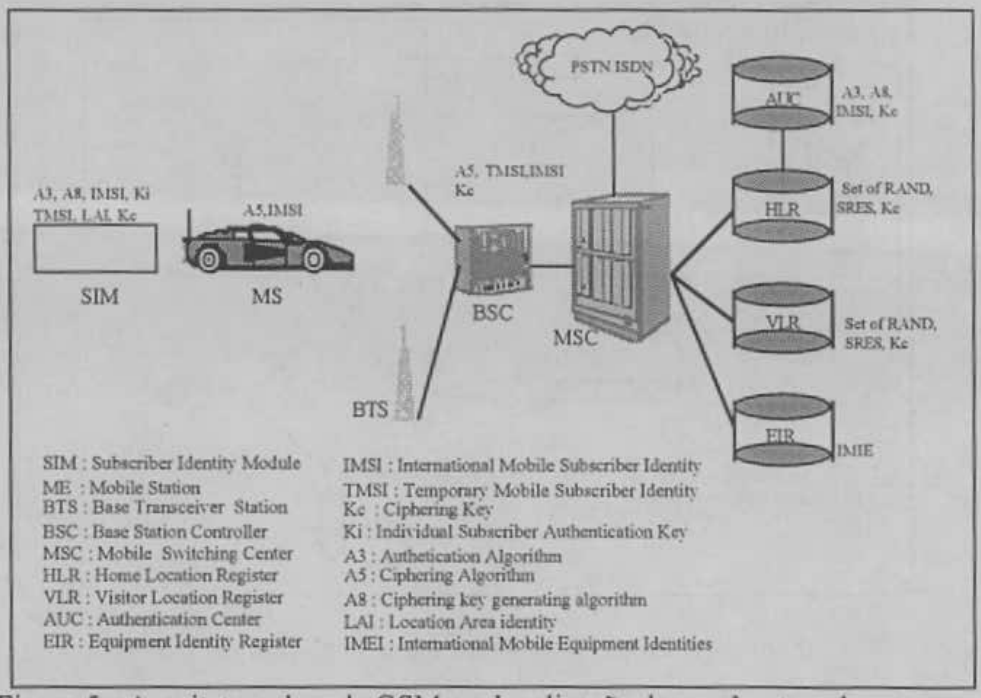

Figura 5 - Arquitetura da rede GSM e a localização dos parâmetros de segurança

Os aspectos de segurança do GSM são detalhados nas recomendações do ETSI. Não entanto certas informações são de acesso restrito, como por exemplo o tamanho das chaves e os algoritmos de criptografia. 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, sem ele o MS não é operável (exceto para ligações de emergência). O SIM fornece mobilidade pessoal e serve para identificar ao usuário. A Figura 5 mostra a distribuição dos parâmetros de segurança entre os elementos da rede GSM.

5.3.1 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 o 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 o 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 6.

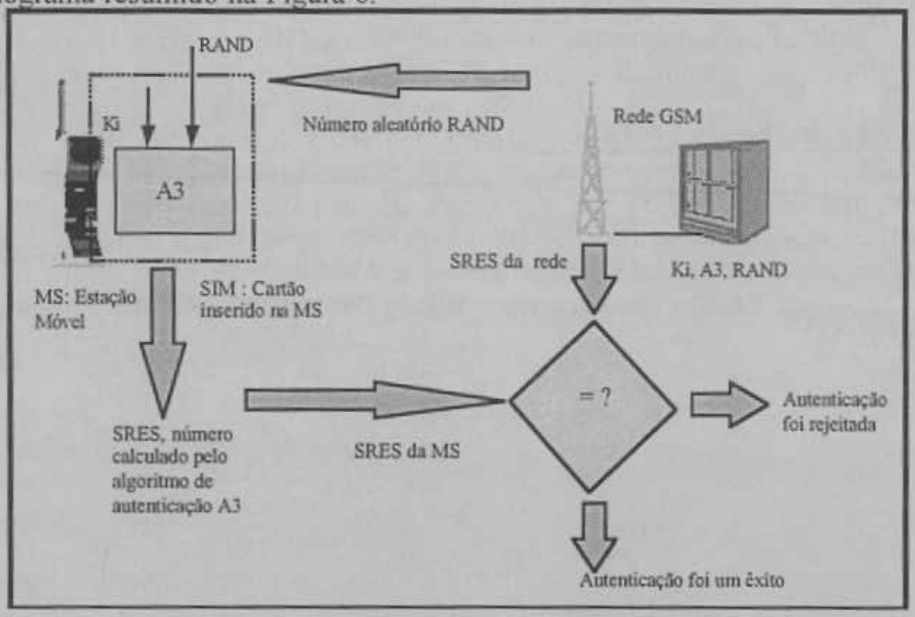

Figura 6 - Processo de Autenticação no GSM

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.

5.3.2 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 RAND e a chave Ki

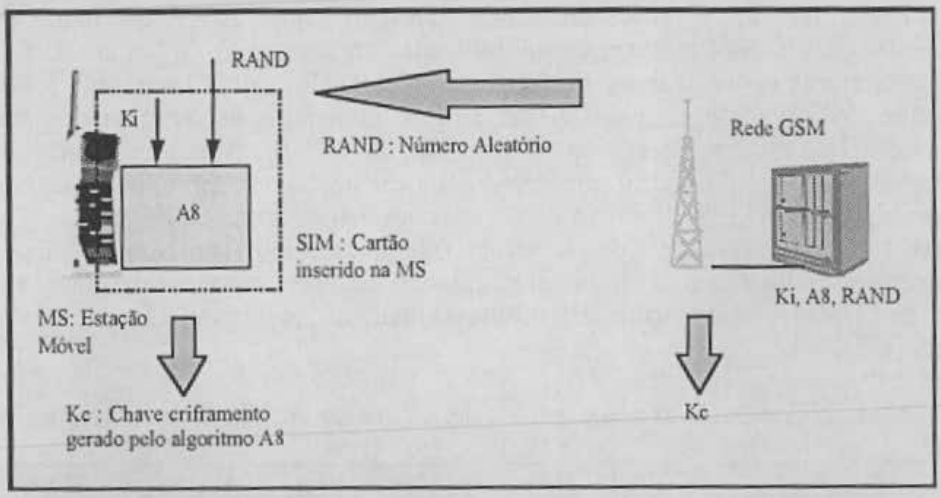

Figura 7 - Processo do calculo da chave de criptografia Kc

usados no processo de autenticação. Assim, Kc é usado para criptografar e decriptografar os dados entre o 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 aos ataques. A chave Kc pode ser trocada em intervalos regulares ou quando necessário por considerações de segurança da rede. A figura 7 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.

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, o MS começa a criptografar e decriptografar os dados usando o algoritmo A5 e a chave Kc. A Figura 8 mostra este processo.

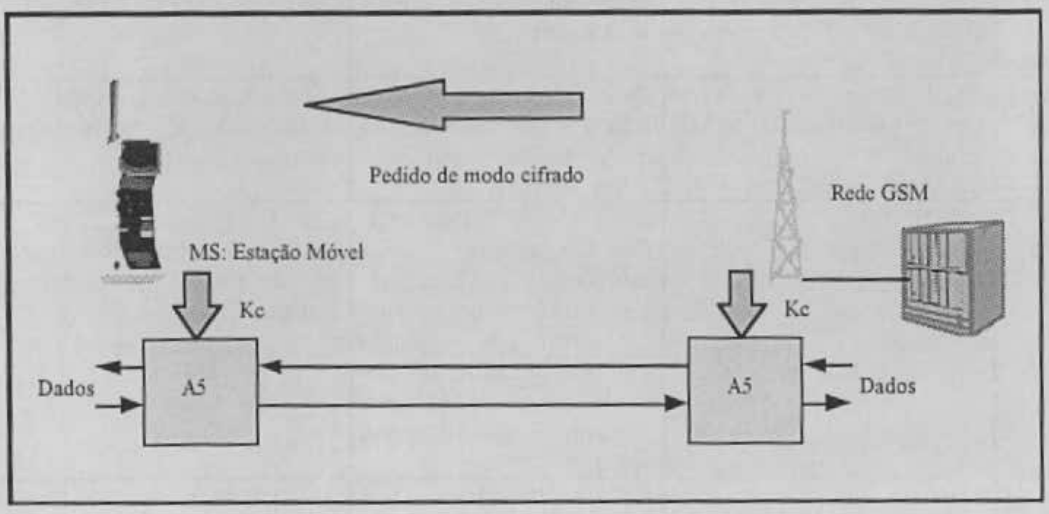

Figura 8 - Inicio do modo de comunicação cifrada

5.3.3 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 o 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 o 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.

5.4 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. Este é um tipo fraude denominada pelas operadoras como *cloning* do telefone celular. Um outro fator, que agrava ainda mais esta situação, 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)*. 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 demonstra mais ainda a vulnerabilidade dos sistemas AMPS [CEC96].

Tabela 2 Comparação dos aspectos de segurança em sistemas de telefonia celular.

	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 identifi-cação não são transmi-tidos pelo ar, por tanto não coloca em risco a segurança do sistema.	Procedimento desafio/ resposta, na qual os parâmetros de identifi-cação não são transmi-tidos pelo ar, por tanto não coloca em risco a segurança do sistema.
Mecanismos de privacidade.	Não utiliza.	Usa criptografia para proteção dos dados trafegados entre o assi-nante e a rede além dos dados de sinalização.	Usa criptografia para proteção dos dados trafegados entre o assi-nante e a rede além dos dados de sinalização.
Mecanismos de proteção da iden-tidade e localiza-ção do assinante	Não utiliza.	Usa criptografia e procedimentos de identi-ficação temporal.	Não disponível.
Facilidade de Interceptação e decodificação dos sinais de RF.	Fácil. *Scanners* que rastre-iam e interceptam sinais analógicos são fáceis de construir ou comprar.	Difícil. Usa canal digital, difícil de ser demodulado e decodificado por *sca-nners* simples.	Difícil. Usa canal digital, difícil de ser demodulado e decodificado por *sca-nners* simples.
Utilização de algoritmos de Criptografia.	Não utiliza.	Usa três algoritmos de chave privada, deno-minados A3, A8, e A5. Este último é um *stream cipher* ou seja é apoiado por mecanismos da ca-mada 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 ta-manho é 40 bits. Se des-conhece 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 nun-ca 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.

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 com 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].

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/DQPSK, 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].

Atualmente os sistemas de telefonia celular digitais o IS-95 (CDMA), o IS-136 (TDMA) e o 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 dual, 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 simultânea do sistema novo e antigo, segundo o modelo *dualmode*. Neste contexto, os novos sistemas, além de oferecerem uma alta capacidade de assinantes por célula, deverão oferecer principalmente, também, características de segurança altamente confiáveis.

O estudo comparativo apresentado mostra as características de segurança dos principais sistemas de telefonia celular, o que poderia servir como base para a especificação das características de autenticação e privacidade dos novos sistemas de telefonia celular a serem adotados pelas concessionárias. Em particular, a partir de um enquadramento dos diversos sistemas estudados, sugerimos um modelo que seja 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 USDC [MAR95]. Na Tabela 2 apresentamos um resumo dos aspecto de segurança dos principais sistemas de telefonia celular, AMPS, GSM e USCD da IS-95 e IS-136.

6. SEGURANÇA EM SISTEMAS PCS.

Sistemas PCS deverão oferecer serviços de comunicação de forma ubíqua (ou seja 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.

6.1 Caraterísticas de Autenticação e Privacidade desejadas em Sistemas PCS.

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

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 solicitados. 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].

6.2 Requisitos dos mecanismo de criptografia em 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 a 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 *handover* 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, será 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 a facilidade de ser gravado em memórias permanentes, semi-permanentes ou temporárias.

g) Requisitos em relação a aspectos legais. O governo pode autorizar judicialmente o grampeado 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.

6.3 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 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 a 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 o assinante este numa rede de visita *(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.

A Figura 9 apresenta um modelo geral do protocolo AKA com a seqüenciação dos três principais processos executados.

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 [NOE95], [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 internacionais organismos de padronização dos sistemas PCS.

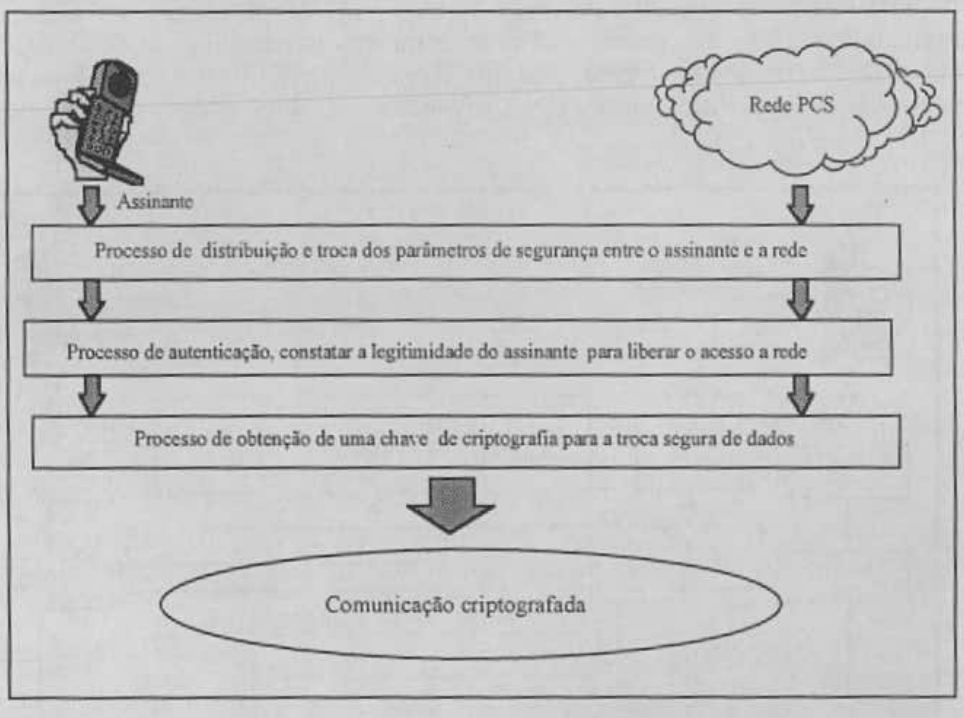

Figura 9 - Os três processos do modelo AKA.

6.4 Padronização dos mecanismos de segurança em 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 3 estão resumidos alguns aspectos de segurança de cada uma das propostas de padronização para sistemas PCS de acordo com o JTC.

Tabela 3 - 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	Ainda não definido	Ainda não definido

Os principais documentos relacionados com aspectos de segurança em PCS, publicados até aqui pelo Comitê T1 do ANSI [FRI94], são:

- *Privacy and Authentication Objectives for Wireless Access to Personal Communications, TR No.22, September 1993*
- *Privacy and Authentication, Vol.1, Common Requirements; Vol.2, GSM Specific Requirements; Vol.3, IS-41 Specific Requirements.*

Além destes padrões, existem ainda várias outras sugestões e propostas que ainda estão em fase de estudos, podendo eventualmente serem padronizadas.

7. INTERCONEXÃO DE REDES HETEROGÊNEAS COM SISTEMAS PCS.

É um fato que os serviços PCS serão fornecidos por múltiplas redes regionais, 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 alguma interface de conexão confiável para facilitar a inter-operabilidade entre elas. Atualmente a interconexão das redes de telefonia celular é feita usando a rede pública comutada (PSTN); em outros casos, como na rede GSM, é através de uma interface especial conhecida como IWF (*Interworking Function*), e para PCS está sendo considerada uma unidade de interconexão de rede, a mesma que está sendo denominada pela literatura especilializada como IIF (*Interworking Interoperability Function*) [HUS96]. Uma IIF deverá obedecer a os protocolos de sinalização da rede Inteligente AIN (*Advanced Intelligent Network*), como por exemplo o SS7 *(Signaling System No. 7).*

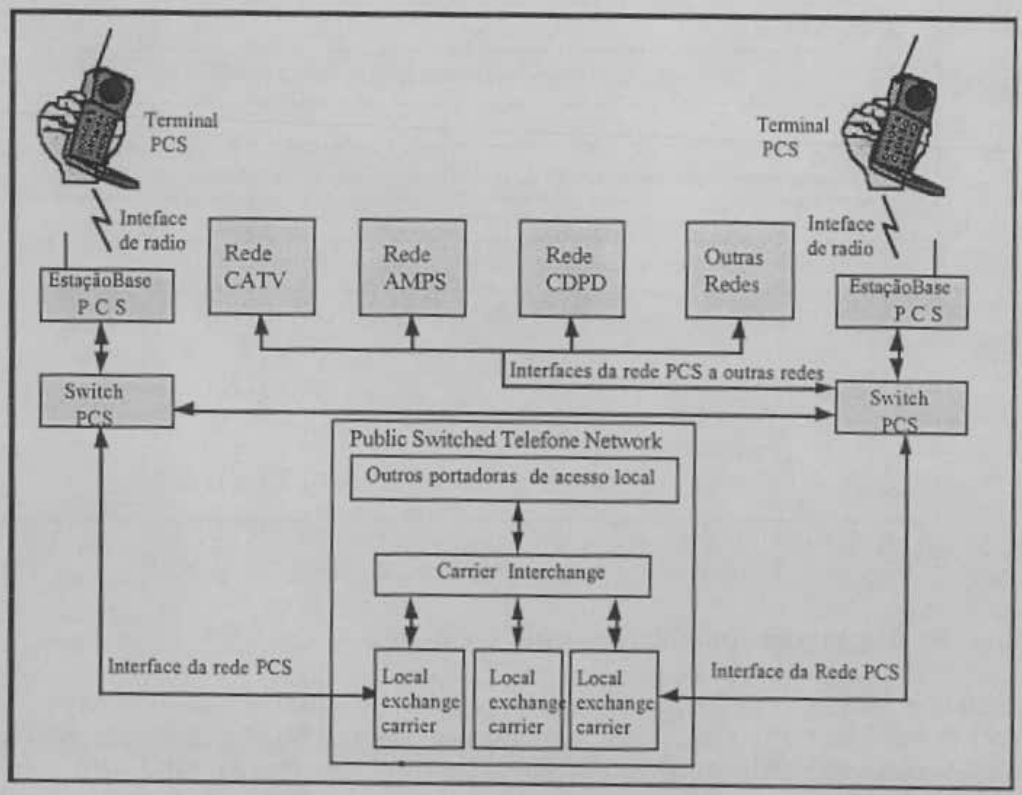

Figura 10 - Interconexão de redes heterogêneas com sistemas PCS

De outro lado, sendo o principal objetivo dos sistemas PCS oferecer a mobilidade pessoal e do terminal, também será necessário que os sistemas PCS interajam de forma compatível com as diversas redes de telecomunicações 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 precisam de uma interface de conexão adequada, a qual deverá estar suficientemente padronizada para tornar possível níveis de comunicações confiáveis. Na Figura 10 representamos a interconexão para 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

possivel, o assinante deverá ter um único *handset* do tipo *multimode*, possibilitando assim a operação em múltiplos ambientes de PCS.

7.1 Segurança na interconexão de redes heterogêneas com sistemas PCS.

As vantagens da interconexão com redes heterogêneas, ou seja, a mobilidade pessoal e o *roaming* universal, colocam os sistemas PCS em uma 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]. Isto nos leva a considerar dois aspectos importantes: primeiro, adotar fortes mecanismos de autenticação e privacidade; e, segundo, projetar interfaces de conexão de alta confiabilidade.

Na tabela 4 é mostrada a confiabilidade da interconexão de Sistemas PCS (baseado no modelo AKA) com as diferentes redes de telefonia celular atuais; AMPS, USCD e GSM. São apresentados duas situações; uma delas quando o *handset* PCS está operando em *roaming*, e a outra quando o *handset* PCS estabelece uma comunicação ponto a ponto.

Tabela 4. Confiabilidade da conexão de redes PCS com redes heterogêneas

Interconexão de Redes Rede-interface-Rede	Autenticação *(Roaming)*	Privacidade *(Roaming)*	Localização *(Roaming)*	Privacidade (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

8. CONCLUSÕES

Pela analise e discussão dos aspectos de segurança em sistemas de telefonia celular e sistemas PCS apresentada, podemos concluir que os sistemas PCS emergentes, provavelmente, adotem 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 2), também pode ser estendido aos sistemas PCS. A partir de um enquadramento dos diversos sistemas estudados, sugerimos um modelo de segurança que seja baseado no protocolo AKA, e em especial da arquitetura GSM.

Também foi feita uma rápida análise referente a questão da interconexão de redes heterogêneas *wireless* com sistemas PCS, a partir da qual conclui-se que os aspectos de autenticação e privacidade vão depender, principalmente, das caracteristicas próprias de cada uma das redes envolvidas na interconexão, bem como do tipo de interface considerada (ver Tabela 4).

Acreditamos que a construção de uma interface confiável deverá ser uma das primeiras etapas a ser resolvida na interconexão de redes heterogêneas PCS. Neste sentido, estamos propondo uma arquitetura de protocolos, baseada no modelo RM-OSI, que representa a interconexão de uma rede PCS padrão J-STD-007 (baseado no GSM), com uma rede de telefonia celular IS-95 (digital americano). A interface proposta é uma IIF (*Interworking Interoperability Function*), e está baseada em mecanismos de sinalização SS7, conforme é mostrado na Figura 11.

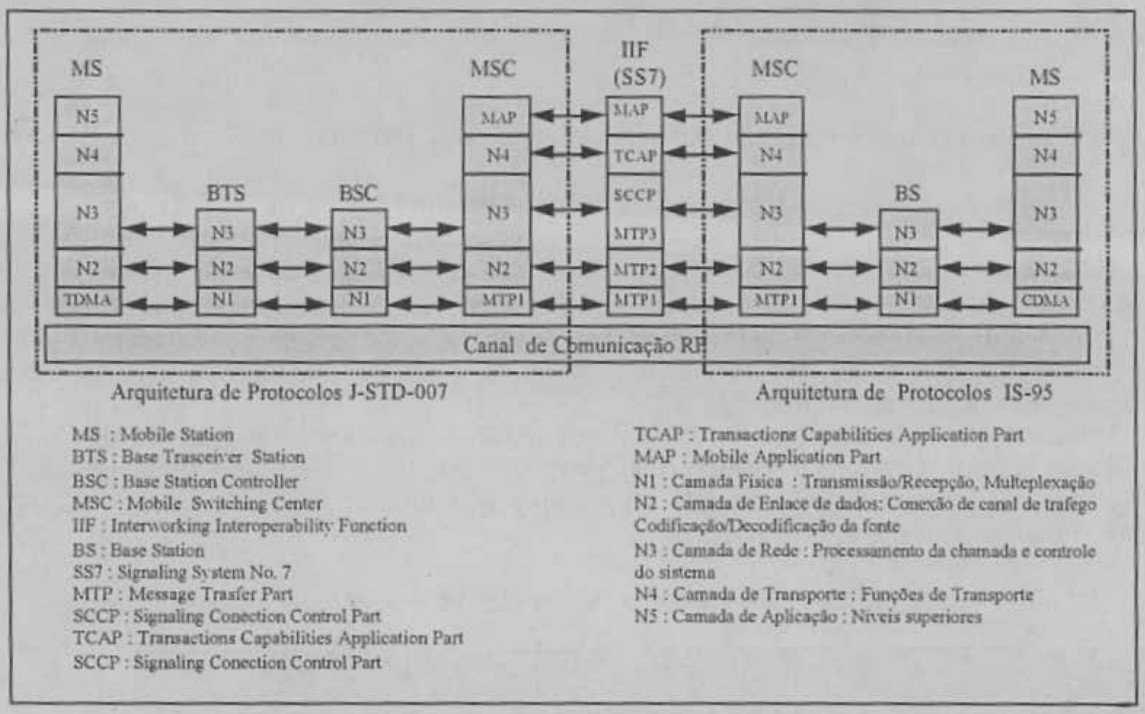

Figura 11 - Arquitetura de protocolos representando a interconexão de uma rede PCS com uma rede de telefonia celular

Finalmente, no que diz respeito à interconexão de redes PCS heterogêneas, deverão ser aprofundados os estudos relativos a uma interface do tipo IIF que permita a interoperabilidade de sistemas PCS com ambientes heterogêneos, que acreditamos, será a questão fundamental na área do desenvolvimento de sistemas de comunicação móveis, pessoais e universais nos próximos anos.

9. REFERÊNCIAS BIBLIOGRÁFICAS

[BEL93] BELLER, M. J. **Fully -Fledged Two Way Public-Key Authentication and Key Agreement for Low Cost Terminals.** Electronic Letters, May 1993, Vol 29, Nro.11, pp. 999-1001.

[BRO95] BROWN, DAN. **Techniques for Privacy and Authentication in PCS**. IEEE Personal Communications, August 1995, pp.6-10.

[CAR96] CARNEIRO, H., SANTIVAÑES, J., BOISSON R. **Arquitetura e Sinalização em Redes Celulares**. Anais do XIV Simpósio Brasileiro de Telecomunicações, Julho 1996, pp. 773 -778.

[CEC96] CECILIO, NILO. **Guerra ao Clone** Revista Nacional de Telecomunicações RNT. Agosto 1996, Ano 18, Nro. 204, pp. 13-16.

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

[COX95] COX, C. DONALD. **Wireless Personal Communications : What Is It ?**. IEEE Personal Communications. April 1995, pp. 20-35.

[FRI94] FRISON, BRAD. **Preparing the Way for PCS**. IEEE Personal Communications. Fourth Quarter 1994, pp. 10-11.

[HUS96] HUSAIN, SYED. **Intelligent Network : A key Plataform for PCS Interworking and Interoperability.** IEEE Communications. October 1996, pp. 98-106

[LI95] LI, OK. VICTOR, XIAOXIN QIU. **Personal Communications Systems (PCS)**. Procedings of the IEEE. September 1995, pp. 1210-1243.

[LIN95] LIN, HUNG-YU. **Authentication Protocols for Personal Communications Systems**. Proceedings of ACM SIGCOMM '95. September 1995, pp. 256-261.

[LOB96] LOBO, ANA PAULA. **Guerra contra o fraude**. Computer World IDG Brasil. Setembro 1996, p. 12.

[LUX95] LUXNER, LARRY. **El Fin de La Linea?**. CommunicationsWeek Latinoamerica. Año 2, Número 2, Segundo Trimestre 1995, pp. 16-17

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

[NOE96] NOERPEL, ANTHONY. **PACS: An Alternative Technology for PCS.** IEEE Communications. October 1996, pp, 138-150.

[PAN95] PANDYA, RAJ. **Emerging Mobile and Personal Communications Systems.** IEEE Communications Magazine. June 1995, pp, 75-82.

[SCO96] SCOURIAS, JOHN. **Overview of the GSM.** http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html, March 1996.

[SIQ96] SIQUEIRA, ETHEVALDO. **Conhecendo o CDMA**. Revista Nacional de Telecomu-nicações RNT. Ano 18 Nro. 208-A, Dezembro 1996, pp 4-5.

[TIA94] TELECOMMUNICATIONS INDUSTRIES ASSOCIATION. **Security And Identification.TIA/EIA/Interim Standard IS-95**. TIA/EIA. March 1994, pp. 2-8.

[WIL95] WILKES, JOSEPH. **Privacy and authentications Needs of PCS**. IEEE Personal Communications. August 1995, pp. 11-15.

[YAC95]YACOBI, YACOB. **Security for Wireless Systems**. IEEE Personal Communications. August 1995, p. 2.