Universidade Estadual de Campinas
Unicamp

Redes GSM e GPRS

Prof. Dr. Omar Branquinho

Luis Fernando B Braghetto
Sirlei Cristina da Silva
Marcelo Lotierso Brisqui
Paulo da Costa

Pós Graduação em Redes Computadores

Índice

Índice de Figuras

Capítulo 1 – Histórico dos meios de transmissão e sua evolução

1.1 – Apresentação

GSM, que significa *Global System for Mobile Communications*, é um sistema aberto, não proprietário. Seu grande diferencial é a capacidade de funcionamento em mais de 170 países. Ele consegue atingir áreas que a cobertura terrestre não alcança.

O GSM difere da primeira geração de sistemas sem fio no uso de tecnologia digital e métodos de transmissão TDM. A voz é codificada digitalmente via um único codificador, que emula as características da fala humana.

O serviço do GSM envolve alta velocidade, serviços de dados multimídia em sistemas sem fio.

A primeira geração de telefones celulares era analógica. No entanto, a geração atual é digital. A transmissão digital tem várias vantagens em relação à analógica para comunicação móvel. Primeiro, a comunicação de voz e dados pode ser integrada em um único sistema. Segundo, quanto mais algoritmos de compactação de voz forem descobertos, menos largura de banda será necessária por canal. Terceiro, os códigos de correção de erros podem ser usados para melhorar a qualidade de transmissão. Por último, os sinais digitais podem ser criptografados para aumentar a segurança.

Existem diferentes padrões no mundo, como o ISO-54 (norte-americano) e o JDC (japonês). Ambos foram criados para serem compatíveis com o analógico, de forma que cada canal AMPS poderia ser usado para comunicação analógica ou digital.

Por outro lado, o sistema digital europeu GSM *(Global System for Mobile Communications)*, foi criado desde o início como um sistema totalmente digital, sem qualquer compromisso em relação a retrocompatibilidade.

Outra característica do sistema GSM é que os aparelhos são habilitados com um pequeno cartão chamado SIM. Assim, por exemplo, o proprietário do celular pode viajar para a França ou Alemanha sem ter de trocar o número de telefone, levando apenas o cartão. Basta instalá-lo em um aparelho local. A agenda também é mantida.

1.2 – Datas, coberturas, concessões

Em 1982, a Conferência Européia de Correios e Telecomunicações (CEPT), da qual participavam as administrações das telecomunicações de 26 países europeus, estabeleceu o *Groupe Spéciale Mobile*. Tal grupo desenvolveu um conjunto de padrões para o que então foi chamado de Rede de Rádio Digital Celular Pan-Européia. Este sistema agora chamado *Sistema Global para Comunicação Móvel*, foi projetado com o intuito de fornecer uma interface comum de rede/terminal e permitir a capacidade de movimentação por toda a Europa. Os vários sistemas analógicos que estavam sendo desenvolvidos na época eram largamente superados em termos de redução de custos por um sistema comum como este.

O trabalho de especificação continuou e em 1987 treze operadoras européias assinaram um Memorandum de Acordo (MoU). Este documento forneceu a indicação esperada pelos fabricantes para que pudessem iniciar com o processo de desenvolvimento

do sistema. Os julgamentos da época conduziram à escolha do TDMA de faixa estreita (*narrowband Time Division Multiple Access*) como a interface aérea utilizada pelo sistema. Em 1989, o trabalho de padronização foi passado para o então criado ETSI. Foi tomada então uma decisão de completar a especificação e desenvolvimento do sistema em duas fases, com a primeira fase entrando em operação comercial em meios de 1991.

O desenvolvimento das especificações GSM dentro do ETSI era responsabilidade do *Special Mobile Group (SMG) Technical Committee*, que era compreendido de subcomitês técnicos trabalhando em:

- Serviços (STC-SMG1)
- Aspectos de Rádio (STC-SMG2)
- Aspectos de Redes (STC-SMG3)
- Serviços de Dados (STC-SMG4)
- Operações, Administração e Manutenção (OA&M) (STC-SMG6)

O GSM foi originalmente criado para uso na banda de 900 MHz. Mais tarde, as freqüências passaram a ser alocadas em 1.800 MHz (banda D), e um segundo sistema, cujo padrão se baseava no GSM, foi configurado. Esse padrão é denominado DCS 1800, mas na verdade ele é basicamente o GSM.

Entre as prestadoras do serviço estão a Oi (que opera no Rio de Janeiro, Minas Gerais, Espírito Santo, Nordeste e Norte) e a TIM (que tem concessão para oferecer serviços em São Paulo e nas regiões Sul e Centro-Oeste do país).

No Brasil, a idéia é a de até o fim de 2004 oferecer serviços GSM em todas as 471 cidades hoje cobertas pela tecnologia TDMA. Por hora, a cobertura GSM estará restrita às regiões metropolitanas.

1.3 – Das redes analógicas aos avançados meios de transmissão voz sobre IP

Na figura abaixo, podemos verificar em qual época surgiram os sistemas analógicos e sua evolução. São os chamados sistemas da 1G (1ª geração) e suas evoluções. (2G, 3G, etc)

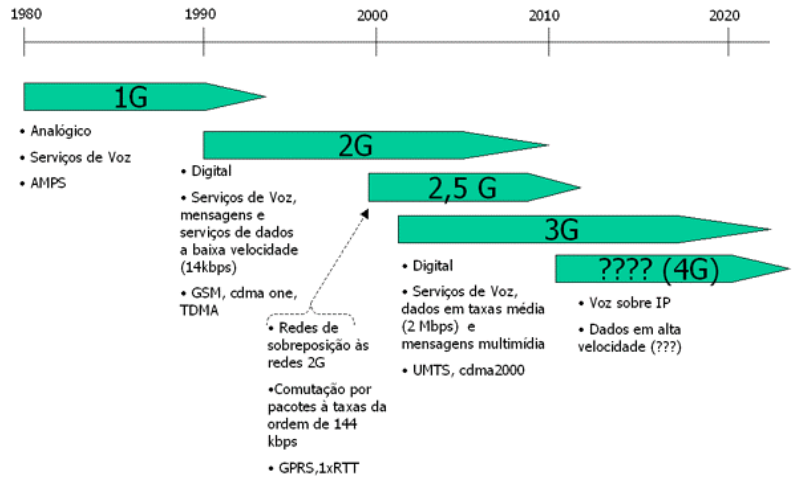

Figura 1: Histórico do 1G, 2G, 3G, 4G

Para ilustramos ainda melhor, comparemos com as inovações tecnológicas desde 1760. Verifique que tivemos o "boom" da eletricidade, carros, aviões, televisores, computadores, bio-tecnologia e INTERNET MÓVEL. O GSM se encaixa nesta inovação (iniciou numa conferência em 1982).

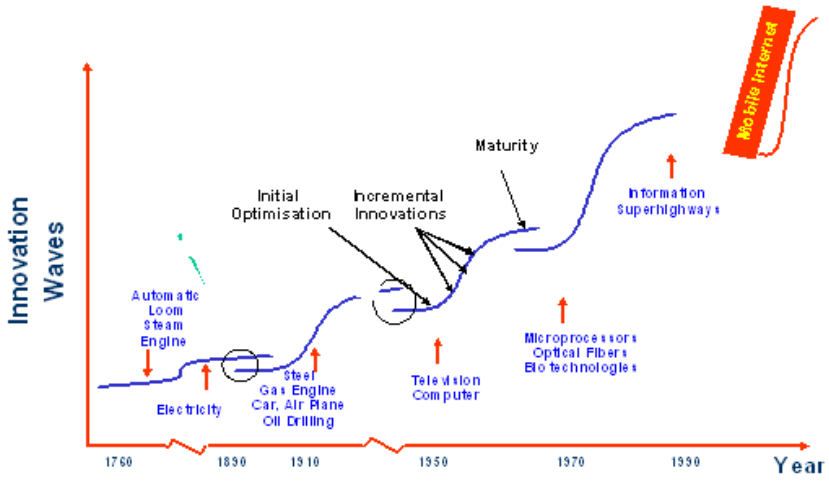

Figura 2: Histórico das Tecnologias Modernas

1.4 – Tendências

Em reportagem recente, o jornal do Brasil explicou uma tendência de tecnologia em altas velocidades. Trata-se do Edge, uma evolução do GPRS. (deve estar disponível comercialmente em 2004, pela operadora Claro)

Abaixo trecho da matéria:

"Quem sonha em acessar a internet de qualquer lugar e no momento que quiser poderá fazê-lo com mais tranqüilidade com o lançamento no Brasil da tecnologia Edge. Ela permitirá a transmissão de dados em redes GSM em alta velocidade, e sua data de lançamento está prevista para o meio de 2004.

O Edge é a evolução do GPRS, que transmite dados em uma velocidade próxima a de uma conexão discada e que está disponível no Brasil através da Oi e Tim. A nova tecnologia chegará quando a Claro lançar comercialmente sua operação em GSM, marcada para outubro de 2003. Enquanto a velocidade do GPRS está próxima dos 40 Kbps, a do Edge é três vezes maior, de até 120 Kbps.

A primeira operadora a lançar comercialmente a tecnologia foi a Cingular, nos Estados Unidos, em junho de 2003. A rede Edge da Claro já está pronta e as estações estão sendo produzidas no Brasil, mostrando como o mercado de telecomunicações do país se tornou dinâmico - diz o vice-presidente da Ericsson Brasil, Jesper Andersen.

No entanto, para que os consumidores possam desfrutar da alta velocidade do Edge, precisarão de um telefone que ofereça suporte à nova tecnologia. Os fabricantes esperam lançar os celulares apenas no começo de 2004 - a Claro deve demorar alguns meses testando-os antes de iniciar a operação comercial. A Sony e Ericsson tem uma placa para notebooks que ainda não foi lançada comercialmente, e a Nokia, apesar de já vender um telefone Edge nos Estados Unidos, levará alguns meses para colocar o aparelho no Brasil.

Em compensação, desde o primeiro dia da nova operação da Claro seus clientes poderão transmitir dados com o GPRS, e o Edge permite que os dados sejam transmitidos de maneira mais eficiente mesmo com os atuais telefones. Isso garantiria um preço mais baixo para a transmissão dos dados, mas não deve acontecer tão cedo.

Vamos chegar com o preço de mercado para transmissão de dados. O preço do GPRS só deverá baixar meses depois do Edge se popularizar. Ou seja, não deve acontecer nem no próximo ano - revela o gerente de Marketing de Serviços da Claro, Marco Catorze.

Quando for lançado, o Edge atenderá quem usa muito o notebook ou o PDA e deseja ter acesso à internet em qualquer lugar, sendo mais rápido que o 1xRTT oferecido pela Vivo e o GPRS da Oi, Tim e da própria Claro. Em um ou dois anos aparecerão os telefones celulares que aproveitarão o potencial oferecido pela alta velocidade da rede para criar novas aplicações: pense em jogos disputados em rede, recepção de vídeo no telefone e teleconferência a baixo custo. São muitas das funcionalidades prometidas para a terceira geração, que exige uma mudança total na atual tecnologia dos telefones celulares e novas concessões públicas - apenas a videoconferência por telefone celular continua fora do alcance do Edge.”

Vale lembrar que o sistema GSM é o mais utilizado do mundo, presente em 70% dos telefones móveis e em 172 países. Ele é um serviço que opera nas bandas D e E, faixas de freqüência liberadas pela Anatel para aumentar a competição na área de telefonia no país. Somam-se aos serviços de banda A e B. Uma importante diferença entre as bandas é a cláusula no contrato Anatel que diz que as empresas da banda A e B, obrigatoriamente, tem que oferecer serviço tanto analógico quanto digital. Enquanto isso, as novas operadoras podem funcionar somente em modo digital e não tem de dar cobertura de celular em todo o território nacional.

Capítulo 2 – Conceitos dos Meios de Transmissão

Basicamente, o GSM é baseado em comutação por circuito. Um computador móvel com um modem especial pode fazer uma chamada usando um telefone GSM da mesma maneira que o faria com um telefone conectado por fio. Vamos entender um pouco mais o que é “Comutação por circuito”, bem como outros métodos existentes.

2.1 – Comutação por Circuitos

Uma rede comutada por circuitos é um tipo de rede no qual o caminho físico é obtido e dedicado para uma única conexão entre dois end-points (hosts) durante o tempo da conexão. O serviço de voz telefônica é deste tipo. A companhia reserva um caminho específico para o número que você discou durante a sua ligação. Durante este tempo, ninguém pode usar as linhas físicas envolvidas. Comutação por circuitos é o contraste de comutação por pacotes.

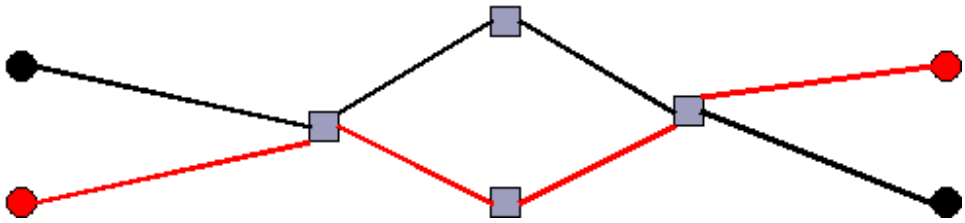

Figura 3: Redes de Circuitos x Redes de Pacotes

Um caminho de comunicação dedicado é estabelecido entre duas estações através dos nós da rede nas redes com comutação por circuitos.

O caminho dedicado é chamado uma conexão comutada por circuito.

Um circuito ocupa uma capacidade fixa de cada ligação durante o tempo da conexão. A capacidade não utilizada pelo circuito NÃO PODE ser usada por outros circuitos.

Vantagens:

1. Largura da banda fixa, capacidade garantida (nenhuma congestionamento).
2. Variação do atraso fim-a-fim baixo (atraso é quase constante).

Desvantagens:

1. Iniciar e Terminar conexões introduz overhead.
2. Utilizador paga o circuito, mesmo quando não utiliza.
3. Outros utilizadores não podem usar o circuito nem sequer se estiver livre de tráfego.
4. Tráfego entre computadores é freqüentemente desigual, deixando a conexão ociosa a maior parte do tempo.
5. Remetente e receptor precisam enviar e receber a mesma taxa.

6. Quando circuito está ocupado, ou no máximo da capacidade, as novas conexões ficam bloqueadas.

2.2 – Comutação por Pacotes

Descreve o tipo de rede no qual os pacotes são roteados através da rede baseado no endereço de destino contido no pacote. Este tipo de comunicação entre o remetente e o destinatário é conhecido como conexão sem estado. A Internet é baseada em comutação por pacotes.

Vantagens
1. Comutação por pacotes utiliza recursos mais eficientemente;
2. Tempo de iniciar e terminar ligações é muito pequeno;
3. É mais flexível (ex. não se preocupa muito com o que é enviou, desde que seja possível colocar em formato de pacote);
4. Emissor e receptor podem transmitir a taxas diferentes;
5. Tipos diferentes de computadores podem comunicar em rede de comutação por pacotes;
6. Redes de comutação por pacotes não recusam uma conexão; no máximo, atrasam a ligação até que o pacote possa ser transmitido;
7. Comutação por pacotes consegue gerir tráfego impulsivo (burst). É mais usado nas redes de computadores;

Desvantagens
1. Nenhuma garantia nos atrasos;
2. Algoritmos são mais complexos;
3. Demasiados pacotes poderão conduzir a um congestionamento da rede comutada por pacotes: pacotes que não são guardados ou entregues podem ser descartados;
4. Pacotes podem chegar a tempos diferentes e numa ordem diferente de aquela em que foram enviados: problemático para uma conversa telefônica.

2.3 – Comutação por Circuitos x Comutação por Pacotes

Os que se opõe à comutação por pacotes, defendem que ela não é apropriada para serviços de tempo-real. (por exemplo: ligações telefônicas e vídeo conferência), por causa da variação e da não previsão do delay fim-a-fim.

Já os que defendem, dizem:

- comutação por pacotes oferece melhor compartilhamento da banda que comutação por circuitos;
- é mais simples, eficiente, e de custo menor para implementar do que a comutação por circuitos.

2.4 - TDMA

Acesso por múltipla divisão do tempo (TDMA - *Time Division Multiple Access*) é uma tecnologia de transmissão digital que permite um número de usuários acessar um único canal de freqüência de rádio sem interferência, locando um único slot (espaço) de

tempo para cada usuário dentro de cada canal. O esquema de transmissão digital TDMA multiplexa três sinais sobre um único canal. O TDMA padrão para celular divide um único canal em seis slots de tempo, com cada sinal usando dois slots, providenciando um ganho em capacidade de 3 para 1 sobre o AMPS. A cada usuário é concedido um slot de tempo especifico para transmissão.

O problema central do sistema de comunicação celular é a escassez do espectro. Isto significa que o sistema celular necessita usar seu espectro de rádio limitado da maneira mais eficiente possível. Empresas estão solucionando este desafio de duas maneiras. A primeira envolve a gradual mudança do formato do sinal de analógico para digital, pois permite um sistema celular empregar menos estações base. O segundo método emprega a modulação de fase digital para permitir um grupo de usuários utilizar o mesmo canal de freqüência de rádio simultaneamente.

Nos anos 80, a indústria da comunicação sem fio começou explorar a conversão da rede analógica existente para digital com o intuito de aperfeiçoar a capacidade. Em 1989, a *Cellular Telecommunications Industry Association* (CTIA) escolheu TDMA ao invés do FDMA da Motorola (hoje conhecido como NAMPS) padrão banda estreita como a tecnologia alternativa dos mercados de celular de 800 MHz existentes e para os emergentes mercados de 1.9 GHz. Com o crescimento da competição tecnológica aplicada pela Qualcomm em favor do CDMA e as realidades do padrão GSM Europeu, o CTIA decidiu permitir as empresas a fazerem suas próprias escolhas de tecnologia.

Os dois maiores sistemas (concorrentes) que dividem a rádio-freqüência (RF) são TDMA e acesso por múltipla divisão do código (CDMA – *Code Division Multiple Access*). Como veremos adiante, CDMA é uma tecnologia de espectro amplo que permite múltiplas freqüências serem usadas simultaneamente. Cada pacote digital de códigos CDMA é enviado com uma única chave. Um receptor CDMA responde somente para aquela chave e pode indicar e demodular o sinal associado.

Por causa desta aceitação pelo sistema global de padronização Europeu para comunicações móveis (GSM) a *Japanese Digital Cellular* (JDC), e a No*rth American Digital Cellular* (NADC), o TDMA e suas variantes são concorrentes à tecnologia a ser adotada por todo o mundo. Porém, nos últimos anos, um debate tem agitado a comunidade da comunicação sem fio sobre os respectivos méritos do TDMA e CDMA.

O sistema TDMA é designado para uso em uma variedade de circunstâncias e situações, que vão do uso em um escritório no centro da cidade até um usuário viajando em alta velocidade em uma rodovia. O sistema também suporta uma variedade de serviços para fins do usuário, tal como voz, dados, fax, serviços de pequenas mensagens, e difusão de mensagens. O TDMA oferece uma flexível interface aérea, provendo alta performance a respeito de capacidade, cobertura, e ilimitado suporte de mobilidade e capacidade para tratar dos diferentes tipos de necessidades do usuário.

2.5 - CDMA

O CDMA (*Code Division Multiple Access*) permite que cada estação transmita em todo o espectro de freqüência continuamente. Várias transmissões simultâneas são separadas através do uso de resultados da teoria de codificação. O CDMA também não pressupõe que os quadros envolvidos em uma colisão estejam totalmente danificados. Em vez disso, ele pressupõe que vários sinais são emitidos linearmente.

Consideremos a teoria do “coquetel” de acesso a canais. Em uma sala grande, vários pares de pessoas estão conversando. O TDM representa quando todas as pessoas estão no meio da sala, mas falam de forma alternada, primeiro uma e depois a outra. O FDM representa quando o grupo de pessoas está separado em blocos, cada um mantendo uma conversa ao mesmo tempo, mas ainda de forma independente das outras. O CDMA representa quando todas as pessoas estão no meio da sala falando ao mesmo tempo, mas cada par em um idioma diferente. A dupla que fala francês só se comunica nesse idioma, rejeitando tudo o mais como ruído. Portanto, a chave para o CDMA consiste em conseguir extrair o sinal desejado ao rejeitar tudo o mais como ruído aleatório.

Capitulo 3 – GSM

3.1 - Introdução

O sistema GSM é um sistema celular digital de segunda geração, concebido com o propósito de resolver os problemas de fragmentação dos primeiros sistemas celulares na Europa. O GSM é o primeiro sistema celular no mundo a especificar modulação digital e arquiteturas de serviços de nível de rede. Antes do GSM, os países da Europa utilizavam padrões diferentes dentro do continente e não era possível a um usuário utilizar um único terminal em toda a Europa.

O padrão GSM foi inicialmente desenvolvido para ser um sistema pan-Europeu e prometia uma série de serviços utilizando a rede digital de serviços integrados RDSI (ou ISDN – *Integrated Services Digital Network*).

O sucesso do padrão GSM excedeu as expectativas e ele é atualmente o padrão mais popular para sistemas celulares e equipamentos de comunicação pessoal em todo o mundo.

Em 1982, foi criado na Europa grupo GSM (*Group Special Mobile*) para desenvolver um padrão digital europeu único. A introdução do GSM se deu inicialmente no mercado Europeu em 1991. Ao final do ano de 1993, vários países não Europeus na América do Sul, Ásia, além da África do Sul e Austrália começaram a operar e adotar o GSM e o padrão tecnicamente equivalente e a partir dele desenvolvido, o DCS 1800. Esse último suporta serviços de comunicação pessoal (PCS – *Personal Communication Services*) nas faixas de rádio de 1.8GHz a 2GHz recentemente criada pelos governos em todo o mundo

Atualmente, GSM é a sigla de *Global System for Mobile Communications*.

3.2 - Arquitetura

A arquitetura do GSM consiste de três subsistemas interconectados que interagem entre eles e com os usuários através de certas interfaces de rede. Os subsistemas são:

- O subsistema estação rádio base (BSS - *Base Station Subsystem*);
- O subsistema de rede e comutação (NSS - *Network and Switching Subsystem*);
- O subsistema de suporte de operação (OSS - *Operation Support Subsystem*).

A estação móvel também é um subsistema, mas é considerada normalmente como parte do subsistema estação rádio base, por propósitos de arquitetura.

No GSM, equipamentos e serviços são designados para suportar um ou mais desses subsistemas.

O BSS, também conhecido como subsistema rádio, provê e gerencia as transmissões entre estações móveis e a central de comutação, MSC. O BSS também gerência a interface de rádio entre as estações móveis e todos os subsistemas do GSM. Cada BSS consiste de um conjunto de controladores de estações rádio (BSCs - *Base Station Controlers*) que conectam o terminal móvel ao NSS, via MSCs. O NSS gerencia as funções de comutação do sistema e permite à MSCs comunicar com outras redes, como a rede de telefonia pública comutada PSTN e a ISDN.

O subsistema OSS suporta a operação e manutenção do sistema GSM, permitindo aos engenheiros monitorarem, diagnosticarem e resolverem problemas de falhas de todo aspecto no sistema GSM. Esse subsistema interage com os subsistemas e é oferecido somente ao *staff* que oferece as facilidades de serviços para a rede na companhia operadora.

A figura abaixo, mostra o diagrama em blocos da arquitetura do sistema GSM. As estações móveis (MS - *Móbile Stations*) se comunicam com o sistema estação rádio base (BSS) através da interface aérea. O BSS consiste de vários controladores de estações rádio base (BSCs) conectados a uma única MSC e cada BSC tipicamente controla várias centenas de estações transceptoras base (BTSs – *Base Transceiver Statios*). Algumas das BTSs podem estar co-localizadas ao BSC através de *links* de microondas ou linhas dedicadas. Os *handoffs* (denominados *handovers* no GSM) entre duas BTSs sob o controle do mesmo BSC são manipuladas pelo BSC, não pela MSC. Isso reduz consideravelmente a carga de comutação da MSC.

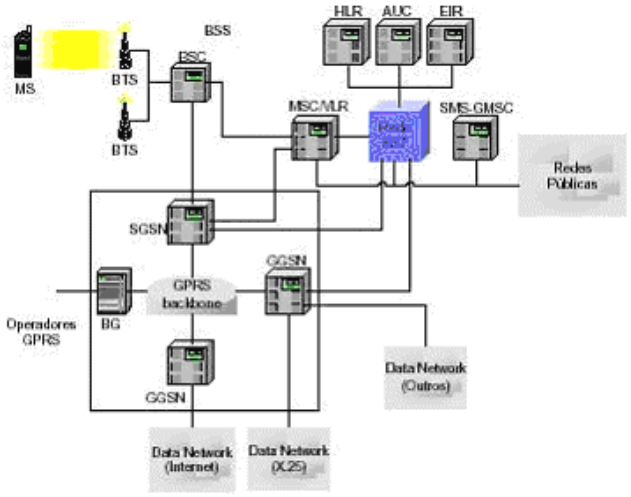

Figura 4: Elementos de uma rede GSM

Como mostrado, a interface que conecta uma BTS a uma BSC é chamada interface *Abis*. Essa interface carrega tráfego e dados de manutenção e é especificada no GSM para ser padronizada por todos os fabricantes. Na prática, contudo, a interface *Abis* para cada fabricante de estação rádio base para o GSM possui alguma particularidade, forçando os provedores de serviço a utilizarem os equipamentos para a BTS e para o MSC do mesmo fabricante.

Os BSCs são fisicamente conectados à MSC via linhas dedicadas ou *links* de microondas. A interface entre um BSC e uma MSC é chamada de interface *A*, que é padronizada dentro do GSM. A interface *A* usa um protocolo SS7 chamado SSCP (*Signaling Correction Control Part*), que suporta a comunicação entre cada assinante e a MSC. A interface *A* possibilita ao provedor de serviços utilizar estações rádio base e equipamentos de comutação feitos por diferentes fabricantes.

O subsistema NSS manipula a comutação das chamadas GSM entre redes externas e os BSCs no subsistema de rádio e é também responsável por gerenciar e prover acesso externo a várias bases de dados de clientes. A MSC é a única unidade central dentro do

NSS e controla o tráfego entre todos os BSCs. No NSS há três diferentes bases de dados chamadas:

- HLR (*Home Location Register*);
- VLR (*Visitor Location Register*);
- AUC (*Authentication Center*).

O HLR compõe uma base de dados que contém informações sobre o assinante e informações sobre o assinante e informações de localização para cada usuário que reside na mesma região de atuação de uma MSC.

A cada usuário em um mercado atendido pelo padrão GSM é atribuída a uma única identidade chamada IMSI (*International Mobile Subscriber Identity*); esse número é utilizado para identificar cada usuário local.

O VLR forma uma base de dados que armazena temporariamente a IMSI e informações de usuário para cada *roamer* que está visitando a área de cobertura de uma MSC em particular.

O VLR está associado a várias MSCs em uma área geográfica e contém informações de assinatura de todos os usuários visitantes nessa área. Estando um *roamer* registrado no VLR, a MSC envia as informações necessárias ao HLR desse usuário visitante de tal forma que as chamadas para esse assinante possam ser devidamente roteadas através da rede.

O AUC compõe uma base de dados fortemente protegida e que tem a função de manipular as chaves de autenticação e criptografia para cada usuário no HLR e no VLR. O centro de autenticação (AUC) contém um registrador chamado EIR (*Equipment Identity Register*), o qual identifica que não se casam com aqueles armazenados no HLR ou no VLR.

O subsistema OSS suporta uma ou várias OMCs (*Operations Maintenance Centers*) que são utilizados para monitorar e manter o desempenho de cada estação móvel (MS), estação rádio base (BTS), controlador de estação rádio base (BSC) e central de comutação (MSC) no sistema GSM. O OSS possui três funções principais que são:

- Manter a operação de todo o hardware e rede de telecomunicações de um determinado mercado;
- Gerenciar todo processo de tarifação;
- Gerenciar todos os terminais móveis no sistema.

Dentro de cada sistema GSM, um OMC é dedicado para todas as funções anteriormente citadas e possui provisões para ajustar todos os parâmetros de uma estação rádio base e os procedimentos de tarifação, bem como prover operadores do sistema com a habilidade de determinar o desempenho e a integridade de cada parte do equipamento do usuário em todo sistema.

3.3 – Subsistema de Rádio do GSM

O padrão GSM utiliza duas bandas de 25MHz que foram alocadas em todos os países membros. A faixa 890-915MHz é utilizada para o *link* reverso (do MS para a ERB) e a faixa 935-960MHz é utilizada para o *link* direto (da ERB para o MS). O padrão GSM utiliza duplexação FDD e uma combinação das técnicas de acesso TDMA e FHMA

(*Frequence Hopping Multiple Access*). As bandas disponíveis para os links diretos e reversos são divididas em canais de banda larga de 200MHz denominadas ARFCNs (*Absolute Radio Frequency Channel Numbers*). O ARFCN denota um par de canais direto e reverso separados de 45MHz, sendo cada canal compartilhado entre um número máximo de 8 usuários, através da técnica TDMA.

Cada um dos 8 usuários utiliza o mesmo ARFCN e ocupa um mesmo *slot* temporal por quadro TDMA, a modulação utilizada é a GMSK, a qual tem a vantagem de possuir envoltória constante, o que reduz consumo, cada *slot* temporal possui uma duração equivalente de 576,92µs, como mostrado tabela abaixo e sendo que um único quadro TDMA do GSM tem duração de 4.615ms. A tabela sumariza os dados sobre a interface aérea do GSM.

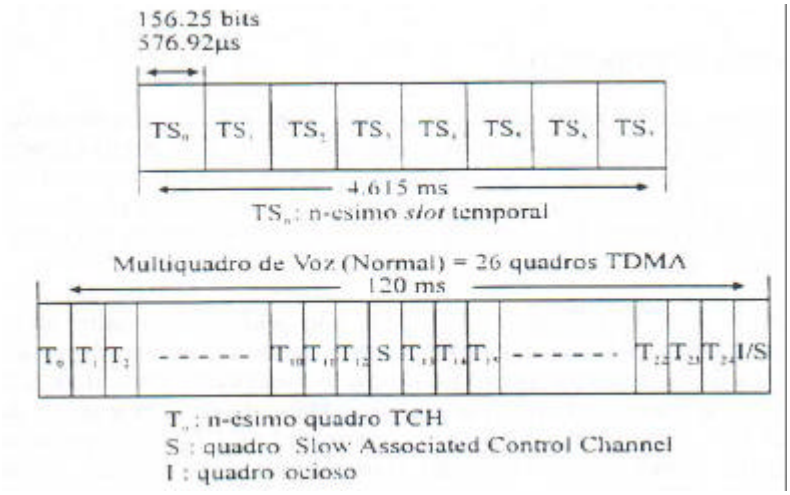

Figura 5: Estrutura de multiquadro e de quadro dedicado de controle de voz no GSM

Parâmetro	Especificações
Freqüência do canal reverso	890-915MHz
Freqüência do canal direto	935-960MHz
Número ARFCN	0 a 124 e 975 a 1023
Espaçamento de freqüência Tx/Rx	45MHz
Espaçamento temporal Tx/Rx	3 slots
Taxa de Transmissão	270,83kbps
Período do Quadro	4,615ms
Usuários por quadro (full rate)	8
Duração do slot	576,9 µs
Duração do bit	3,692 µs
Modulação	GMSK com BT = 0,3
Espaçamento de canal ARFCN	200KHz
Interleaving (máximo atraso)	40ms
Taxa do Codificador de Voz	13kbps

Tabela 1: Sumário das especificações da interface aérea do padrão GSM

3.4 - Tipos de Canais no GSM

Existem dois tipos de canais lógicos no GSM, chamados canais de tráfego (TCH – *Traffic Channels*) e canais de controle (CCH – *Control Channels*). Os canais de tráfego transportam voz codificada ou dados do usuário e têm função e formato idênticos para os *links* direto e reverso. Os canais de controle transportam sinalização e comandos de sincronismo entre a estação rádio base e o terminal do usuário. Certos tipos de canais de controle são definidos para o *link* direto ou para o reverso. Há seis tipos diferentes de TCHs no GSM, e um número ainda maior de CCHs, ambos descritos abaixo.

3.4.1 – Canais de Tráfego TCH

Os canais de tráfego do GSM podem operar tanto em *full-rate* quanto *half-rate* e podem transportar tanto voz digitalizada quanto dados do usuário. Quando transmitido em *full-rate*, o tráfego e transportado em todos os quadros GSM. Quando transmitido em *half-rate*, esse tráfego é dividido para ocupar quadros alternados. Em outras palavras, dois usuários de canais operando em *half-rate* irão utilizar o mesmo *slot* de tempo, mas irão transmitir em quadros alternados.

3.4.2 – Canais de Tráfego CCH

Existem três principais canais de controle no sistema GSM. São eles:

- O canal de broadcast (BCH – *Broadcast Channel*);
- O canal de controle comum (CCCH – *Common Control Channel*);
- O canal de controle dedicado (DCCH – *Dedicated Control Channel*).

Cada canal de controle consiste de vários canais lógicos distribuídos no tempo para prover as funções de controle necessárias ao sistema GSM.

Os canais diretos BCH e CCCH são implementados somente em alguns canais ARFCN e os *slots* temporais são alocados de forma bastante específica.

As especificações do GSM definem 34 ARFCNs como padrões para os canais de controle tipo *broadcast*. Para cada canal *broadcast*, o quadro 51 não contém nenhum dado nos canais diretos BCH/CCCH e é considerado como sendo um quadro ocioso. Contudo, o canal reverso CCCH é capaz de receber informações de assinantes durante o TS0 de qualquer quadro (até mesmo do quadro ocioso). Por outro lado, dados DCCH podem ser enviados em qualquer TS em qualquer quadro, e quadros inteiros são dedicados especificamente a certas transmissões DCCH.

O conjunto de canais BCH é definido por três canais em separado, aos quais é dado acesso ao TS0 durante vários quadros da seqüência de 51 quadros. A Figura 3.6 mostra como os BCH são alocados no quadro.

Os três tipos de BCH são:

Broadcast Control Channel (BCCH)

É um canal de controle direto que é utilizado para transmitir informações em *broadcast* tais como identificação de rede e de célula e características de operação da célula (estrutura atual de canais de controle, disponibilidade de canal e congestionamento).

Frequency Correction Channel (FCCH)

O FCCH é uma seqüência de dados especial que ocupa TS0 a cada primeiro quadro do GSM (quadro 0) e é repetida a cada 10 quadros em multiquadro de canais de controle.

Syncronization Channel (SCH)

O SCH é transmitido em *broadcast* no TS0 do primeiro quadro subseqüente ao quadro do FCCH e é utilizada para identificar a estação rádio base servidora, enquanto permite ao terminal móvel estabelecer sincronismo de quadro com a estação rádio base.

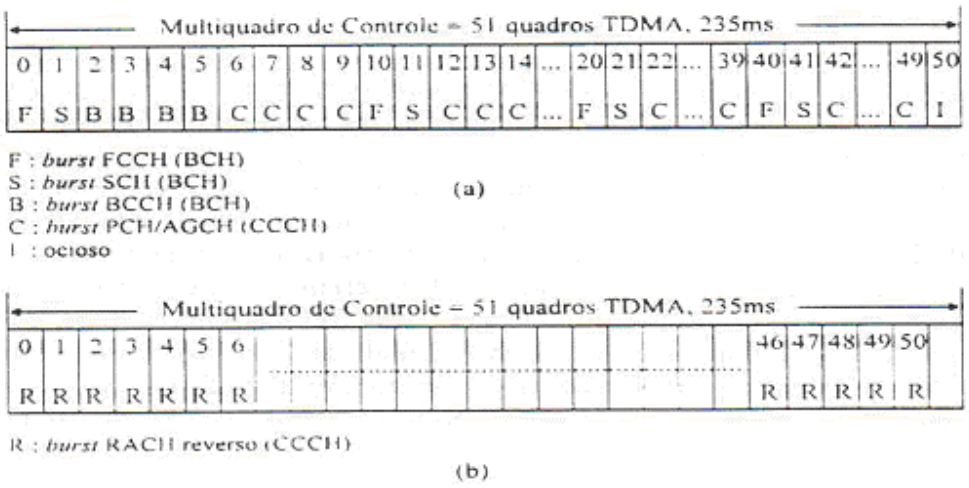

Figura 6: (a) Multiquadro de canais de controle (Link direto e reverso)

3.5 – Exemplo de chamada no GSM

Para entender como os vários canais de controle e tráfego são utilizados, considere uma chamada de um terminal móvel no sistema GSM.

Primeiramente a unidade de usuário deve estar sincronizada à estação rádio base mais próxima, enquanto monitora o BCH. Tendo recebido mensagens FCCH, SCH e BCCH, o assinante estará travado (*locked*) ao sistema e a um BCH apropriado.

Para originar uma chamada o usuário primeiro digita o número pretendido e pressiona a tecla *send* no telefone GSM. O terminal móvel transmite um *burst* de dados RACH (*Random Access Channel* - que é um canal do *link* reverso e o canal de concessão

de acesso), utilizando o mesmo ARFCN que a base à qual ele está associado. A estação rádio base então responde com uma mensagem AGCH (*Access Grant Channel* – que é um canal do *link* direto) no CCCH que aloca ao terminal móvel um novo canal para uma conexão SDCCH (*Stand-alone Dedicated Control Channel* – que transportam dados de sinalização seguindo a conexão do terminal móvel à estação rádio base, imediatamente anterior ao envio de uma alocação de TCH pela estação rádio base). A unidade do usuário, que está monitorando o TS0 do BCH, irá receber sua alocação de ARFCN e TS do AGCH e irá imediatamente se "sintonizar" aos novos ARFCN e TS.

3.6 - Estrutura de quadro do GSM

Cada usuário transmite *bursts* de dados durante o TS a ele alocado. Esses dados podem ter um dos cinco formatos específicos, como definido pelo padrão GSM. A figura 7 ilustra os 5 tipos de *bursts* de dados utilizados para controle e tráfego. Os *bursts* normais são utilizados para transmissões no TCH e DCCH nos *links* direto e reverso. Os *bursts* no FCCH e SCH estão presentes no TS0 de quadros específicos e são utilizados para transmitir em *broadcast* as mensagens de controle de sincronismo de freqüência e tempo no *link* direto. Os *bursts* no RACH são utilizados por todos os terminais móveis para acessarem serviços da estação rádio base e o *burst* "mudo" (*dummy*) utilizado como ordenador de informações para TS não utilizados no *link* direto.

A Figura abaixo (7) ilustra a estrutura de dados em um *burst* normal. Esse *burst* consiste de 148 bits que são transmitidos a uma taxa de 270.83333Kbps (um tempo de guarda equivalente à duração de 8.25 bits é provido ao final de cada *burst*). Do total de 148 bits por TS, 114 são bits de informação que são transmitidos em dois blocos de 57 bits, um próximo ao início e outro próximo ao fim do *burst*.

A parte central consiste de um a seqüência de treinamento de 26 bits que permite equalizador adaptativo do terminal móvel ou da estação rádio base ajustarem seus coeficientes em função das características do canal antes que os bits de controle chamados *flags* de roubo (*stealing flags*). Esses dois *flags* são utilizados para distinguir se o TS contém voz (TCH) ou dados de controle (FACCH), dado que ambos compartilham o mesmo canal físico. Durante um quadro, uma entidade de um assinante GSM utiliza um TS para transmitir, um TS para receber e pode usar seis TSs adicionais para medir a intensidade do sinal em 5 estações rádio base adjacentes à base servidora.

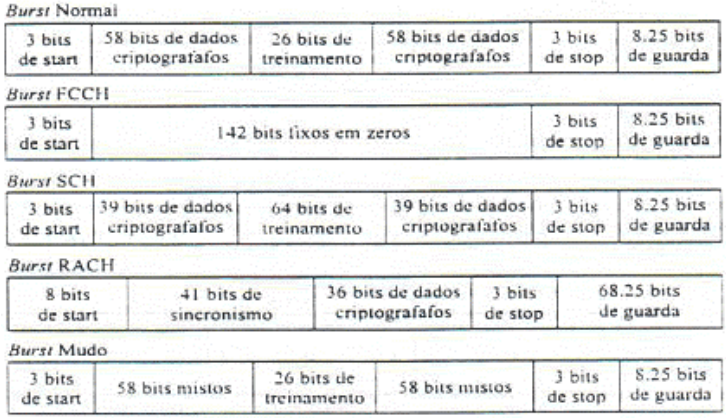

Figura 7: Bursts de dados por slot no GSM

Como mostrado na figura 8, há 8 TSs por quadro TDMA e o período do quadro é de 4,615ms. Um quadro contém 8 X 156,25 = 1250 bits, embora alguns períodos de bit não sejam utilizados.

A taxa de quadros é de 270,83Kbps/1250bits/quadro = 216,66quadro/segundo. Os quadros de número 13 e 26 não são utilizados para tráfego e sim para propósitos de controle. Cada um dos quadros normais de tráfego de voz é agrupado em estruturas maiores denominadas multiquadros (ou *multiframes*) que por sua vez são agrupados em superquadros e hiperquadros (os hiperquadros não estão sendo mostrados na figura 8). Um multiquadro contém 26 quadros TDMA e um superquadro contém 51 multiquadros ou 1326 quadros TDMA. Um hiperquadro contém 2048 superquadros ou 2.715.648 quadros TDMA. Um hiperquadro completo é enviado em 3 horas, 28 minutos e 54 segundos e é importante para o sistema GSM, pois os algoritmos de criptografia contam com o número do quadro (FN – *Frame Number*) em particular e uma segurança suficiente somente pode ser obtida utilizando-se um grande número de quadros, como o hiperquadro.

A figura 5 mostra que os multiquadros de controle somam 51 quadros (235,365ms), em oposição aos 26 quadros (120ms) utilizados pelos multiquadros de canais de controle dedicados e de tráfego. Isto é feito intencionalmente para assegurar que qualquer assinante GSM (na célula servidora ou adjacente) certamente irá receber as transmissões SCH e FCCH através do BCH, independente do quadro ou TS que esteja utilizando.

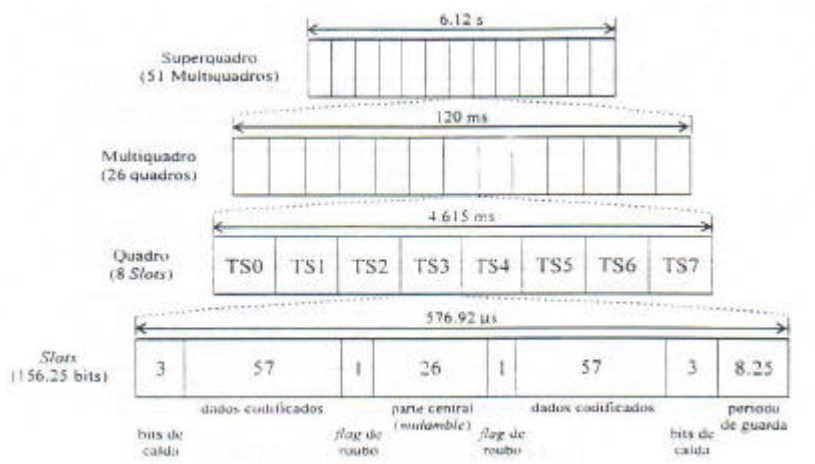

Figura 8: Estrutura de quadro do GSM

3.7 – Processamento de Sinal no GSM

A Figura 9 ilustra todas operações do transmissor ao receptor no sistema GSM. As várias partes mostradas na figura são descritas a seguir:

Codificação de voz: O codificador de voz do GSM é baseado na técnica RELP (*Residually Excited Linear Predictive*) que é melhorada pela inclusão de um preditor de longa duração (LTP – *Long Term Predictor*). O codificador fornece 260 bits para cada

bloco de voz de 20ms, e que resulta em uma taxa de 13Kbps. Esse codificador de voz foi escolhido dentre os vários disponíveis na década de 80, a partir de testes subjetivos de opinião. Nas especificações do sistema GSM foi prevista a incorporação de codificadores operando na metade dessa taxa (*half-rate*).

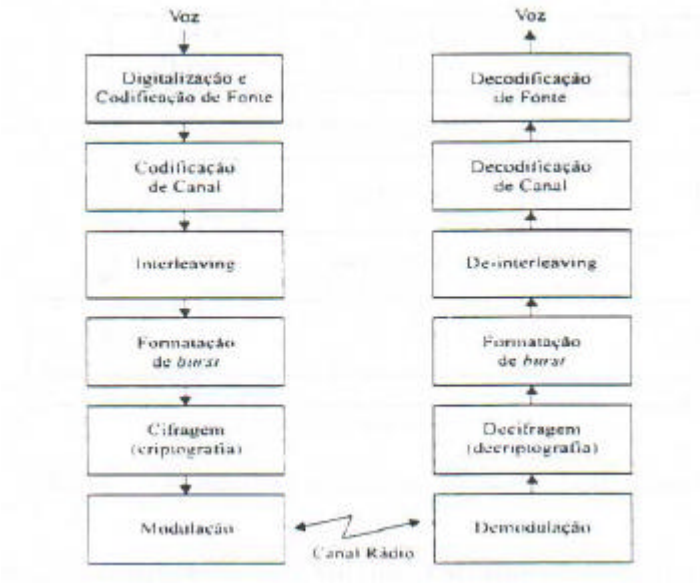

Figura 9: Operações no GSM da entrada à saída de voz

Codificação de Canal TCH/FS, SACCH e FACCH: Os bits de saída do codificador de voz são ordenados em grupos para a proteção contra erros, baseando-se na "significância" desses bits na qualidade do áudio. O processo de codificação de canal aumenta a taxa de transmissão de voz para 22,8Kbps. Esse esquema é mostrado na Figura 10.

Codificação de canal para os Canais de Dados: A codificação oferecida pelo padrão GSM para os canais de dados *full-rate* (TCH/F9.6) é baseada na manipulação de 60 bits de dados de usuário a cada intervalo de 5ms, de acordo com a recomendação para modens CCITT v.110 modificada.

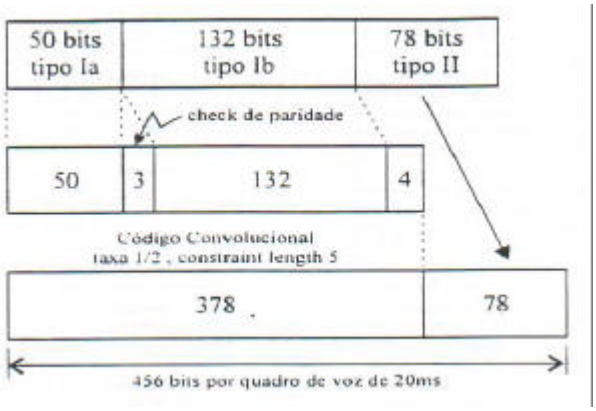

Figura 10: Proteção contra erros nos dados de voz do GSM

Codificação de Canal para Canais de Controle: As mensagens nos canais de controle do sistema GSM são, por definição, compostas por 128 bits. Essas mensagens são codificadas através de um código cíclico binário reduzido, seguido de um codificador convencional de taxa ½.

Interleaving: De forma a minimizar o efeito de desvanecimentos repentinos nos dados recebidos, os 456 bits codificados a cada quadro de voz ou de mensagens de controle de 20ms são subdivididos em blocos de 57 bits. Os 8 sub-blocos resultantes são espalhados por 8 *slots* TCH consecutivos (8 quadros consecutivos para um slot específico). Se um *burst* é perdido devido ao desvanecimento ou a interferências, o *interleaving* garante que não sejam perdidos bits codificados consecutivos, o que permite que um número suficiente de bits seja recebido corretamente por ação da correção de erros.

Cifragem: A cifragem modifica o conteúdo dos 8 blocos entrelaçados através do uso de técnicas de criptografias conhecidas somente pelo terminal móvel e pela estação rádio base. A segurança é aumentada pelo fato do algoritmo de criptografia se modificar de chamada a chamada. Dois tipos de algoritmos, chamados A3 e A5, são utilizados no GSM para evitar acesso não autorizado a rede e para prover privacidade na comunicação via rádio, respectivamente. O algoritmo A3 é utilizado para autenticar cada terminal móvel, verificando se a senha do usuário contida no SIM através da chave de criptografia no MSC. O algoritmo A5 provê o embaralhamento dos 114 bits de dados codificados enviados a cada TS.

Formatação de Burst: A formatação de *burts* adiciona dados binários aos blocos criptografados com o objetivo de auxiliarem na sincronização e na equalização do sinal recebido.

Modulação: A modulação utilizada no GSM é a GMSK com BT=0.3, onde 0.3 descreve a largura de faixa (ponto de 3dB) do filtro gaussiano de formatação dos pulsos em relação à taxa de transmissão de bits. A modulação GMSK é uma forma especial de modulação FM. Os dígitos binários “1s” e “0s” no GSM provocam o desvio de portadora em ± 67,708KHz. A taxa de transmissão no canal é de 270,83 Kbps, que é exatamente quatro vezes o desvio de freqüência da portadora. Essa modulação minimiza o espectro ocupado pelo sinal modulado e, assim, aumenta a eficiência espectral. Inicialmente o sinal é modulado em MSK e depois é filtrado por um filtro de resposta gaussiana para suavizar as transições de freqüência abruptas que poderiam aumentar a energia do sinal modulado fora da faixa de interesse.

Frequency Hopping: Sob condições normais, cada *burts* de dados pertencente a um determinado canal físico é transmitido utilizando-se uma mesma portadora. Contudo, se os usuários em uma célula em particular sofrem grandes problemas devido a propagação do sinal por multipercursos, o operador da rede pode definir essa célula como uma *hopping cell* e, nesse caso, uma técnica de espalhamento espectral SFH (*Slow Frequency Hopping*) é implementada para combater os efeitos de multipercursos e interferências nesta célula. A técnica SFH é completamente especificada pelo provedor de serviços.

Equalização: A equalização é desempenhada no receptor com a ajuda da seqüência de treinamento transmitida na parte central de cada TS. O tipo de equalização não é especificado no padrão GSM e é deixada por conta do fabricante dos transceptores.

Demodulação: A porção do sinal transmitido no canal direto que é de interesse do usuário é determinada pelo TS e ARFCN alocados. O sinal do TS apropriado é demodulado com a ajuda da sincronização provida na formatação dos *bursts.* Após a demodulação, a informação binária e decifrada, de-entrelaçada e decodificada pelo decodificador de canal e de fonte.

Capítulo 4 - GPRS

4.1 –Conceitos de GPRS

O GPRS (*General Packet Radio Service* - Serviço de Radio Geral por Pacotes) é um novo serviço "*novoice*" que permite que a informação em forma de dados seja emitida e recebida através de uma rede de telefonia móvel. Ele complementa os atuais serviços de comutação por circuitos GSM (*Global System for Mobile)* e os serviços de envio de mensagens via rede celular denominado de SMS (*Short Message System*).

As redes GPRS foram desenvolvidas para suportar os serviços de dados, pois as mesmas foram criadas baseadas em transmissão por comutação de pacotes, diferentemente das GSM que ainda utilizam a comutação por circuitos. Na comutação por pacotes, como visto anteriormente, utiliza de forma mais eficiente a banda devido a transmissão do tráfego ser em rajadas o que é a característica dos serviços de dados.

O GSM e o GPRS compartilham uma única base dinâmica e flexível, com várias características semelhantes entre si, como bandas, freqüências, estrutura de frames e técnicas de modulação. No entanto, a cobrança pelo uso de GPRS é feita por quantidade de dados (Kbits) transmitidos enquanto no GSM é feita por tempo de conexão (segundos).

O sistema de GPRS fornece uma solução básica para uma comunicação IP entre estações móveis (MS – *Mobile Station*) e os Hosts da Internet (IH – *Internet Host*) ou uma LAN incorporada. Possuindo diversas características como:

- **Velocidade**: Na teoria as velocidades máximas chega a 171,2 kilobits por segundo, porém só são possíveis no GPRS usando todos os oito times-slots ao mesmo tempo. Isto é aproximadamente três vezes mais do que as redes de telecomunicações atualmente. Permitindo que a informação seja transmitida de forma mais rápida e eficiente através da rede móvel. GPRS pode prover um serviço móvel de dados relativamente menos caro se comparado a SMS (*Short Message System*) e aos demais serviços de dados comutados circuito.
- **Immediancy:** Facilidade de se conectar a rede dados. O GPRS não necessita de realizar conexões dialup, o usuário fica do tempo todo "conectado". O immediacy é uma das vantagens de GPRS quando comparado aos serviços de comutação por circuitos. Esta característica é largamente utilizada em transferência de dados críticos e de forma online, tais como a autorização remota do cartão de crédito, onde seria inaceitável manter muito tempo o cliente a espera da conclusão de uma transação.
- **Novas Aplicações:** GPRS facilita o uso de diversas aplicações novas que não é possível utilizar em redes GSM devido às limitações na velocidade de dados comutados circuito (9,6 kbps) e do comprimento de mensagem do SMS (160 caracteres). Existem dois grupos de aplicações as verticais e as horizontais. *As horizontais* são aplicações voltadas para os clientes "*person-to-person*" incluindo as ferramentas comuns como: Web, chat, FTP (*File Transfer Protocol*), e-mails, leitor de cartão magnético. *As verticais* são aplicações adaptadas para resolver exigências

de uma transmissão de dados de uma empresa especifica como: aplicações de venda de serviços, transações bancárias, aplicações de Telemetria entre outros.

Quando a mensagem a ser enviada em uma rede GPRS for maior que tamanho designado para a transferência, a mesma é dividida em diversos pacotes. Quando estes pacotes alcançam o destinatário, são remontados para dar forma à mensagem original. Todos os pacotes recebidos são armazenados em buffers. Os pacotes originados no MS (*Mobile Station*) podem pegar vários canais diferentes durante a transmissão dos pacotes.

4.2 – Arquitetura Lógica do Sistema GPRS.

As partes do sistema GPRS que realizam a comutação dos pacotes são chamadas de SGSN (*Serving GPRS Support Node*) ele é o centro da rede e fornece o roteamento para as demais partes, faz interface entre a rede de comutação por pacote (rede de dados) e a rede de comutação por circuitos (HLRs, EIRs e outros). Os principais componentes da arquitetura lógica de um sistema GPRS estão listados na figura abaixo.

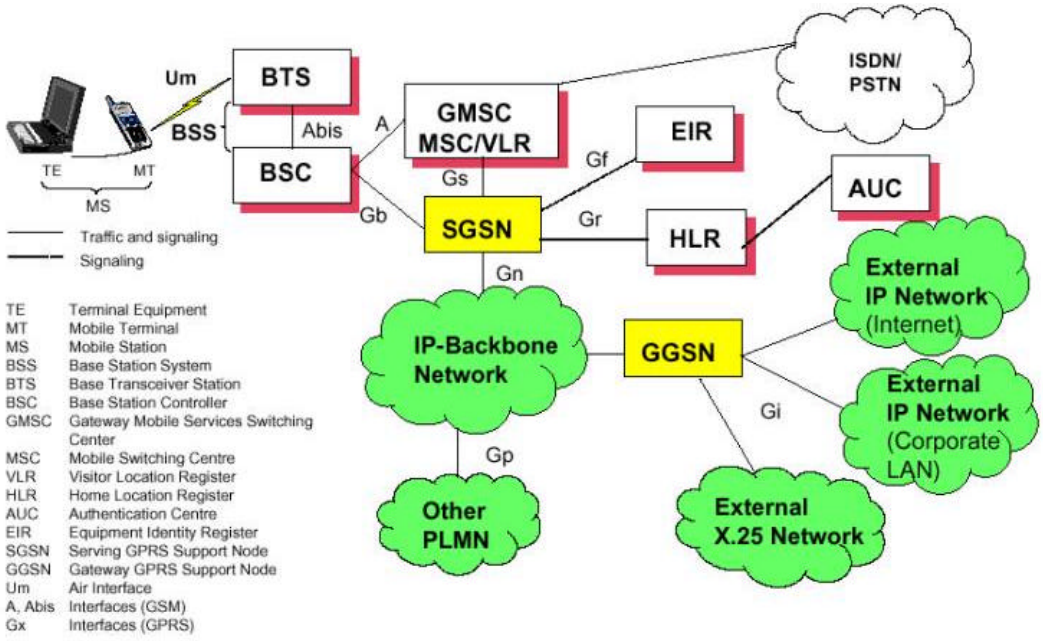

Figura 11: Componentes da Rede GSM

TE*(Terminal Equipament*): É o terminal onde o usuário final trabalha caracterizado pelo computador, o sistema recebe endereçamento IP para conectividade em uma rede local ou Internet.

MT *(Mobile Terminal*): É como um modem que fornece a conexão do TE na rede GPRS utilizando uma ligação com o SGSN. É estabelecido um túnel entre o TE e o SGSN.

MS (*Mobile Station*): A junção de um TE e um MT forma um MS. Os componentes necessários para o MT e TE são agrupados no conceito de GPRS em um único equipamento. Dependendo da característica da rede GPRS, os MSs podem operar em 3 modalidades diferentes:

- **Classe A:** operação permite que um MS tenha uma conexão comutada por circuito ao mesmo tempo em que é envolvida em transferência do pacote.
- **Classe B:** esta operação permite que um MS faça conexão comutada por pacote e comutada por circuito mas não ao mesmo tempo. Entretanto, o MS que pode ser envolvido em transferência do pacote e receber uma chamada para o tráfego de comutação por circuito. O MS pode então suspender transferência do pacote enquanto durar a conexão por circuito e mais tarde recomeçar transferência do pacote.
- **Classe C:** a modalidade de operação permite que um MS seja unido somente a um serviço. Um MS que suporta somente GPRS e o tráfego não comutado por circuito trabalhará sempre na modalidade da classe C de operação.

BSS (*Base Station*): Uma BSS consiste de uma BSC (*Base Station Controller*) e uma BTS (*Base Transceiver Station).* O BTS é um equipamento de rádio que envia e recebe informações sobre a comunicação das BSCs com os MSs. Um grupo de BTSs é controlado por um BSC. O BTS deve conter softwares específicos para GPRS. A BSC gerencia as chamadas comutadas por circuitos e comutadas por pacote e deve ser equipada com software e hardware para o sistema GPRS. O BTS separa as chamadas comutadas por circuito MS originadas da transmissão de dados do pacote, antes que o BSC envie chamadas para MSC/VLR, e dados da comutação por pacote para o SGSN.

MSC (*Mobile Service Switching Center*): é responsável pelo tráfego de pacotes que tem os MSs como origem ou destino e por funções como autenticação, roteamento, gerenciamento de mobilidade, controle de acesso e contabilidade de uso da rede de rádio.

GMSC (*Gateway Mobile Services Switching Center*): Faz o roteamento das chamadas entre a rede GSM e a PSTN. Não há mudança neste produto para o GPRS.

GGSN *(Gateway GPRS Support Node):* gerencia o roteamento entre a rede GPRS e outras redes de dados (Internet, X.25,etc). Também é responsável por controlar a alocação de endereços IP por parte dos MSs e por traduzir os formatos de pacotes de endereços externos para o formato de endereçamento GPRS e vice-versa**.**

HLR *(Home Location Register):* é a base de dados que armazena a informação da subscrição para cada pessoa que possui uma subscrição do operador de GSM/GPRS. O HLR armazena a informação tanto para uma comunicação por circuito como por pacote. A informação encontrada no HLR inclui, por exemplo, serviços suplementares, parâmetros de autenticação, Access Point Name (APN) como o Internet Service Provider, endereço IP. Além disso, o HLR inclui a informação sobre a posição (localização Geografica) do MS.

Para o GPRS, a informação do cliente é trocada entre HLR e SGSN. Nota-se que as informações de autenticação para GPRS estão recuperadas diretamente do HLR para SGSN. São armazendas nos HLRs informações de clientes quando destina-se a outras operadoras, roaming.

VLR *(Visitor Location Register*): a base de dados contem a informação sobre todo o MSs que é fica situado atualmente na região da posição da MSC ou da distribuição de SGSN respectivamente. O SGSN contem a funcionalidade de VLR para uma comunicação por pacotes.

SGSN *(Serving GPRS Support Node*): um componente primário na rede GSM para o uso do GPRS. O SGSN envia e recebe pacotes destinados para a MS que seja anexado dentro da área de serviço SGSN. O SGSN fornece roteamento de pacotes e serve a todos os usuários GPRS que estão fisicamente dentro da área de serviço geográfica de SGSN. Um usuário GPRS pode ser servido por todo o SGSN na rede, tudo dependende da localização do mesmo.

4.3 – Protocolo de transmissão GPRS.

A interface chamada de *Um* é o link lógico formado na comunicação um MS *(Mobile Station)* e um BSS *(Base Station System).* A estrutura de protocolos responsável pela transmissão de dados do usuário, é construído na forma de camadas, semelhante a estrutura de camadas OSI. A primeira camada é implementada no BTS *(Base Tranceiver Station)*. O PCU (*Packet Control Unit* – Unidade de Pacote de Controle), como é um novo componente, é tratado em outra camada do protocolo. Segue a estrutura de camadas do protocolo GPRS.

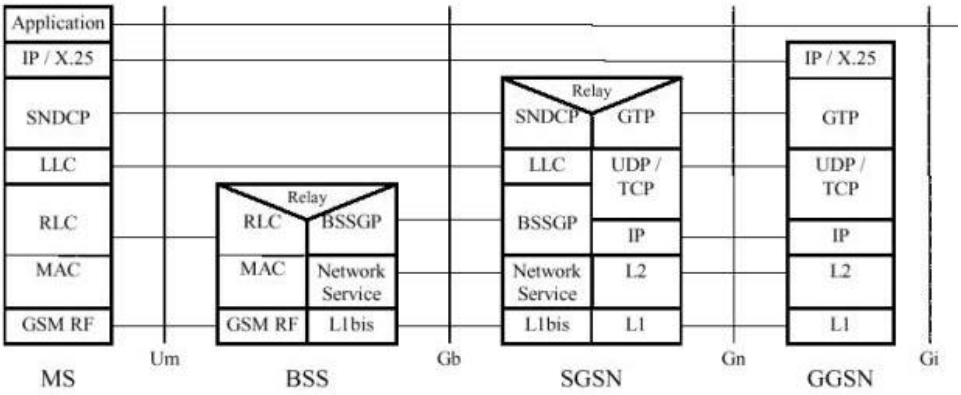

Figura 12: Estrutura e Camadas de Protocolos do GPRS

SNDCP (*Subnetwork Dependent Convergence Protocol*) permite às camadas superiores acessarem as facilidades de transmissão ao nível de rede. Localiza abaixo da camada de rede e acima da LLC (*Logical Link Control*). Possui as seguintes subfunções:

- Multiplexação dos pacotes em uma ou várias camadas:
- Compressão de protocolos de informação e controle bem como dados do usuário;
- Segmentação e montagem.

A camada **LLC** (*Logical Link Protocol*) estabelece conexões lógicas cifradas independentemente dos protocolos da interface de rádio entre os MS e a SGNS. O LLC permite que o usuário permaneça com a mesma conexão quando se move entre as células de uma mesma SGNS. O LLC suporta:

- Processos de transferência de PDUs (*Packets Data Unit*) LLC em ambos os modos *Acknowledged* e *unacknowledged*.
- Processo de detecção de correção de PDUs LLC perdidos ou corrompidos.
- Processo de controle de fluxo e cifragem de PDUs LLC.

As camadas **RLC** (*Radio Link Control*) / MAC (*Media Access Control)* realizam a conexão entre o MS e o BSS através da interface aérea;

A camada **GSM RF** é a conexão física (via radio freqüência) entre a *Mobile Station* e a BSS;

O BSSGP (*Base Station System GPRS Protocol*) transporta informações de rotas e parâmetros de QoS (*Quality of Service*) entre a BSS e o SGSN. O NS (*Network Services*) transporta o PDU do BSSGP.

L1 e **L2** são as camadas de enlace e meio físico;

O **GTP** (*GPRS Tunneling Protocol*) é responsável pelo tunelamento dos dados do usuário entre o SGSN e os elementos do Backbone GPRS. O GTP encapsula todo os dados PTP (*Point-to-Point*), PDP (*Packet Data Protocol*) e PDU (*Packet Data Units*). Prove mecanismos de controle de fluxo entre os GNSNs caso seja solicitado.

TCP carrega os PDUs no backbone da rede GPRS para os protocolos que necessitam de transporte confiável, como o x.25. **UDP** utilizado para protocolos que não necessitam de confiabilidade na transmissão**. IP** prove o roteamento dos pacotes e sinalização. Na figura abaixo está a estrutura de multi-frame, encapsulada nas diversas camadas:

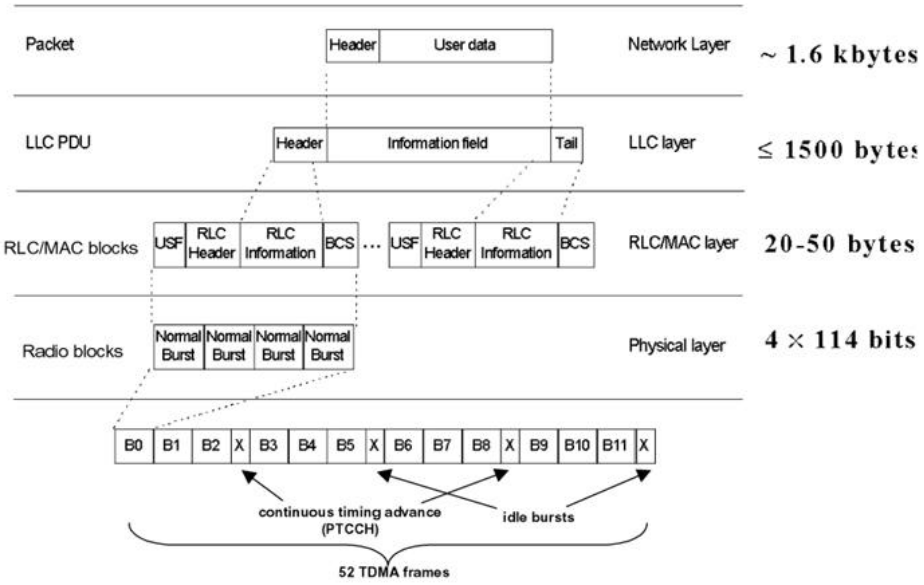

Figura 13: Estrutura multi-frame

4.3.1 – Radio Block

A Camada RLC/MAC possui duas funções: **RLC** que prove uma solução de radio dependente do enlace confiável. **MAC** que controla o acesso sinalizado para os canais do radio, faz o mapeamento do frame LLC para o canal GSM físico. Segue a figura abaixo ilustrando o cabeçalho de um PDU LLC.

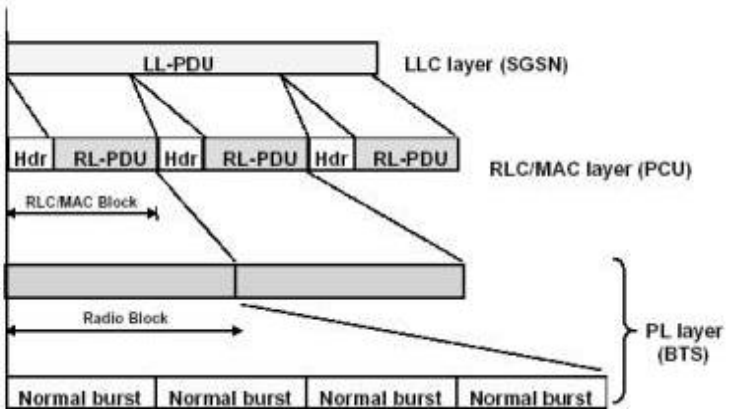

Figura 14: Cabeçalho de uma PDU LLC

4.3.2 – Canais Lógicos.

O número de canais lógicos é similar aos existentes na rede GSM, porém os mesmos são padronizados. Os canais lógicos são mapeados nos físicos e utilizados para pacotes de dados dedicados. Estes canais são chamados de PDCH (*Packets Data Channel*). Os principais canais lógicos do GPRS são:

Pacotes comuns de controle de Canais:

- PRACH: Random Access CHannel (uplink)
- PPCH: Packet Paging CHannel (downlink)
- PAGCH: Packet Access Grant CHannel (downlink)
- PTCCH: Packet Timing advance Control Channel (uplink/downlink)
- PNCH: Packet Notification CHannel (downlink)

Canais de Broadcast

- PBCCH: Packet Broadcast Control CHannel (downlink)

Pacote de trafico de canais

- PDTCH: Packet Data Traffic CHannel (uplink/downlink)
- PACCH: Packet Associated Control Channel (uplink/downlink)

4.4 - Estados e Modos do protocolo GPRS.

Existem três tipos de estados gerenciados pelo protocolo GPRS. Listados abaixo:

Idle State: O *mobile station* está ligado porem não está com o GPRS agregado. O MS é invisível para o GPRS. Exemplo se o MS estiver fora da área de cobertura GPRS;

Standby State: O *mobile station* está agregado ao GPRS e envia atualizações diárias das rotas para o SGNS a todo o momento para a atualização da mesma.

Ready State: O pacote está sendo transferido ou foi recentemente terminada uma transmissão. Um "*ready timer*" define como ao logo do tempo o MS retornará ao estado de "*ready*" após a transferência. Este tempo é definido pelo SGN e pode receber valores de zero a infinito, ou seja, um MS pode nunca retornará ao estado de *Standby*. O MS envia células de atualização para o SGSN todas as vezes que a mesmo troca de célula. No estado de *Ready* não é necessário enviar uma atualização para o MS. O SGSN envia frames LLC para o PCU (*Packet Control Unit*) e o mesmo por sua vez envia uma mensagem instantânea para o MS, desde que a localização seja conhecida.

A figura abaixo mostra os estados do protocolo GPRS, no na visão do Mobile State e do SGSN.

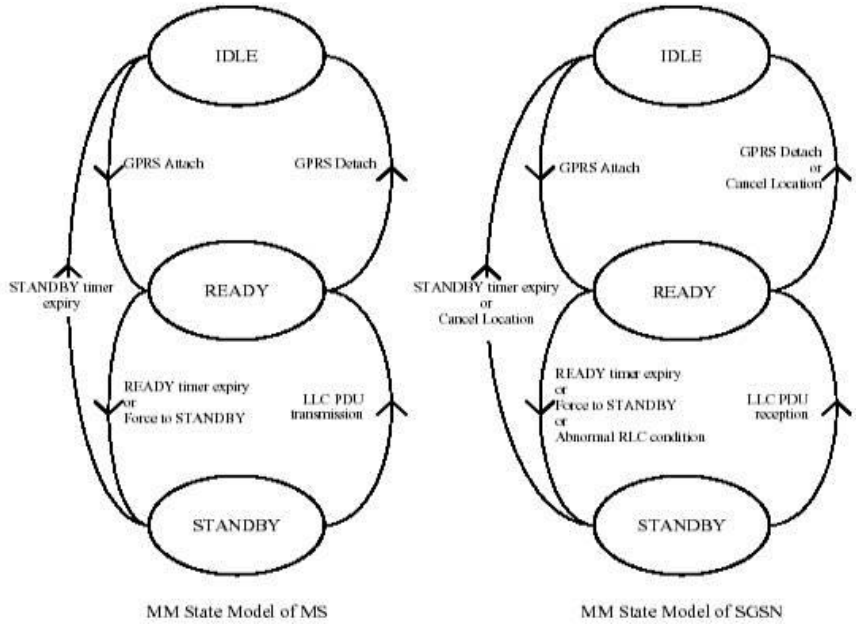

Figura 15: Diagrama de Estado do GPRS

Existem dois tipos de modos de operação do radio GPRS:

Pacotes em modo Idle: quando nenhum pacote é transmitido

Pacotes em modo de transferência: o pacote é transferido de tanto em uplink como em downlink ou ambos simultaneamente. O MS é somente reorganizado pelo PCU (*Packet Control Unit*) quando um pacote está no modo de transferência. A rede pode prover controle da "paginação" tanto para uma rede de circuitos quanto para uma rede de pacotes. "Paginação de mensagens" significa o uso de canais de controle são os mesmos tanto para GSM como para GPRS. São divididos em três tipos de modalidade de transmissão na rede:

- ***Modo de operação I*:** é enviado um CS de paginação de mensagem para um GPRS agregado ao MS no canal de controle ou no canal de trafego. Isto significa que o MS deve somente monitorar um canal de paginação, e envia CS de paginação ao canal de trafego quando o mesmo é designado para o canal de controle de pacotes.
- ***Modo de operação II:*** A rede envia um CS de paginação para um GPRS agregado ao MS através do canal de monitoração CCCH, visto anteriormente. Desta forma a MS só monitora este canal, mesmo que atribuído a um canal de dados.
- ***Modo de operação III:*** A rede envia um CS de paginação para um GPRS agregado ao MS através do canal de monitoração CCCH, porem é utilizado canais distintos para mensagens GPRS, sendo assim é necessário monitorar ambos os canais.

4.4. Implementação da rede GPRS.

O centro de uma rede GPRS está concentrado na GSNs, e compostos pelos seguintes componentes:

- Gerenciamento da rede: incluindo operação e manutenção da bilhetagem.
- Serviços de rede: o que prove os serviços de Internet. Este conjunto de componentes é denominado de "*GPRS Internal Backbone*" formado pela conexão de roteadores entre os GSNs. No entanto é possível incluir roteadores separados do backbone GPRS, desde que possua um equipamento DCE entre os GSNs.

A conectividade IP do GPRS prove:

- Comunicação entre as diferentes partes de um sistema GPRS incluindo: Mobile Station, SGSN, GGSN, administração de hosts e prove acesso a usuários na rede;
- Comunicação com a Internet

Existem dois diferentes níveis de comunicação IP: Comunicação com a rede GPRS para sinalização, controle, etc. A figura abaixo demonstra um tipo de implementação de *GPRS Internal Backbone*.

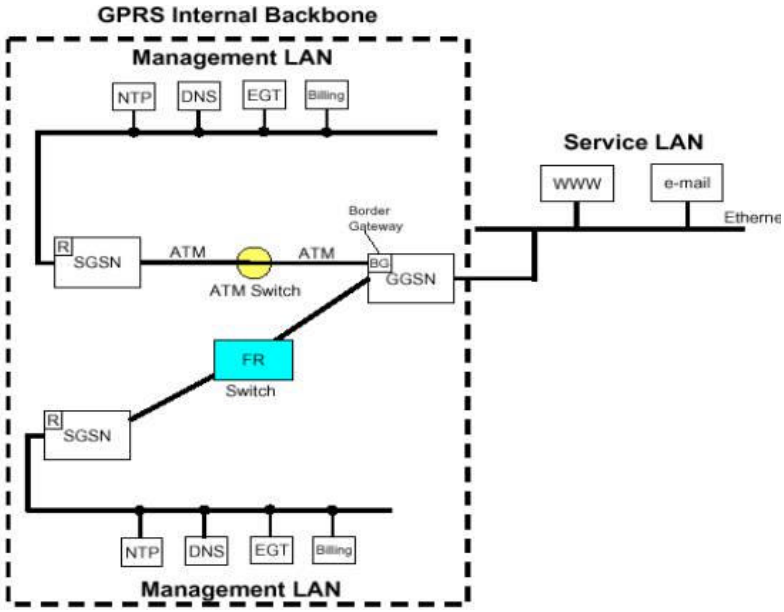

Figura 16: GPRS Internal Backbone

O sistema GPRS prove a conectividade IP entre MSs e IHs utilizando um padrão do sistema. A transferência é baseada nos protocolos de Internet, a transmissão é realizada fim-a-fim utilizando os meios aéreos. O MS é responsável por fornecer a conexão do usuário da rede através do modem. O endereço IP utilizado na comunicação do sistema pode ser publico, privado, dinâmico ou estático. Os endereços dos MS públicos ou privados são definidos de acordo com a topologia de rede adotada e a forma de acesso a Internet. Os endereços dinâmicos são geralmente adotados para visitantes do SGSN quando o mesmo está em roaming recebe um endereço temporário, e o mesmo permanece com este endereço somente enquanto estiver na rede visitada, sendo necessário desta forma um range menor de endereços. O endereço IP estático é definido no HLR geralmente é utilizado para acesso a redes seguras que utilizam o IP como parte da verificação de acesso.

Os roteadores realizam o roteamento de todos os MSs conectados ao sistema GPRS enviando os pacotes para o Backbone. Para a segurança desta transação são envolvidos aplicações e serviços como: autenticação em RADIUS (utilizando PAP (*Password Authentication Protocol)* ou CHAP *(Challenge Handshake Authentication Protocol))*; uso de IPSec ou PVC para tunelamento dos dados; uso de NAT *(Network Address Transalation)* em caso de uso de endereços privados.

Para comunicação entre os roteadores são suportados vários protocolos de roteamento como RIP *(Routing Information Protocol),* OSPF *(Open Shortest Path First)* e BGP *(Border Gateway Protocol).*

4.5. Aplicações GPRS

Existem muitas aplicações residenciais que podem ser aplicadas para o GPRS, mas existe uma grande variedade de aplicações corporativa. Estima-se que aproximadamente 30% a 50% do business-to-business da Internet possa ser realizado nos *Mobile Stations* com a alta demanda do uso das mesmas via wireless. Dentre as diversas aplicações temos:

- Chat: O GPRS é como uma extensão da Internet, permite que usuários utilizem grupos de chats. Porem não suporta serviços *point-to-multipoint* para uma mesma frase. Suporta a distribuição de frases simples para um grupo de pessoas.
- Serviços de informações como textos e gráficos: já utilizados pelos atuais serviços de SMS, porem com o GPRS será possível complementar estes textos com mensagem maiores e a inclusão de gráficos, figuras, e recursos audiovisuais;
- Tratamento de imagens: como as máquinas fotográficas e scanners, é possível tratar imagens enviar fotos e apresentações. Gravar informações como vídeo conferencia;
- Web: Acesso a Internet tradicional.
- Recursos de áudio: Alta velocidade para o uso de serviços de áudio;
- Serviços de FTP: transferência de arquivos e imagens entre MSs;
- Serviços e-mail corporativo e Internet: provê serviços de e-mail tanto para a Internet quanto para grandes corporações;
- Serviços de localização: serviços integrados com o posicionamento de satélites que localizam a posição que um determinado MS está localizado.

Existem diversas aplicações para os sistemas GPRS e muitas sendo ainda desenvolvidas na maioria dela baseadas em linguagem Java Script . Os atuais MS GSM não

suportam as aplicações GPRS, é necessário várias implementações. Existe ainda uma larga expansão na rede GPRS para suportar aplicações da Internet com a performance semelhante.

4.6 Considerações GPRS

As redes GPRS estão sendo implantadas como sendo um degrau para a migração das atuais redes moveis de comutação por circuito GSM para os sistemas móveis de terceira geração. Foi desenvolvida utilizando as técnicas de comutação por pacote, preparando a infra-estrutura atual do sistema móvel celular para o trafego de aplicações e dados em pacotes IP. Existem ainda muitas barreiras como performance, resolução, porém os usuários de telefones celulares já podem contar com uma ferramenta móvel de comunicação com a Internet e demais serviços.

Capítulo 5 – Segurança em GSM/GPRS

5.1 – Introdução a Segurança em Celulares

No antigo sistema analógico AMPS (*Advanced Mobile Phone System*) ouvir conversas era uma tarefa relativamente simples, e podia ser feito por um scanner de rádio. A segurança do aparelho era baseado no número de série do aparelho (ESN – *Electronic Serial Number*) que era enviado em aberto. Qualquer um então poderia "ouvir" e clonar um aparelho.

Os sistemas CDMA e TDMA, conhecidos pelo público como sistemas digitais, dificultaram a captura dos dados das conversações já que as mesmas eram enviadas moduladas digitalmente e multiplexadas por tempo (TDMA) ou por divisão de código (CDMA), porém mesmo assim um "hacker" poderia capturar os dados, decodificá-lo e interceptar as informações.

As partes importantes da segurança em celulares ficam por conta de autenticar o assinante, confidencialidade da informação (dados, voz e sinalização). Especificamente em GPRS é preciso ainda proteger informações que dizem respeito à cobrança. Como o pagamento em GPRS é feito sobre volume de dados, informação desnecessária precisa ser filtrada e os tickets de cobrança gerados pelo sistema, precisam ser protegidos.

5.2 – Algoritmos do GSM/GPRS

Os algoritmos de segurança do GSM são usados para prover autenticação e privacidade dos usuários em uma rede GSM.

O GSM usa três tipos de algoritmos chamados A3, A5 e A8. Normalmente A3 e A8 são utilizados simultaneamente (conhecido como A3/A8). Os algoritmos A3/A8 são implementados no cartão SIM e nas redes GSM. É usado para autenticar os assinantes e gerar uma chave para criptografia dos dados e voz.

O algoritmo A5, por sua vez, embaralha a voz e dados dos usuários entre o handset e a BSU para prover privacidade. Um algoritmo A5 é implementado em ambos.

Cada usuário tem sua IMSI (*International Mobile Subscriber Identity*), única em todas as redes GSM ao redor do mundo e que não varia (a não ser em caso de perda ou troca do SIM-Card pelo assinante, por exemplo). O IMSI tem, nas redes GSM, função análoga ao do ESN nos celulares analógicos. Porém sendo esta identificação única, fazer com que a IMSI trafegasse abertamente (clear text) seria permitir que o telefone pudesse ser clonado ou que o assinante do serviço pudesse ter sua localização traçada.

Para proteger o IMSI, o GSMI utiliza o um TMSI (*Temporary Mobile Subscriber Identity*). Em geral, no momento em que o aparelho móvel é ligado, o IMSI é transmitido e

a rede, no VLR, estabelece uma relação entre o IMSI e um TMSI gerado. A partir deste momento, somente o TMSI trafega.

A substituição do TMSI ocorre a cada troca de VLR (havendo possível troca de operadora) e, eventualmente, mediante requisição de uma das partes.

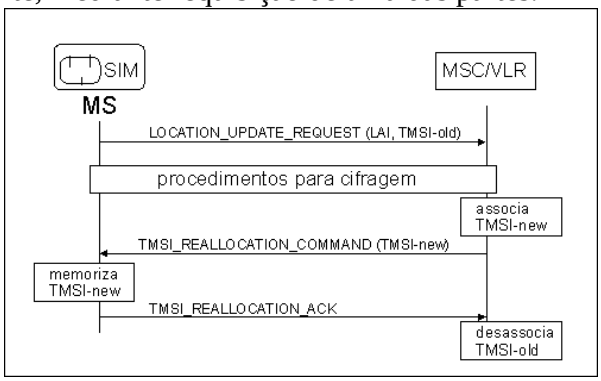

Figura 17: Esquema de Troca do TMSI

O sistema GPRS substituiu o TMSI pela TLLI (*Temporary Logical Link Identity*). A diferença entre os dois é que o TMSI é tratado pelo MSC nas redes GSM, enquanto o TLLI é tratado em GPRS pelo SGSN.

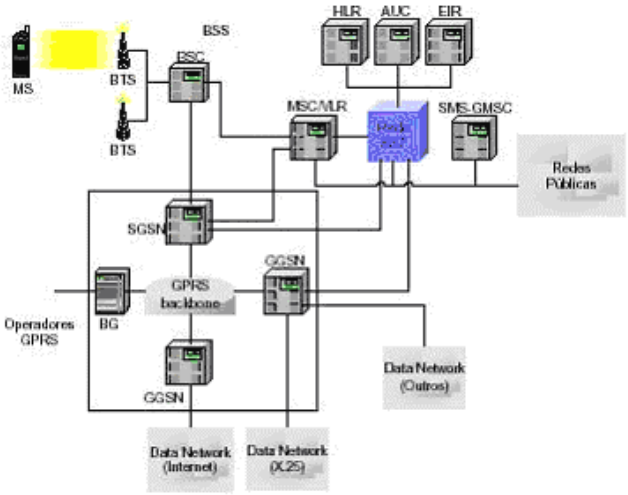

Figura 18: Elementos de uma rede GSM

As redes GSM-GPRS autenticam a identidade do assinante através de um mecanismo de desafio e resposta (*challenge-response mechanism*). A BTS envia para a MS um número aleatório de 128 bits (RAND). O SIM-Card então recebe o número RAND e computa, fornecendo RAND e uma chave Ki (compartilhada entre o SIM-card e a) como parâmetro do algoritmo A3 – uma função de Hash dependente de chave – um número (SRES) de 32 bits. O número SRES é verificado pela AUC, que também conhece A3, Ki e

RAND. O SRES calculado pelo SIM só será igual, portanto, caso ele tenha o mesmo Ki. Uma das questões polêmicas quanto a este procedimento é que a baixa capacidade de processamento do SIM-Card impede que Ki seja uma chave grande, o que torna o sistema relativamente frágil. Como A3 é um algoritmo somente utilizando dentro do SIM-Card e da AUC, ele não é especificado pelos padrões GSM ou GPRS – cada operadora é livre para adotar seu próprio A3.

Em redes GSM, após a autenticação, uma chave Kc é estabelecida entre BTS e MS e todas as mensagens são criptografadas por ambos usando a chave Kc com um algoritmo simétrico (o A5 criptografa streams ao invés de blocos). O A5 tem três versões:

- A5/2 – utilizada geralmente pelo GSM (exceto quem usa A5/1).
- A5/1 – utilizada nos EUA e Europa e é mais robusta do que o A5/2.
- A5/0 – utilizada por países sob sanções da ONU e não utiliza criptografia.
- A5/3 – uma nova versão do A5, baseada no algoritmo Kasumi (que também será usada em 3G) foi regulamentada e padronizada, porém ainda não está efetivamente em uso.

O A5/1 (versão com exportação restrita) tem chave de 64 bits, mas seus 10 últimos bits não são usados, gerando uma chave real de 54bits. Uma implementação deste algoritmo criptoanalisada por Briceno em 1999 pode ser encontrada e se baseia que durante os primeiros 0,1s os codificadores de voz codificam um silêncio gerando aproximadamente 1300 bits de dados que podem ser criptoanalisados. Mais tarde descobriu-se algo semelhante no A5/2, e oficialmente um ataque ao A5/2 tem complexidade de $O(2^{16})$.

O GPRS substitui o A5/1 e o A5/2 pelo GPRS/A5. A diferença está na cada em que a criptografia é feita. O GSM faz na camada RR entre a MS e a BTS, o GPRS faz na camada LLC entre o MS e a SGSN. A BTS então não tem acesso a informação do GPRS. Existem várias versões do GEA. Se um aparelho GPRS vai se conectar a uma rede estrangeira, ele inicia uma negociação para se estabelecer uma versão de GEA com a qual os dois sejam compatíveis. Se nenhuma intersecção for encontrada, a conexão tem que ser feita em sinal aberto.

5.2.1 - Introdução a Algoritmos de Criptografia Simétricos

Algoritmos de criptografia simétricos são aqueles que para criptografia e decriptografia são usadas a mesma chave. Um algoritmo bom deste tipo, a segurança dos dados reside na chave (de alguma maneira confiável as partes deverão saber da chave). O mais conhecido algoritmo simétrico é o DES (*Data Encryption Standart*) e atualmente o novo padrão é o AES (*Advanced Encryption Standart*). A cifragem pode ser via blocos ou via streams.

5.2.1.1 - Cifradores de Blocos

A informação (por exemplo um conjunto de bytes) é dividida em blocos ou grupo de bits fixos. O DES usa uma chave de 56bits em blocos de 64 bits de dados claros, gerando 64 bits criptografados. Ainda os cifradores de blocos podem ser divididos em

CBC, ECB e CFB. CBC e CFB são modos onde o bloco depende dos dados e chave do último bloco.

5.2.1.2 - Cifradores de Streams

Estes operam em um modo bit-a-bit, produzindo um bit encriptado a partir de um bit em texto claro. Estes são normalmente implementados em portas XOR (Exclusive OR) dos dados com a chave. A segurança deste algoritmo é determinada pelas propriedades especiais da chave. Uma chave-stream totalmente aleatória garante a cifragem efetiva dos dados.

O algoritmo do GSM A5 usado para criptografar voz e sinalização é um cifrador de stream com três LFSR controlados por clock (tempo).

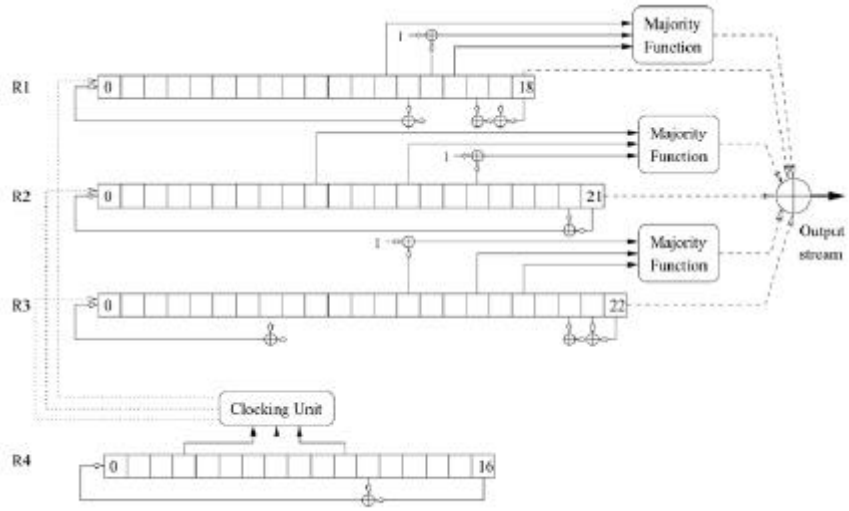

Figura 19: Estrutura Interna do A5/2

5.2.1.3 - Hashs

Normalmente uma função de hash é uma via única que gera uma saída de tamanho fixo, e uma vez aplicado um hash em uma entrada é computacionalmente impossível determinar a entrada a partir de sua saída. Também conhecida como "*One-time Hash*". Os exemplos mais conhecidos de algoritmos de hash são MD5 e SHA1. Isto é útil para motivos de autenticação, onde o transmissor e receptor usam uma função de hash dependente de chave em uma situação de desafio-resposta. Uma função de hash dependente de chave é facilmente implementada adicionando no final da mensagem a chave e calculando o seu hash. Outro aspecto é no uso de cifradores simétricos de bloco usando CFB, onde a chave para o próximo bloco é o hash do bloco atual. Os algoritmos do GSM/GRPS A3 e A8 usam algoritmos que são funções de hash dependentes de chave. O

GSM A3 e A8 são similares em funcionalidade e normalmente são implentados juntos em um algoritmo chamado COMP128.

5.3 - Aspectos de segurança do GSM

Os aspectos de segurança do GSM consistem em autenticar, confidencialidade de identidade e de voz e dados, além da garantia dos dados de sinalização. Como já visto, um assinante é identificado por um IMSI e essa informação gera uma chave de autenticação (Ki) que é análogo ao ESN do AMPS, e a autenticação é feita por um esquema de desafio-resposta, enquanto os dados críticos (tais como chaves) nunca são transmitidos pelo canal de rádio. O MS é identificado através de uma TMSI (Temporary Mobile Subscriber Identity) ao qual é cedido pela rede GSM e trocado periodicamente (durante hand-offs por exemplo).

O sistema de segurança do GSM depende do SIM (Subscriber Identity Module). O SIM contém um IMSI, uma chave pessoal (Ki), um algoritmo de geração de chaves (A8), um algoritmo de autenticação (A3) e um número de Identificação Pessoal (PIN – Personal Identificator Number) e o telefone contém um algoritmo de criptografia (A5). Os algoritmos (A3, A5 e A8) estão presentes em uma rede GSM. O Centro de Autenticação (AUC), parte do OMS, consiste no banco de dados de autenticação dos assinantes. Estas informações consistem em IMSI, o TMSI e o LAI (Location Area Identifier) e a chave de autenticação individual do assinante (Ki) para cada assinante. Todos os itens (MS, SIM e Rede GSM) são necesários. Isto resolve os problemas de segurança e impede fraudes como clonagem e escuta das conversas telefônicas.

A figura mostra a distribuição de informação de segurança entre os três elementos (MS, SIM, GSM). Enquanto nas redes GSM a segurança é distribuida através do AUC, o HLR (Home Location Register) e o VLR (Visitor Location Register). O AUC é responsável por gerar conjuntos de RAND, SRES e Kc que são armazenados na HLR e VLR para autenticação e privacidade.

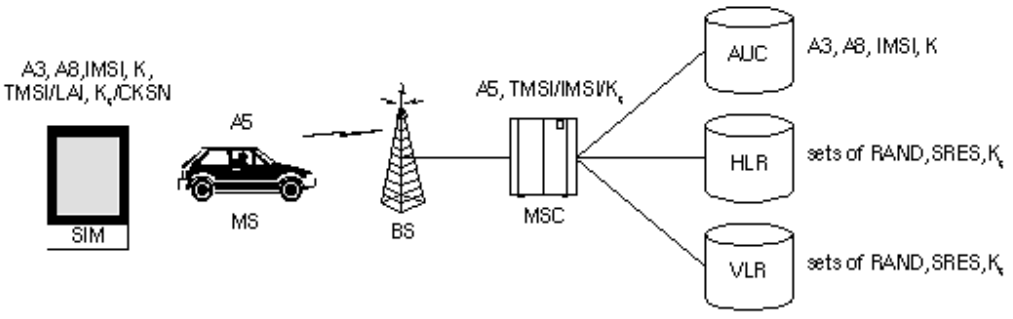

Figura 20: Algoritmos na rede GSM

5.3.1 - Autenticação.

A Rede GSM autentica a identidade do assinante no esquema de desafio resposta. Um número RAND (randômico de 128 bits) é enviado ao MS. O MS calcula uma resposta assinada de 32 bits (SRES) baseada na cifragem do número randômico (RAND) usando o algoritmo A3 baseado na chave individual do usuário (Ki). Quando a rede GSM receber a resposta SRES, ela repete o cálculo e verifica a identidade do usuário se o resultado dos cálculos forem iguais. Se a resposta SRES for autenticada, então o MS foi autenticado e pode continuar, senão a conexão é desfeita e é gerado um indicador de falha.

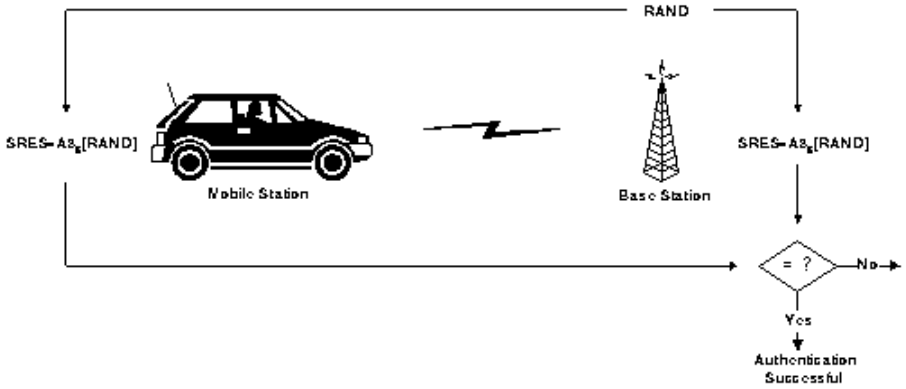

Figura 21: Autenticação em Redes GSM

5.3.2 - Sinalização e Confidencialidade dos Dados.

O SIM contém um algoritmo para criação de chaves cifradas (A8) que é usada para produzir uma chave de 64-bits (Kc). A chave é calculada aplicando o mesmo número randômico (RAND) usado no processo de autenticação para a geração da chave (A8) com uma chave individual de autenticação (Ki). A chave Kc é usada para cifrar e decifrar texto entre o MS e a BSS. Um nível adicional de segurança é alcançado tendo maneira de altera a chave, fazendo um esquema menos susceptível à “hackers”. A chave pode ser alterada em tempos regulares conforme requerido pela rede GSM. Vejamos o cálculo da chave Kc.

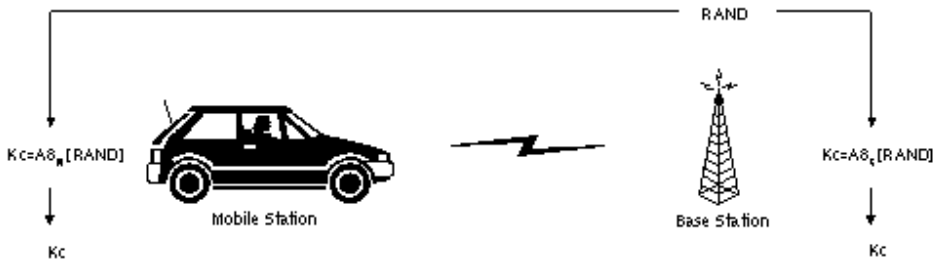

Figura 22: Cálculo do Kc nas redes GSM

De maneira similar o processo de autenticação, o cálculo de criptografia (Kc) é feito internamento ao SIM. Entretanto informações sensitivas tias como informações de chaves (Ki) nunca são reveladas pelo SIM. Voz e dados criptografados entre o MS e a rede é feito usando o algoritmo A5. Comunicação cifrada é iniciada pelo comando de requisição de ciframento da rede GSM. Uma vez recebido este comando, a MS começa a cifrar e decifrar usando o algoritmo A5 e a chave Kc.

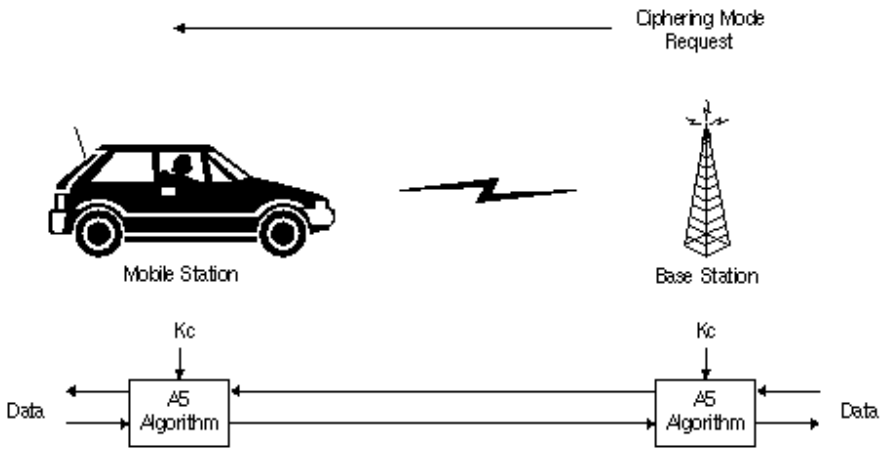

Figura 23: Criptografia de Dados em GSM

5.3.4 - Confidencialidade da Identidade do Assinante.

Para garantir a confidencialidade a TMSI é usada (*Temporary Mobile Subscriber Identity*). A TMSI é enviada para a MS após a autenticação e criptografia ser estabelecida. A MS responde confirmando a recepção TMSI e essa é válida na LAI que ela está. Se a localidade for alterada, é necessária a adição e realocação de outro TMSI.

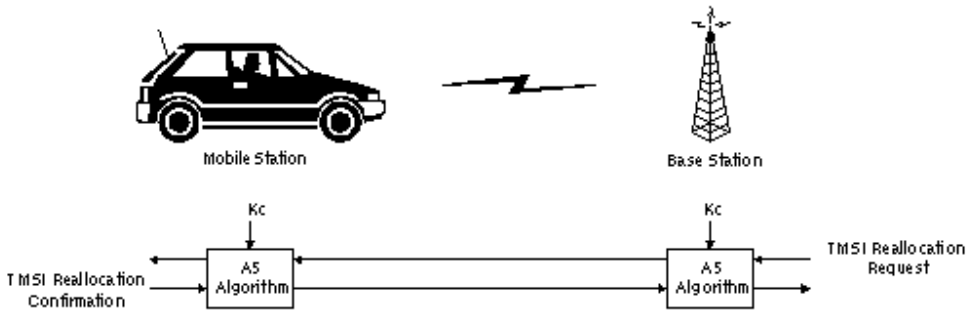

Figura 24: Realocação do TMSI

5.4 - GSM – Algoritmos de Ciframento

Uma parte da implementação do GSM A5 vazou na Internet em Junho de 94. Mais recentemente houve rumores que esta implementação era uma versão antiga e possuia algumas diferenças para o código atualmente mostrado. Porém os seguintes itens são usados no A5:

- A5 é um cifrador de stream consistindo em três LFSR controlados por clock com 19, 22 e 23 níveis.
- O controlador de clock tem uma função de transbordo no meio dos bits de cada um dos três shift-registers.
- A soma dos níveis dos três shift-registers é 64. Uma variável de sessão de 64-bit é usada para inicializar o conteúdo dos shift-registers.
- Duas streams de 114 bits são usadas de chaves para cada frame TDMA, e é efetuado um XOR dos dados de uplink e downlink com as chaves.
- Os rumores que o A5 tem uma chave “efetiva” de 40 bits.

5.4.1 - Restrição de Exportação de Tecnologia de Criptografia

O objetivo do GSM é prover uma técnica de celulares digitais para a Europa. Como conseqüência disso, as restrições de exportação e outras restrições legais da criptografia precisam ser verificadas.

Os detalhes técnicos do algoritmo de criptografia do GSM ainda guarda alguns segredos. Estes algoritmos foram desenvolvidos na Grã-bretanha, e um fabricante que desejar implementar criptografia deve aceitar as exigências do governo Inglês. As agências de Inteligência dos EUA, França, Inglaterra entre outras ficam preocupadas com a exportação de criptografia forte porque essa pode ser usada por nações hostis. A Europa e outros poucos como Hong Kong e EUA usam o algoritmo A5/1. Uma versão mais fraca chamada A5/2 foi aprovada para exportação em todos os países do mundo, exceto em alguns como Russia que não podem usar criptografia (A5/0). Espera-se que em breve estes países possam receber a versão A5/2.

5.4.1.1 - Tamanho das Chaves

O tamanho da chave muitas vezes está associada diretamente à força da criptografia. Assumindo que a força bruta (teste de todas as chaves) seja a única maneira de quebrar uma cifragem, a tabela abaixo nos dá uma idéia de quanto tempo leva para um computador capaz de realizar um milhão de tentativas por segundo levaria:

32 bits = 1,19h
40 bits = 12,7 dias
56 bits = 2291 anos
64 bits = 584542 anos
128 bits = $10{,}8 \times 10^{24}$ anos (o universo tem $1{,}6 \times 10^{10}$ anos).

Assumindo que normalmente um A5 tem 40 bits de chave efetiva (64 declaradas), este é bastante seguro para prover segurança de uma informação com curto espaço, tornando difícil atacar o mesmo.

5.5 – Ataques ao GSM

5.5.1 - O Ataque de Shamir, Biryukov e Wagner

Na época os melhores ataques ao GSM A5/1 (versão mais robusta do A5) necessitavam de muito processamento e estavam na ordem de complexidade de 2^{40} a 2^{45} passos para um ataque "pelo ar". Isto tornava um ataque ao GSM impraticável. Este ataque consiste em preparar um ataque em 2^{48} passos e a partir daí o ataque pode acontecer em tempo real em um PC. Este ataque requer uma amostra de 2 minutos de conversação, e o PC descobre o algoritmo em 1 segundo, outro ataque é pegando dois segundos de conversação e calcula-se a chave em poucos minutos

5.5.2 - O Ataque de Goldberg e Wagner

Em 1999, Ian Goldberg e David Wagner anunciaram um ataque durante a Crypto99 no A5/2 (versão menos robusta) que requeria alguns poucos bits e apenas 2^{16} passos, demonstrando que a versão "de exportação" do A5 é bastante insegura.

5.5.3 - O Ataque de Briceno, Goldberg e Wagner

O SIM nunca deveria deixar vazar a chave, mesmo que o atacante tenha acesso ao SIM, entretanto os três autores descobriram uma falha matemática no algoritmo que pode comprometer a chave. Em situações normais, o SIM é questionado para assinar um pacote,

e dependendo da resposta a ERB autoriza ou não isso. Entretanto, provou-se que com aproximadamente 150mil tentativas é possível coletar informações e deduzir a chave, o que leva de 8 a 12 horas em um leitor de smartcard que faz 6 perguntas/segundo ao SIM, porém este ataque é tecnicamente difícil via ar, já que o atacante precisa simular uma ERB e enviar perguntas ao MS.

5.5.4 - O novo ataque de Barkan, Biham e Keller

Como se sabe, existem três tipos de algoritmos usados em GSM. A5 é um cifrador de streams, o A3 é um algoritmo de autenticação e o A8 é um algoritmo de "acordos de chaves" (key-agreement). O A3/A8 não foi totalmente especificado, deixando as operadoras decidirem, porém muitas operadoras usam um "quase padrão" COMP128. Apesar de detalhes não terem sido revelado, garantem que é possível ter acesso a conversação .

À revista New Scientist, estes pesquisadores disseram que é possível explorar uma falha de segurança não na criptografia em si, mas em como a tecnologia é aplicada aos aparelhos. No sistema GSM, a voz é digitalizada mas, antes de os dados serem criptografados, eles incluem uma espécie de CRC. É entre estes dois pontos que a ligação pode ser interceptada, dizem: entre o aparelho e a estação-base da rede.

Eli Biham, o cientista que comandou o estudo, disse à revista que duvidou a princípio que esta operação pudesse ser feita, mas que vários testes provaram ser possível, sim, quebrar este sistema de segurança. E que a técnica permite que a ligação seja interceptada antes de ser atendida - estudos antigos conseguiram formas nada práticas de se ouvir apenas os primeiros minutos de uma conversa, lembrou.

5.5.5 - Ataques ao GSM na prática

Comunicação móvel está sendo rapidamente disponível nos últimos anos. Ele provê serviços importantes para usuários que desejam ter um serviço mais flexível, porém para isto pagam mais do que as linhas fixas, um dos possíveis desejos do atacante é falar gratuitamente (ou que outra pessoa pague pelo serviço).

Existem vários tipos de fraudes em telefones celulares, vamos tentar classificar e mostrar um ponto de vista sobre isso.

Um ataque ao antigo modelo AMPS é relativamente fácil, porém um ataque a uma rede digital, como a GSM, requer mais equipamentos para executar, e isso pode desencorajar o atacante.

O custo para a operadora deste ataque pode ser interno ou externo. O interno é apenas uma perda de lucro pela operadora, por não estar tarifando uma chamada ou por um cliente usar um recurso sem permissão. Por outro lado o externo depende de dinheiro. Por exemplo quando um cliente da operadora A vai para a operadora B, a operadora A paga para a B pelo uso da rede GSM, e se o atacante estiver em roaming, a operadora terá que desembolsar pelo tráfego, sem receber do seu assinante.

O ataque externo geralmente acontece quando o usuário da operadora A se desloca para B para efetuar chamadas (geralmente internacionais) se "beneficiando" do não pagamento dessa chamada. Isto acontece porque as operadoras têm um atraso na troca de bilhetagem uma com as outras (normalmente de 12 à 48h).

A clonagem de aparelhos (fazendo com que um pague por outro) é um grande problema, porém o GSM tem uma excelente proteção contra clonagem.

A clonagem de GSM é bem mais difícil (mas possível), porém clonar um SIM não é considerado um problema. O problema está na autenticação. O algoritmo COMP128 que é o mais usado é a razão disso. Dado certos ambientes, o algoritmo pode deixar vazar a chave secreta (Ki).

Um fato interessante é que muitas vezes as operadoras usam exemplos de fraudes para forçar as autoridades a aumentar as penas pelo crime contra elas. Nos EUA o ato de scanear a rede da operadora com a intenção de usar, fraudar, possuir ou clonar telefones pode dar de 10 a 15 anos de prisão. Porém se existem poucas fraudes, elas usam isso como publicidade boa para que seus assinantes sejam encorajados a usar os seus celulares.

Outro tipo de fraude é o uso criminal da comunicação, ou seja, usar o celular para efetuar um ataque sem ser encontrado. Por exemplo, um assinante usa um telefone GSM para acessar a Internet e roubar informações e/ou dinheiro digitalmente. As operadoras podem identificar o local de onde o telefone está com uma precisão variando de acordo com o número de ERBs. Quanto mais ERBs em um local, maior a precisão. Estatísticas dizem que 80% dos traficantes de drogas usam celulares clonados, e muitos são capturados usando o rastreamento do telefone.

Por exemplo, no modo analógico (AMPS) o ESN é o identificador do telefone. Um "hacker" poderia escutar o ESN de algum telefone em sua área e reprogramar um outro telefone para informar as ERBs o mesmo ESN. Neste caso, várias medidas podem ser tomadas, porém entre as mais usadas estão a Detecção de Telefones Duplicados, RF fingerprinting (fingerprint é uma impressão digital e normalmente dois telefones diferentes com o mesmo ESN tem características de RF diferentes), Verificação de Velocidade (chamadas em locais distantes com poucos minutos de diferença), Verificação de Perfil (média estatística de uso de um assinante), etc.

5.6 - Conclusão

No atual momento, as fraudes possíveis em GSM acabam não valendo a pena devido à dificuldade no ataque, já que requerem alto número de equipamentos e a complexidade dos ataques fazem com que nem sempre se usufrua os "benefícios do ataque". Possivelmente no futuro isso se torne mais simples, porém no atual momento esses ataques são muito caros e impraticáveis.

Bibliografia

Hynninen, Jukka
Experiences in Mobile Phone fraud
http://www.niksula.cs.hut.fi/~jthynnin/mobfra.html

Mynttinen, Juha
End-to-End Security Mobile Data in GSM
http://www.hut.fi/~jmynttin/netsec/paper.pdf

Margrave, David
GSM Security and Encryption
http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html

Peng, Chengyan
GSM and GPRS Security
http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers/peng.pdf

Luna, Herbert; Rochol, Juergen
Um estudo comparativo e a questão de interconexão com redes heterogêneas
http://labcom.inf.ufrgs.br/artigos/seguranca_em_sistemas.pdf

Briceno, Marc; Goldberg, Ian; Wagner, David
A pedagogical implementation of A5/1
http://packetstormsecurity.nl/crypt/cryptanalysis/a51-pi.htm

GSM, Global System for Mobile Communications
GSM Security Algorithms
http://www.gsmworld.com/using/algorithms/index.shtml

GSM, Global System for Mobile Communications
A5/3 and GEA3 Specifications
http://www.gsmworld.com/using/algorithms/docs/a5_3_and_gea3_specifications.pdf

Uma Visão sobre Segurança nas Redes GSM, GPRS e UMTS
Penha, André; Souza, Rafael Nanya; Boldrini, Rafael
http://www.ic.unicamp.br/~980649/sec.html

GSM Clonning
Briceno, Marc; Goldberg, Ian
http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html

Conheça as vantagens e desvantagens do sistema GSM
Abreu Jr., Wanderley J.
http://www.terra.com.br/informatica/2002/11/14/006.htm

Israelenses quebram segurança da telefonia GSM
Reuters Internacional
http://informatica.terra.com.br/interna/0,,OI137473-EI553,00.html

Cientistas acham criptografia do GSM vulnerável
Mesquita, Renata; Reuters Internacional
http://info.abril.com.br/aberto/infonews/092003/09092003-7.shl

Kurose, James; Keith, Ross
Computer Network: A Top Down Approach Featuring the Internet
Second Edition, Editora Addison Wesley

Tenembaum, Andrew S.
Redes de Computadores – 3a. Edição
Editora Pretince Hall

Jornal do Brasil Online
Novo celular chega em 2004 - Edge
http://jbonline.terra.com.br/jb/papel/cadernos/internet/2003/09/14/jorinf20030914005.html

What Is?Com
http://www.whatis.com

Guimarães, Dayane Adionei
Material do curso Comunicações Móveis II
Pós-Graduação “Engenharia de Redes e Sistemas de Telecomunicações” - INATEL

Sistemas GSM
Curso Corporativo - Oferecido pela Universidade Federal Fluminense

Usha Communications Technology -
GPRS Gerneral Packet Radio Service
Johan Runebou ERA/LY/UX – Ericsson – GPRS Overview

Mobileipworld.com
http://www.3g-generation.com/gprs_and_edge.htm

Os primeiros passos do GPRS
http://www.telemoveis.com/articles/item.asp?ID=387

GSM, Global System for Mobile Communications
GPRS Platform
http://www.gsmworld.com/technology/gprs/index.shtml