

LOCALIZAÇÃO GEOGRÁFICA ATRAVÉS DE APARELHO CELULAR

Allan Rangel Cordeiro

Curso de Engenharia Elétrica – Universidade Federal do Paraná

Curitiba – Paraná – Brasil

e-mail: al_ee@ufpr.br

Resumo - Este artigo tem como objetivo demonstrar a viabilidade de aplicação de um sistema de localização geográfica através de aparelhos celulares, utilizando-se para isso do atual sistema GSM em operação nas cidades brasileiras. O projeto visa estudar uma alternativa ao já difundido GPS (*Global Positioning System*), sem que para isto necessite do auxílio de satélites ou outros novos investimentos.

NOMENCLATURA

AOA	<i>Angle of Arrival</i>
ARFCN	<i>Absolute Radio Frequency Channel Number</i>
AUC	<i>Authentication Centre</i>
BSC	<i>Base Station Controller</i>
BSS	<i>Base Station Subsystem</i>
BTS	<i>Base Transceiver Station</i>
CCH	<i>Control Channel</i>
CCITT	<i>Comitê Consultivo de Telefonia e Telegrafia Internacional</i>
Cell ID	<i>Cell identity</i>
CGI	<i>Cell Global Identity</i>
DCS	<i>Digital Cellular System</i>
DoD	<i>Department of Defense</i>
DSSS	<i>Direct Sequence Spread Spectrum</i>
EIR	<i>Equipment Identity Register</i>
ERB	<i>Estação Rádio Base</i>
FHMA	<i>Frequency Hopping Multiple Access</i>
FHSS	<i>Frequency Hopping Spread Spectrum</i>
GMLC	<i>Gateway Mobile Location Centre</i>
GMSC	<i>Gateway Mobile Switching Centre</i>
GPS	<i>Global Positioning System</i>
GSM	<i>Global System for Mobile</i>
HLR	<i>Home Location Register</i>
HO	<i>Handover</i>
IMEI	<i>International Mobile Equipment Identity</i>
IMSI	<i>International Mobile Subscriber Identity</i>
LAC	<i>Location Area Code</i>
LAI	<i>Location Area Identifier</i>
LBS	<i>Location Based Service</i>
LCS	<i>Location Services</i>
LMU	<i>Location Measurement Unit</i>
MAP	<i>Mobile Application Part</i>
ME	<i>Mobile Equipment</i>
MS	<i>Mobile Station</i>
MSC	<i>Mobile Switching Center</i>
MSISDN	<i>Mobile Subscriber Integrated Services Digital Network Number</i>
NMC	<i>Organização de Gerenciamento da Rede</i>
OMC	<i>Operation and Maintenance Center</i>
OMS	<i>Operation and Management Subsystem</i>
PCS	<i>Personal Communication System</i>

PLMN	<i>Private Land Mobile Network</i>
RTPC	<i>Rede de Telefonia Pública Comutada</i>
RTT	<i>Round Trip Time</i>
SIM	<i>Subscriber Identity Module</i>
SMLC	<i>Serving Mobile Location Center</i>
TA	<i>Timing Advanced</i>
TCH	<i>Traffic Channel</i>
TDMA	<i>Time Division Multiple Access</i>
TDOA	<i>Time Difference Of Arrival</i>
TRAU	<i>Transcoder and Rate Adapter Unit</i>
UIT	<i>União Internacional de Telecomunicações</i>
VLR	<i>Visitor Location Register</i>

I. INTRODUÇÃO

Com o desenvolvimento da tecnologia novas necessidades vão sendo incorporadas visando facilitar o dia-a-dia das pessoas. Nos últimos anos o GPS (*Global Positioning System*) tem sido cada vez mais utilizado como sistema de localização geográfica global. Inicialmente utilizado principalmente em atividades como navegação marítima, está sendo adicionado ao cotidiano das cidades brasileiras, atrelado à softwares que localizam o aparelho em um mapa da cidade em questão.

Existem atualmente dois sistemas efetivos de posicionamento por satélite; o GPS (EUA) e o Glonass (russo); além de dois sistemas em implantação: o Galileo europeu e o Compass chinês. Tal diversidade mostra-se estrategicamente importante, uma vez que o sistema GPS é controlado pelo DoD (Departamento de Defesa dos Estados Unidos da América) para uso exclusivo militar e, embora atualmente, esteja disponibilizado o uso e civil gratuito, não existem garantias de que assim continuará.

Ao longo deste trabalho iremos demonstrar um sistema alternativo para localização geográfica, baseado no rastreamento do aparelho celular do cliente, à ser utilizado principalmente nas grandes cidades. O trabalho será desenvolvido sobre o sistema celular GSM em operação, visando reduzir ao máximo novos custos para sua implementação.

II. A TECNOLOGIA GSM

A principal tecnologia utilizada atualmente no sistema celular brasileiro é o GSM (*Global System for Mobile Communication*). Primeiramente será apresentado a seguir um breve resumo da tecnologia GSM.

O GSM é atualmente utilizado em vários países. Começou a ser usado na Europa e em seguida se difundiu pelo mundo. Esta tecnologia pode ser separado em 3 sistemas: GSM900 (frequência de 900MHz), DCS1800 (*Digital Cellular System* na frequência de 1800MH) e

PCS1900 (*Personal Communication System* na frequência de 1900MHz), a operadora celular TIM SUL, por exemplo, trabalha especificamente com as frequências de 900 e 1800 MHz. Segue a faixa de frequência do GSM utilizada:

TABELA I
Frequências utilizadas pela TIM SUL em MHz

	GSM 900	DCS 1800	PCS 1900
Estação Móvel -> ERB	880-915	1710-1785	1850-1910
ERB -> Estação Móvel	925-960	1805-1880	1930-1990
Espaçamento entre frequências de Transmissão e Recepção	45	95	80

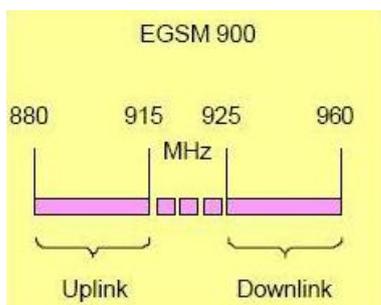


Fig. 1. No *Extended GSM 900*, o *uplink* está na faixa de 800 a 915 Mhz e o *downlink* de 925 a 960 Mhz

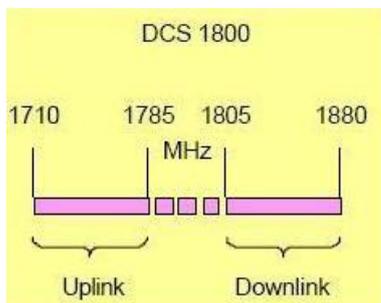


Fig. 2. No DCS 1800, o *uplink* está na faixa de 1710 a 1785 Mhz e o *downlink* de 1805 a 1880 Mhz

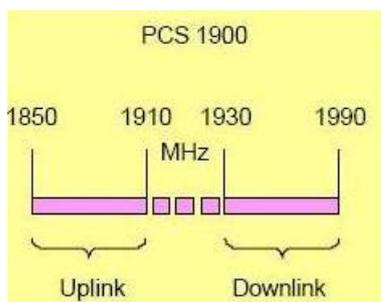


Fig. 3. No PCS 1900, o *uplink* está na faixa de 1850 a 1910 Mhz e o *downlink* de 1930 a 1990 Mhz

A rede GSM é formada por várias entidades. Sua arquitetura é muito flexível, o que torna extremamente viável e vantajosa para as operadoras dos sistemas móveis celulares. Podemos dividi-la em três partes principais, sendo a estação móvel, o subsistema estação base e o subsistema de rede.

MS – Mobile Station: É a estação móvel, terminal utilizado pelo assinante no qual é inserido o *SIM Card* (chip que contém as informações do usuário, e armazena um número de 15 dígitos que identifica uma dada estação móvel, o IMSI – Identidade Internacional do Assinante Móvel).

BTS: Uma célula de rádio, ou BTS (*Base Transceiver Station*) é a menor área de serviço em uma PLMN (Rede Pública de Comutação Móvel). Uma célula consiste de uma estação rádio-base que transmite através de uma pequena área geográfica (representada por um hexágono). O tamanho máximo de uma célula pode ter até 35 km de raio para o sistema GSM900 e até 8km de raio para o DSC1800/PCS1900.

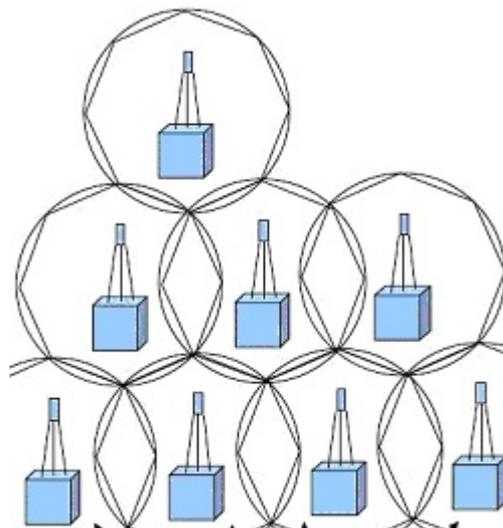


Fig. 4. Conjunto de células ou BTSs

BSS (Base Station Subsystem – Sistema da estação base): se comunica com a estação móvel do assinante através de interface de rádio-frequência.

A BSS é composta pelos equipamentos:

- **BSC (Base Station Controller):** responsável pelas funções inteligentes da BSS, atribuindo conexões de canal de tráfego a partir da SSS à BTS, e também controla toda a BSS. Uma BSC pode controlar várias BTSs e várias TRAU.
 - **BTS (Base Transceiver Station):** compreende os equipamentos de transmissão e recepção de rádio. Contém um ou mais transceptores (TRX) e serve até 24 células.
 - **TRAU (Transcoder and Rate Adapter Unit):** é o equipamento onde codificação e decodificação são executadas assim como a adaptação da taxa.
- Cada BSS é conectada a uma MSC (Central de Comutação de Serviços Móveis) que pertence ao SSS (Subsistema de comutação - Switching Subsystem) e é responsável pelo roteamento das conexões de canal de tráfego. As MSCs estão conectadas entre si e à rede fixa.

A BSC é responsável pela configuração dos canais de rádio, saltos de frequência e transição entre células (*hand-over*) sendo responsável por prover a interface da MS com a MSC (Centro de Comutação Móvel). Uma BSC pode gerenciar os recursos de uma ou mais BTS.

O Subsistema de rede é a parte responsável pela interconexão da rede GSM com a rede pública (RTPC) e também por todo gerenciamento da base de dados e o processamento das informações através das interfaces. Composto de elementos de rede como, o Centro de

Comutação de Serviços Móveis (MSC), o Registro de Localização de Unidade Móvel Local (HLR), o Registro de Localização de Unidade Móvel Visitante (VLR), o Equipamento de Identificação de Registro (EIR), e o Centro de Autenticação de Unidade Móvel (AuC).

Os principais componentes do Subsistema de Rede para o desenvolvimento desse artigo são o MSC, o HLR e o VLR.

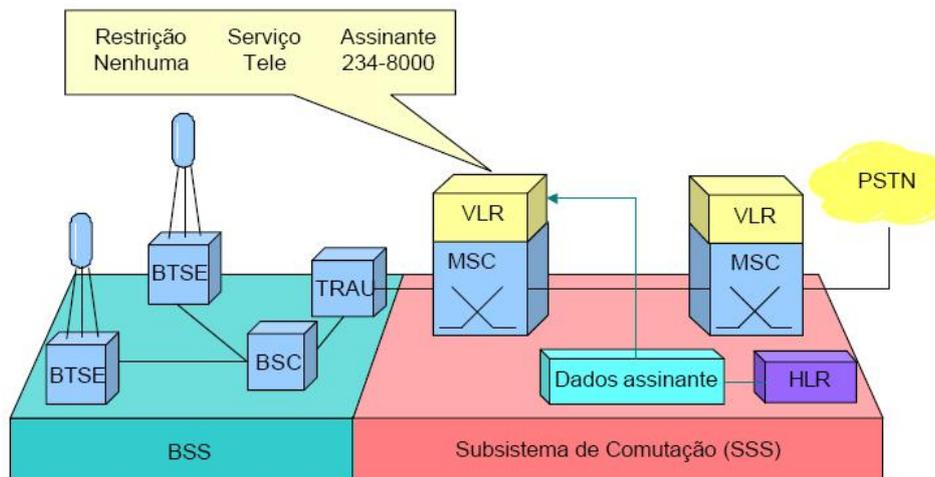


Fig. 5. Componentes da BSS e do SSS

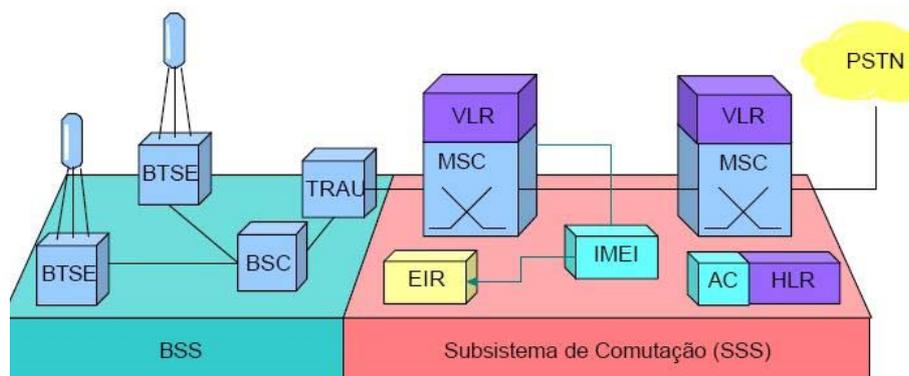


Fig. 6. Base de dados do cliente

MSC (Mobile Switching Center): É a Central de Comutação e Controle, que controla várias BSSs. A MSC é responsável pelas funções de comutação e sinalização para as estações móveis. Essa central controla o tráfego entre diversas células. E nela encontramos as informações dos assinantes, tais como o VLR (*Visitor Location Register – Registro de Localização de Visitante*), onde os celulares que não estão na sua área local possam ser localizados; o HLR (*Home Location Register – registro de Localização de Unidade Móvel Local*); o AuC (*Authentication Centre – Central de Autenticação*) que é responsável pela autenticação dos assinantes no uso do sistema, e possibilita a autenticação do IMSI, sendo também responsável por gerar a chave para criptografar a comunicação entre o MS e a BTS.

HLR: É uma base de dados na qual os assinantes móveis são criados, cancelados e bloqueados. Contém as identidades de assinantes permanentes, assim como os serviços que um assinante está autorizado a utilizar. Armazena e gerencia todas as assinaturas da rede móvel, pertencente a uma operadora específica. Inclui dados dos assinantes como: Identidade do assinante (IMSI, MSISDN - *Mobile Subscriber Integrated Services Digital Network Number*); serviços complementares de assinantes; informação de localização do assinante; gerenciamento da base de dados da assinatura; comunicação com os MSCs (*Gateway Mobile Switching Centre*); comunicação com os AuC's; comunicação com os VLR's.

VLR: contém os dados relevantes de todos os assinantes móveis atualmente na área de serviço de uma MSC. Os

dados permanentes são os mesmos que os encontrados no HLR. A localização de dados no VLR reduz o tráfego de dados ao HLR, pois este não é sempre responsável pelo fornecimento dos dados. Há um VLR para cada área de serviço de uma MSC; atua como um armazenamento temporário (informação de assinatura) para as EMs que estão numa área de serviço de uma MSC particular; verifica IMSI do assinante e checka se o mesmo tem registro em sua área, ou não; caso não encontre registro de uma EM, envia requisição para o HLR.

EIR (Equipment Identity Register): permite verificar a situação legal do equipamento pelo sistema indicando, por exemplo, se determinado aparelho foi roubado. É a base de dados que armazena os IMEIs (Identidade Internacional do Equipamento Móvel – número de 15 dígitos determinado pelo fabricante) dos terminais móveis, da OMC

(Organização de Operação e Manutenção), entidade funcional através da qual a operadora monitora e controla o sistema e a NMC (Organização de Gerenciamento da Rede). Esta central ainda possui interfaces para ligar outras redes, como a PLMN (Redes Privadas de Telefonia Fixa), padrão SS#7 (Sistema de Sinalização número 7), a RPTC (Redes Públicas de Telefonia Comutada) e redes RDSI (Rede Digital de Serviços Integrados).

OMS (Subsistema de Operação e Manutenção): centraliza a monitoração dos componentes de rede da SSS e da BSS. É formado pelos Centros de Operação e Manutenção (OMC). A operação e manutenção para SSS e BSS são independentes, mas podem ser realizados num mesmo local.

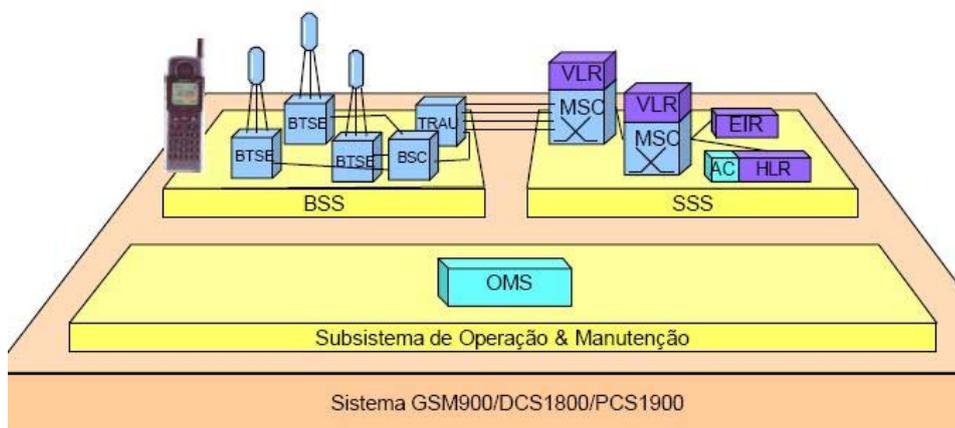


Fig. 7. Subsistema de Operação e Manutenção

O *Handover* (HO) é o processo de comutação de uma chamada em andamento de um canal de rádio para outro, é necessário para reter uma chamada quando o usuário passa de uma área de cobertura de uma célula para outra.

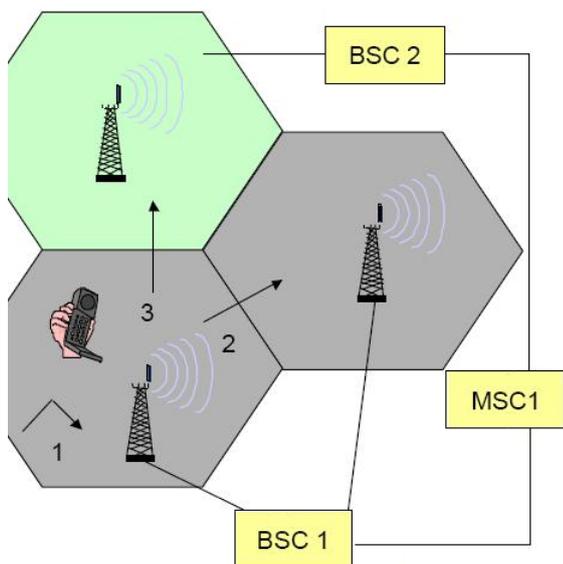


Fig. 8. 1 – Handover intra-célula
2 – Handover intercélula interno
3 – Handover intercélula externo

A BTS é a torre propriamente dita (ERB – estação rádio base), é nela em que estão as antenas, normalmente direcionais, voltadas para um azimute (ângulo em que a antena estará posicionada na torre em relação ao norte geográfico) de acordo com a região que se deseja irradiar preferencialmente o sinal. Interface Abis é o link (normalmente microondas) entre a BSC e a BTS. Uma BSC normalmente controla várias BTSs de uma região.

As bandas do GSM são divididas em canais de RF, onde cada canal consiste de um par de frequências (Transmissão e Recepção) com 200 KHz de banda cada. Conclui-se que o DCS 1800 possui 373 canais; e o GSM 900, 124 canais. Estes canais receberam uma numeração conhecida como ARFCN (*Absolute Rádio Frequency Channel Number*). As frequências portadoras dos canais de RF são moduladas em 0,3GMSK (*Gaussian Minimum Shift Keying* – tipo de modulação digital que reduz o espectro do sinal modulado) por um sinal digital com taxa de 270,833 kbit/s. Este sinal digital é dividido em 8 intervalos de tempo (*time slots*) possibilitando o múltiplo acesso por divisão no tempo TDMA das Estações Móveis.

TABELA II
Slots de tempo

	Período	Composição
Sinal de 270,833 kbit/s	4,615 ms	8 slots de tempo
Slot de tempo	576,9 us	156,25 bits
Bit	3,692 us	-

O GSM assim como o TDMA (IS-136) é uma combinação de FHMA (*Frequency Hopping Multiple Access*) e TDMA.

Existem dois tipos básicos de canais lógicos no sistema GSM que ocupam a estrutura do quadro (frame) TDMA: TCH (canal de tráfego) e CCH (canal de controle); eles transmitem a informação do usuário, voz, dados e os dados de controle da sinalização.

O TCH suporta duas taxas de informação: a *Full Rate*, quando o canal de RF tem 8 canais e cada canal utiliza um time slot. A segunda, o *Half Rate*, quando o canal de RF tem 16 canais, neste caso 2 canais lógicos ocupam alternadamente um mesmo time slot.

As taxas de informação para os canais de tráfego (TCH) são:

TABELA III
Canais de tráfego

	<i>Full Rate</i>	<i>Half Rate</i>
Voz	13 kbit/s (22,8 kbit/s bruta)	11,4 kbit/s
Dados	9,6 kbit/s, 4,8 kbit/s e 3,6 kbit/s	4,8 kbit/s e 2,4 kbit/s

Temos ainda o BCH (*Broadcast Channel*) no qual o MS localiza a célula de melhor nível de sinal, e o MS permanece nesse canal.

A eficiência de utilização do espectro (capacidade do sistema) GSM é muito boa, em 200kHz tem capacidade para 8 chamadas, enquanto que o AMPS e o TDMA em 30kHz tem capacidade para 1 chamada e 3 chamadas, respectivamente.

O sistema GSM apresenta uma menor interferência co-canal, ou seja, quando uma célula utiliza o canal 620, por exemplo, nenhuma de suas vizinhas (ao redor) ou células próximas devem utilizar esta mesma frequência pois terá interferência, assim como também não se pode usar canais adjacentes, neste caso seriam os canais 619 e 621. Temos assim uma melhor utilização do espectro do sistema.

O recurso de *frequency hopping* (saltos de frequências), é capaz de tornar mais eficaz o reuso de frequências.

O método FHSS (*Frequency Hopping Spread Spectrum* - Espelhamento por Saltos em Frequências) faz parte da técnica *Spread-Spectrum* que, espalha a informação por uma banda muito maior do que a necessária para sua transmissão. Para tal, FHSS divide a banda total em vários canais de pequena largura de banda. Desta forma, transmissor e receptor saltam por estes canais conforme uma seqüência pseudo-aleatória conhecida por ambos.

Até pode-se dizer que o FHSS usa a largura de banda de forma ineficaz, pois ocupa toda a banda para realizar o espelhamento; Sistemas em FHSS geralmente apresentam velocidades inferiores em relação aos que trabalham em DSSS (*Direct Sequence Spread Spectrum*). Porém quando

se fala em segurança, o FHSS é robusto; pois receptores não desejados, não conhecem a seqüência pseudo-aleatória utilizada, encherçando sistemas FHSS como ruídos de curta duração.

Exemplo: alguns dispositivos WLAN que operam na faixa de 2400 a 2483 MHz utilizam FHSS. Neste caso, divide-se a banda em 79 canais de 1MHz e os saltos ocorrem no mínimo a cada 0,4 segundo.

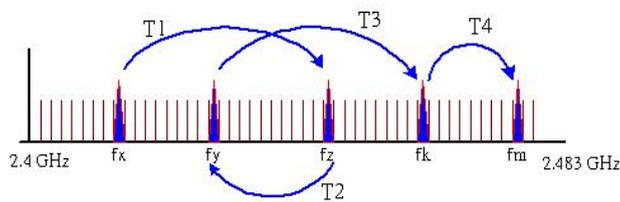


Fig. 9. Método de Espelhamento por Saltos de Frequências

Outra importante característica da Modulação por Espalhamento de Espectro é que esta provê uma proteção contra interferência externa com potência finita. O sinal causador de interferência pode consistir de um ruído de banda larga bastante poderoso ou de uma forma de onda de múltiplas frequências que são dirigidas ao receptor de forma a degradar a comunicação. A proteção contra estas interferências é obtida fazendo com que o sinal contendo a informação ocupe propositalmente uma largura de banda maior do que a necessária para transmiti-lo. Isto faz com que o sinal transmitido tenha uma aparência semelhante ao ruído. O sinal pode então propagar-se através do canal sem ser imprópriamente detectado.

Já foi descrito ao longo do texto algumas interfaces da arquitetura GSM, segue abaixo mais o complemento destas interfaces

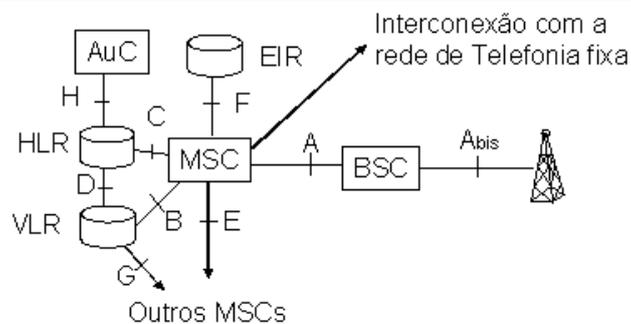


Fig. 10. Interfaces da rede GSM

As interfaces da arquitetura de uma rede GSM, apresentadas na figura, foram padronizadas de modo a permitir a interoperabilidade com outras redes, incluindo roaming internacional, e permitindo a utilização de diversos fornecedores na sua implantação.

Interface Abis entre ERB (BTS) e BSC: Esta interface suporta dois tipos de links: canais de tráfego a 64 kbit/s levando voz ou dados do usuário e canais de sinalização BSC-BTS a 16 kbit/s.

Interface A entre BSC e MSC: Está especificada pelas normas do GSM. A camada física é um 2 Mbit/s padrão CCITT (Comitê Consultivo de Telefonia e Telegrafia Internacional) que é o órgão responsável pelo estudo técnico de questões relativas a operação, tarifação e

elaboração de recomendações para padronizar as telecomunicações a nível mundial.

Interfaces C, D, E, F, G: Foram padronizadas pelo protocolo MAP (*Móbile Application Part*) que utiliza os serviços de transação e transferência de mensagens do Sistema de Sinalização número 7 (SS#7).

Em um sistema de telefonia fixa é necessário que exista entre as centrais telefônicas, além dos troncos com os canais de voz, um sistema de sinalização por onde são trocadas mensagens de modo a se estabelecer uma chamada telefônica entre dois assinantes. O Sistema de

Sinalização número 7 é o padrão adotado pela UIT (União Internacional de Telecomunicações) e utiliza um canal dedicado para a comunicação.

Interface entre MSC e redes de Telefonia Fixa: A interconexão entre MSC e redes fixas utiliza o Padrão SS#7 TUP ou ISUP.

Interfaces B e H: As interfaces B entre MSC e VLR e H entre HLR e AUC não estão padronizadas pois tratam-se de interfaces internas do MSC/VLR e do HLR/AUC.

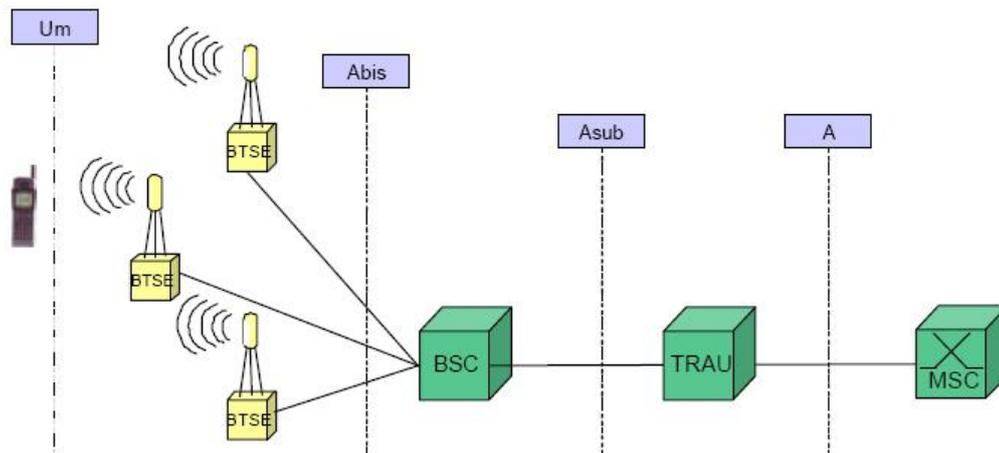


Fig. 11. Rede GSM

Os serviços de localização padronizados para o GSM permitem estimar com precisão a localização da estação móvel servindo de base para vários serviços oferecidos ao assinante.

III. LOCALIZAÇÃO GEOGRÁFICA CELULAR

Para competir com o mercado de telefonia fixa, a TIM celular lançou o serviço TIM-FIXO, o qual é um exemplo da utilização de LBS (*Location Based Service*). Através do sistema GSM, é identificado o local de utilização do aparelho e deste modo somente são permitidas ligações dentro de um limite territorial pré-determinado, o qual geralmente se trata da residência do cliente. Em troca desta restrição o assinante tem planos específicos e tarifas menores para a realização de chamadas.

Para o funcionamento do sistema é utilizada uma técnica, desenvolvida pela operadora, que faz a localização do ME em nível de rede, chamada CELL-ID, a qual explicaremos adiante.

Para possibilitar a localização geográfica de um aparelho celular em uma rede de telefonia móvel, é necessária a adição de alguns elementos à arquitetura da rede. Estes permitem que a rede determine a localização de um telefone celular, trazendo a possibilidade de aplicação do serviço proposto.

O LGS é o serviço de localização de vital importância em um LBS. Ele envia os dados referentes à localização para uma aplicação LBS. Sendo o responsável por determinar o melhor método de localização de um móvel, realizar a conversão de sistemas, identificar o alvo (IMEI,

IMSI, IP), estimar a precisão das informações, proteger a privacidade das informações e possibilitar a realização de cobranças dos serviços prestados.

Outros componentes importantes na arquitetura LBS são: *Gateway Mobile Location Center* (GMLC) e o *Serving Mobile Location Center* (SMLC).

O GMLC é o primeiro nó que um cliente LCS acessa em uma rede GSM ou UMTS. O GMLC pode também solicitar informações de roteamento ao HLR e após realizar seu registro de autorização, enviar os pedidos de posicionamento para a MSC e receber as estimativas de localização das devidas entidades.

Dependendo do tamanho da rede podemos ter um ou vários GMLCs, além da possibilidade para interligação entre GMLCs de diferentes operadores, como apoio de posicionamento para assinantes em *roaming*. Os pedidos de localização são recebidos por um GMLC de um LCS cliente, que coordena todo processo de posicionamento e, finalmente, retorna como os dados de localização do cliente. Na arquitetura GSM ele está ligado ao SMLC via MSC. Através de sua integração com as BSCs, o GMLC pode ser visto como a interface entre o SMLC e um LCS *client*, em diversas redes de acesso.

O SMLC coordena e controla todo o processo de localização de um ME, incluindo a avaliação das medições dos intervalos de tempo, alocação dos recursos, cálculos das posições e ainda das precisões alcançadas. É visto como um elemento de rede separado ou de funcionalidade integrada a BSC, de modo que auxilia o LCS. Dependendo do método utilizado pode controlar uma ou várias LMUs (*Location Measurement Unit*), equipamento essencial nas

aplicações de LBS e indicá-las como medir as transmissões de *downlink* e *uplink*.

Os diferentes SMLCs provenientes de outras redes de acesso devem interagir entre si, coordenando o posicionamento dos assinantes que se deslocam entre os acessos destas redes.

O LMU observa a transmissão dos dados de diferentes estações-base ou a partir de terminais efetuando medições de tempo. Esse equipamento está associado à BSS de uma rede GSM, realizando medições de rádio, baseado em serviços de localização. A observação de *downlink* detecta uma compensação no tempo entre as faixas horárias de diferentes estações-base e é utilizada para alcançar uma posterior sincronização necessária em alguns métodos de localização existentes. As observações do *uplink* de terminais também servem como ferramentas utilizadas para alguns métodos de localização. As coordenadas das BTS das referidas LMUs, devem ser bem conhecidas, a fim de relacionar as medições dos intervalos para os respectivos terminais ou estações-base.

Existem algumas topologias possíveis para o serviço de localização, neste documento é apresentado o modelo a seguir.

A aplicação é o órgão responsável pelo controle do serviço. Este aplicativo é responsável pela realização das rotinas, cadastramento dos usuários e processamento das informações de posicionamento geográfico.

Método do Cell-ID

Está entre os primeiros métodos de localização geográfica, onde a localização do aparelho celular é obtida a partir da identificação da BTS que atende o cliente. Este é o método utilizado no serviço do TIM-Fixo citado anteriormente. Através da identificação do setor utilizado é possível restringir a área obtida, uma vez que cada setor geralmente abrange 120° a partir da torre. Dependendo de fatores como local, obstáculos, relevo, quantidade de BTSs próximas, dentre outros, este método obtêm uma precisão que varia entre 50m e 30km (em áreas urbanas e rurais respectivamente). Apesar de barato e de fácil implementação, tal método não é muito preciso.

Método do Timing Advanced (TA)

O *Timing advanced* (TA) é o tempo de latência entre o aparelho móvel e a estação rádio base que ele está utilizando, esta medição é conhecida como RTT (*Round Trip Time*). A graduação deste método segue uma escala de 550m; de modo que temos *timing advanced 1* para valores próximos à 550m, e *timing advanced 2* para valores próximos a 1100m, como ilustrado na tabela a seguir.

TABELA IV
Escala de medidas de Timing Advanced

Distância	TA
0 – 550 m	0
550 – 1100 m	1
1100 – 1650 m	2

Para que seja definido qual o melhor setor a ser utilizado, a rede GSM requisita o nível de intensidade de até 6 células próximas ao cliente, de modo a definir qual será a servidora e possíveis candidatas à *handovers*; com esta informação podemos estimar a distância do aparelho celular à cada um dos setores em questão.

Admitindo-se que o sinal trafega à velocidade da luz, é medido o tempo entre a transmissão e recepção do sinal entre o móvel e a BTS e então estimada a distância do celular a partir da torre. Cruzando estes dados com os obtidos a partir de outras BTSs vizinhas, é possível chegar à localização aproximada do cliente.

Para que o mesmo seja aplicável é necessário a instalação de um LMU junto às ERBs, equipamento responsável pela captura e registro do tempo de viagem do sinal ao aparelho móvel. Em seguida o LMU envia estes dados ao SMLC que é encarregado de determinar a localização do aparelho celular.

Cada distância obtida possui uma margem de erro inerente, mas através de um procedimento de triangulação destas medidas é possível obter a área mais provável da localização geográfica do aparelho celular.

De acordo com a prática de campo verifica-se uma média de precisão deste método em torno de 243-248m para locais urbanos e de 755-785m em áreas rurais.

Para o serviço proposto, sempre em que ocorre o início de uma chamada, a MSC utilizada reporta o número de CGI (*Cell Global Identity*), que identifica o setor da BTS utilizado, ao cliente LCS. Este por sua vez, solicita o TA (*Timing Advanced*) à Central de comutação (MSC).

Respeitando a sequência de comunicação: ME – BTS – BSS – MSC – HLR – GMLC – Cliente LCS.

Vale lembrar que em regiões urbanas devido à menor área de abrangência de cada setor e ao maior número de BTSs devemos obter uma maior precisão neste método de localização geográfica.

A central de comutação caberá a tarefa de identificar os setores utilizados pelo cliente e reportar esta informação à aplicação de LBS. A aplicação se encarregará de requisitar o TA para através do método descrito anteriormente possamos obter a localização do móvel.

Exemplo prático:

Temos abaixo na Fig. 10 o mapa da região de Curitiba, no bairro Campo Comprido. Foram representadas 3 BTSs reais da operadora TIM; e cada setor foi indicado por uma linha azul que mostra a sua direção.

Através da medição dos TAs em relação à cada uma das torres foram traçadas as circunferências de TA (em amarelo). Como a graduação segue uma escala de 550m, deve-se respeitar a respectiva margem de erro. Deste modo foram traçadas 2 circunferências ao redor de cada BTS representando os respectivos valores de máximo e mínimo para a incerteza.

O aparelho celular, representado pela marcação amarela ao centro, está à 671 m da torre 'A'; 904 m da torre 'B' e 1522 m da torre 'C'. Receberia indicações de TA = 1, TA = 1 e TA = 2, para as torres 'A', 'B' e 'C' respectivamente.

Uma vez que $TA = 1$ indica que o cliente está entre 550 e 1100 m da torre devemos marcar a região que este exemplo ilustra um caso hipotético onde existem apenas 3 BTSs nas proximidades, porém em regiões

corresponde à intersecção das medidas, em vermelho na figura abaixo. urbanas facilmente encontram-se mais de 6 BTS próximas, o que aumenta a precisão do método.



Fig. 12 – Caso prático utilizando 3 BTSs.

Tal aplicação pode ser adotada facilmente como alternativa ao GPS, tanto para localização geográfica dentro de centros urbanos, quanto em outras finalidades. Podemos pensar na localização de pessoas com necessidades especiais ou portadores de doenças como o Alzheimer, que causa perda de memória e poderia levar uma pessoa a se perder facilmente. Deste modo, através de um contrato com a operadora de telefonia celular os familiares poderiam localizá-la em caso de necessidade. Vale ressaltar ainda outro enfoque que pode ser explorado a partir deste estudo, como o serviço de localização de frota de caminhões ou automóveis, e busca de eventuais veículos roubados, uma vez que a preocupação com segurança vem ganhando cada vez mais espaço na sociedade atual.

II. CONCLUSÕES

Sistemas de localização geográfica estão sendo utilizados em diversas áreas tanto para fins comerciais quanto pessoais. O sistema GPS é amplamente utilizado, porém está baseado no sistema de satélites militares norte americano, o qual não possui garantias de continuidade de disponibilização ao grande público. Deste modo é importante e até mesmo estratégico que busquemos novas formas para implementar este serviço.

Aproveitando-se da estrutura e equipamentos já utilizados no sistema GSM em operação e utilizando-se de aparelhos celulares, o quais estão geralmente ao alcance da maioria das pessoas; temos a oportunidade de pensar em novos serviços passíveis de serem disponibilizados.

Com relação ao desenvolvimento do trabalho, houve certa dificuldade para encontrar algumas informações vitais para o seu desenvolvimento; como por exemplo à respeito do funcionamento do serviço TIM-Fixo (Cell-ID). Uma vez que este possui pouca precisão, não se mostrou adequado e foi necessário buscar outra alternativa. Após pesquisa, o método escolhido se utiliza da medida de *Timing Advanced*, e através de uma triangulação de sinais permite uma maior precisão.

O projeto proposto é de fácil aplicação e possui relativo baixo custo de implementação, o que pode ser visto como atrativo à sua adoção e futuros estudos relacionados.

AGRADECIMENTOS

O autor agradece à orientação que receberam do Professor Dr. Ewaldo Luiz M. Mehl na elaboração deste trabalho. Agradece também à empresa TIM CELULAR e funcionários pelo empréstimo de material técnico utilizado na pesquisa.

REFERÊNCIAS

- [1] w1.siemens.com/entry/br/pt - Siemens Brasil – acessado em 15/04/2009
- [2] www.wirelessbrasil.org - Conceitos GSM – acessado em 09/05/2009
- [3] www.anatel.gov.br - acessado em 25/04/2009.

- [4] HEINE, Gunnar. GSM Networks: Protocols, Terminology and Implementation. Artech House mobile communications library. 685 Canton Street, Norwood, MA. United States. Second Edition, 1999.
- [5] SVERZUT, José Umberto. Redes GSM, GPRS, EDGE E UMTS: evolução a caminho da terceira geração. 1 ed. São Paulo: Érica Ltda, 2005.
- [6] NETO, Vicente Soares; PETRUCCI, Lucilio Augusto; TEIXEIRA, Paulo Sérgio de Assis. Sistema de Propagação e Rádio Enlace. Primeira Edição. São Paulo: Editora Érica, 1999
- [7] SIEGMUND M. Redl; Matthias K. Weber; Malcolm W. Oliphant. "An Introduction to GSM", Artech House, March 1995.
- [8] BLOGH, J.S; HANZO L.S. Third – Generation Systems and Intelligent Wireless Networking: smart antennas and adaptive modulation. England. John Wiley & Sons, Ltd, 2002.

DADOS BIOGRÁFICOS

Allan Rangel Cordeiro, nascido em 19/06/1986 em Curitiba (Paraná), é Graduando do Curso de Engenharia Elétrica da Universidade Federal do Paraná. Foi estagiário da empresa On-Line Engenharia (2006 - 2007), COPEL Distribuição S/A (2007-2008) e também da TIM CELULAR S/A (2008-2009) na área de Telecomunicações.