

A ENGENHARIA POR TRÁS DO SINAL

Do Terreno ao Usuário Final

O ciclo completo das redes móveis: do planejamento
à operação, de 2G a 6G



Wagner R Bomfim

A ENGENHARIA POR TRÁS DO SINAL

Do Terreno ao Usuário Final

A Enciclopédia Definitiva do Ciclo de Vida de Sistemas Móveis:

Planejamento, Engenharia, Implantação, Integração,
Aceitação, Drive Test, Otimização e Operação, de 2G a 6G

PREÂMBULO DO AUTOR

Este livro nasceu de uma constatação simples e incômoda: não existe, em nenhum idioma, uma obra que cubra o ciclo completo de um sistema móvel celular — do momento em que uma operadora identifica uma necessidade de cobertura até o instante em que o usuário final pressiona "enviar" e vê a mensagem chegar ao destino. Os livros existentes ou são técnicos demais, ou são superficiais demais, ou fragmentados demais. Esta obra preenche esse vazio.

Não é um livro para ser lido de uma só vez. É uma enciclopédia de referência, para consulta permanente de engenheiros, gestores, estudantes e curiosos. Cada capítulo foi escrito para ser autossuficiente, mas o conjunto forma uma narrativa completa: a biografia de um sinal, da terra ao celular.

ÍNDICE GERAL

- PARTE I. FUNDAMENTOS, HISTÓRIA E ARQUITETURA DAS REDES MÓVEIS
- PARTE II. ESTRATÉGIA, NEGÓCIO E PLANEJAMENTO DE EXPANSÃO
- PARTE III. AQUISIÇÃO, ESTUDO E APROVAÇÃO DO TERRENO
- PARTE IV. ENGENHARIA EXECUTIVA E INFRAESTRUTURA
- PARTE V. CONSTRUÇÃO, INSTALAÇÃO E CONTROLE DE QUALIDADE
- PARTE VI. CONFIGURAÇÃO, INTEGRAÇÃO E COMISSIONAMENTO
- PARTE VII. ACEITAÇÃO TÉCNICA E ENTREGA OPERACIONAL
- PARTE VIII. DRIVE TEST E VALIDAÇÃO DE CAMPO
- PARTE IX. OTIMIZAÇÃO E ENGENHARIA DE PERFORMANCE
- PARTE X. TRANSMISSÃO, CORE E SERVIÇOS END-TO-END
- PARTE XI. OPERAÇÃO, MANUTENÇÃO E GESTÃO DE REDE
- PARTE XII. EXPERIÊNCIA DO USUÁRIO FINAL

- PARTE XIII. TECNOLOGIAS EMERGENTES E FUTURO
- PARTE XIV. GESTÃO INTEGRADA DE PROJETOS E OPERAÇÕES
- PARTE XV. O PROJETO COMPLETO: DO ZERO À OPERAÇÃO

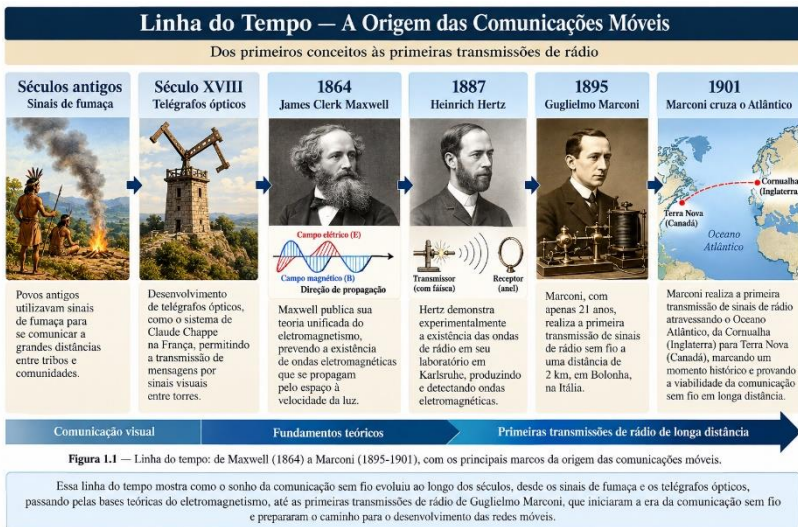
PARTE I. FUNDAMENTOS, HISTÓRIA E ARQUITETURA DAS REDES MÓVEIS

Capítulo 1. A origem das comunicações móveis

1.1 O sonho antigo da comunicação sem fio

A história das comunicações móveis não começa com o celular. Começa com um sonho antigo da humanidade: comunicar-se à distância sem fios. Esse sonho atravessa séculos — desde os sinais de fumaça dos povos indígenas até os telégrafos ópticos do século XVIII, passando pelas experiências de Faraday, Maxwell e Hertz no século XIX, que estabeleceram as bases teóricas do eletromagnetismo.

Em 1864, James Clerk Maxwell publicou sua teoria unificada do eletromagnetismo, prevendo a existência de ondas eletromagnéticas que se propagam pelo espaço à velocidade da luz. Em 1887, Heinrich Hertz demonstrou experimentalmente a existência dessas ondas, produzindo e detectando ondas de rádio em seu laboratório em Karlsruhe. Mas foi Guglielmo Marconi, um jovem italiano de 21 anos, quem transformou a teoria em tecnologia prática. Em 1895, Marconi transmitiu sinais de rádio a uma distância de 2 km em Bolonha. Em 1901, cruzou o Atlântico, transmitindo da Cornualha (Inglaterra) para Terra Nova (Canadá). A era da comunicação sem fio havia começado.



No entanto, a comunicação móvel — no sentido de permitir que usuários se movam enquanto se comunicam — demorou décadas para se tornar realidade. As primeiras aplicações do rádio eram fixas: comunicação navio-terra, estações costeiras, telegrafia sem fio. A mobilidade exigia superar desafios técnicos formidáveis: antenas compactas, baixo consumo de energia, handover (a transferência de uma chamada de uma estação base para outra sem interrupção), e gestão de espectro.

1.2 Os primeiros sistemas móveis: antes do celular

Antes do conceito celular, existiam os sistemas de rádio móvel terrestre (Land Mobile Radio). Nos anos 1920 e 1930, a polícia de Detroit e outras cidades americanas usavam rádio em viaturas para comunicação com a central. Esses sistemas eram

simplex (uma frequência, um falante por vez), com alcance limitado e capacidade mínima.

Durante a Segunda Guerra Mundial, o desenvolvimento de rádios portáteis (walkie-talkies) acelerou. Após a guerra, surgiram os primeiros sistemas de telefonia móvel comercial, como o MTS (Mobile Telephone Service) nos Estados Unidos, em 1946. O MTS usava uma única estação base de alta potência cobrindo uma cidade inteira, com pouquíssimos canais disponíveis. Em Nova York, o sistema tinha apenas 12 canais para toda a cidade — e a lista de espera para obter uma linha chegava a anos.

O problema fundamental era a capacidade. Com uma única estação base de alta potência, não havia como reutilizar frequências. O espectro era um recurso escasso, e o MTS o desperdiçava. A solução viria com a ideia celular.



Figura 1.2 — Comparação entre o sistema MTS (uma única estação base) e o sistema celular (muitas estações base), mostrando a evolução da arquitetura, cobertura e capacidade.

O sistema MTS utilizava uma única estação base de alta potência para cobrir uma grande área, com poucos canais e capacidade muito limitada. O sistema celular introduziu o conceito de múltiplas células de baixa potência, permitindo a reutilização de frequências, aumentando significativamente a capacidade da rede e viabilizando a comunicação móvel em larga escala.

1.3 A invenção do conceito celular

A ideia celular é atribuída a D. H. Ring, dos Laboratórios Bell, que em 1947 descreveu um sistema de comunicações móveis baseado em células hexagonais com reutilização de frequências. A ideia era simples, mas revolucionária: em vez de uma única estação base de alta potência cobrindo uma cidade inteira, usar muitas estações base de baixa potência cobrindo pequenas áreas (células). Cada célula usava um subconjunto das frequências disponíveis. Células suficientemente distantes podiam reutilizar as mesmas frequências sem interferência significativa.

O padrão de reutilização mais comum é o de 7 células: um cluster de 7 células usa todas as frequências disponíveis, e esse cluster se repete geometricamente pelo território. A distância entre células que reutilizam a mesma frequência é chamada de distância de reuso (D), e a relação D/R (onde R é o raio da célula) define a qualidade da rede. Quanto maior D/R , menor a interferência, mas menor a capacidade total (menos reutilização).

Padrão de Reutilização de Frequências em Redes Celulares

Cluster de 7 células ($N = 7$) e distância de reuso (D)

1. Cluster de 7 células ($N = 7$)



Célula	Grupo de frequência	Cor
A	Grupo 1	Amarelo
B	Grupo 2	Verde
C	Grupo 3	Vermelho
D	Grupo 4	Azul
E	Grupo 5	Laranja
F	Grupo 6	Roxo
G	Grupo 7	Cinza

2. Repetição do cluster na rede



3. Distância de reuso (D)



4. Fórmulas principais

$$N = i^2 + j^2 + j$$

N = tamanho do cluster
 i, j = inteiros
(ex.: $i = 2, j = 1$)

Para $N = 7$:

$$N = 2^2 + 2 \cdot 1 + 1^2 = 7$$

($i = 2, j = 1$)

$$D = R \cdot \sqrt{3N}$$

D = distância de reuso
 R = raio da célula
 N = tamanho do cluster

5. Benefícios da reutilização de frequências



Maior capacidade
Permite o uso das mesmas frequências em células diferentes (não adjacentes).



Uso eficiente do espectro
O espectro limitado é reutilizado várias vezes na rede.



Menor interferência
Células suficientemente distantes reutilizam as mesmas frequências sem interferência significativa.



Escalabilidade
Permite atender um grande número de usuários em áreas extensas.

Figura 1.3 — Diagrama de clusters hexagonais: padrão de reutilização de 7 células, com cores diferentes para cada grupo de frequências. Ilustração detalhada mostrando o cluster, a repetição e a distância de reuso D .

Relação D/R em Redes Celulares

Distância de reuso (D), raio da célula (R) e número de células por cluster (N)

1. Diagrama do cluster e da distância de reuso



Célula	Grupo	Cor
A	1	Amarelo
B	2	Verde
C	3	Vermelho
D	4	Azul
E	5	Laranja
F	6	Roxo
G	7	Cinza

Células que utilizam o mesmo grupo de frequências (ex.: células A) são separadas pela distância de reuso D , evitando interferência significativa.

$$D = R \times \sqrt{3N}$$

D = distância de reuso (distância entre células que utilizam o mesmo grupo de frequência)

R = raio da célula (em km)

N = número de células por cluster
(i e j são inteiros na fórmula geral)

3. Exemplo numérico para $N = 7$

Para um cluster de 7 células ($N = 7$):

$$D = R \times \sqrt{3 \times 7} = R \times \sqrt{21}$$

$$\sqrt{21} \approx 4,583$$

$$D \approx 4,583 \times R$$

Exemplo prático:
Se o raio da célula for $R = 1$ km:

$$D = 1 \times \sqrt{21}$$

$$D \approx 4,583 \text{ km}$$

Se $R = 2$ km:

$$D = 2 \times \sqrt{21}$$

$$D \approx 9,166 \text{ km}$$

4. Impacto da relação D/R na rede



Maior D/R

- Células mais distantes reutilizam a mesma frequência
- Menor interferência entre células co-canais
- Melhor qualidade de sinal
- Menor capacidade total (menos reutilização de frequências)



Menor D/R

- Células mais próximas reutilizam a mesma frequência
- Maior interferência entre células co-canais
- Maior capacidade total (mais reutilização de frequências)
- Requer melhor controle de interferência (planejamento)

Apesar da ideia brilhante, a tecnologia dos anos 1940 e 1950 não permitia implementar o conceito celular. Faltavam computadores para gerenciar o handover, componentes miniaturizados para os terminais, e espectro alocado. O conceito ficou adormecido por décadas.

1.4 O primeiro sistema celular comercial: NTT no Japão

O primeiro sistema celular comercial do mundo foi implantado pela NTT (Nippon Telegraph and Telephone) no Japão, em 1979. Era um sistema analógico, operando na faixa de 800 MHz, com células relativamente grandes. Inicialmente cobria apenas Tóquio, mas expandiu-se rapidamente para outras cidades.

O sistema da NTT usava modulação FM, canais de 25 kHz, e controle centralizado. Os terminais eram grandes e pesados — instalados em carros, não portáteis. Mas era um sistema celular verdadeiro: reutilizava frequências, fazia handover, e permitia mobilidade.

1.5 AMPS: o sistema que popularizou o celular

Enquanto o Japão pioneirava, os Estados Unidos desenvolviam seu próprio sistema. Em 1983, a AMPS (Advanced Mobile Phone System) entrou em operação comercial nos Estados Unidos, desenvolvida pelos Laboratórios Bell. O AMPS operava na faixa de 800 MHz, com canais de 30 kHz, modulação FM, e controle distribuído.

O AMPS foi um sucesso estrondoso. Pela primeira vez, o celular se tornou acessível ao público em geral — embora ainda caro. Os primeiros terminais eram "tijolos" de vários quilos, mas a mobilidade era real. Em 1987, havia mais de 1 milhão de assinantes AMPS nos Estados Unidos.



1.6 NMT: o sistema nórdico

Em paralelo, os países nórdicos (Suécia, Noruega, Dinamarca, Finlândia) desenvolveram o NMT (Nordic Mobile Telephone), que entrou em operação em 1981. O NMT foi o primeiro sistema celular com roaming internacional automático — um usuário sueco podia viajar para a Noruega e continuar usando o celular. O NMT operava em 450 MHz (NMT-450) e depois 900 MHz (NMT-900).

O NMT foi crucial para o desenvolvimento da indústria de telecomunicações nórdica, especialmente a Ericsson e a Nokia, que se tornariam gigantes globais.

1.7 Os sistemas de primeira geração (1G): características comuns

Os sistemas 1G compartilhavam características fundamentais:

- **Analógicos:** a voz era modulada diretamente em FM, sem digitalização.
- **Foco em voz:** não havia serviços de dados (exceto tons de controle).
- **Capacidade limitada:** cada canal ocupava 25-30 kHz, e o número de canais por célula era pequeno.
- **Segurança nula:** qualquer pessoa com um scanner podia ouvir as conversas.
- **Padronização fragmentada:** AMPS nos EUA, TACS no Reino Unido, NMT nos países nórdicos, NTT no Japão. Um terminal não funcionava em outro país.
- **Terminais caros e grandes:** consumo de energia alto, baterias volumosas.

Apesar das limitações, o 1G provou que a comunicação móvel era viável e desejável. O caminho para a digitalização estava aberto.

Capítulo 2. A evolução dos sistemas analógicos à era digital

2.1 Por que digitalizar?

A transição do analógico para o digital não foi apenas uma mudança tecnológica — foi uma revolução conceitual. A digitalização trouxe benefícios que o analógico jamais poderia oferecer:

Qualidade de voz: no sistema analógico, o sinal degrada gradualmente com a distância e a interferência. No digital, o sinal é regenerado a cada repetidor, mantendo a qualidade até o limite de cobertura. Além disso, técnicas de correção de erro (FEC — Forward Error Correction) permitem recuperar parte da informação perdida.

Capacidade: a compressão digital de voz (codecs) reduz drasticamente a taxa de bits necessária. Enquanto um canal analógico ocupa 25-30 kHz, um canal digital GSM ocupa 200 kHz mas carrega 8 conversas simultâneas (TDMA), resultando em 25 kHz por conversa — mas com qualidade superior e possibilidade de compressão adicional.

Serviços de dados: o digital permite transmitir qualquer tipo de informação — texto, imagem, vídeo — não apenas voz. O SMS nasceu dessa capacidade.

Segurança: a criptografia digital protege as conversas de interceptação. O GSM introduziu autenticação e criptografia desde o início.

Eficiência espectral: técnicas digitais como TDMA, CDMA e OFDMA permitem compartilhar o espectro de formas muito mais eficientes que o analógico.

Integração com computadores: o digital permite que a rede móvel se integre naturalmente com a internet e outros sistemas digitais.

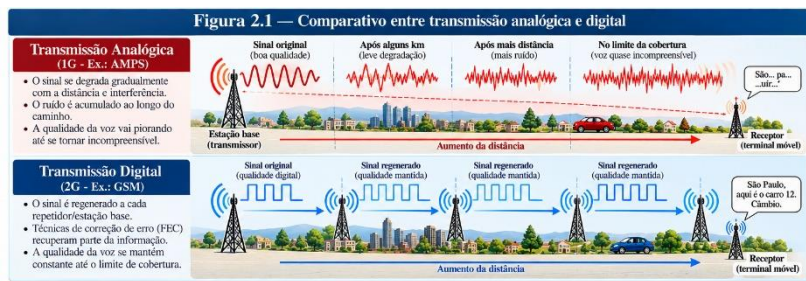


Figura 2.2 — Comparativo entre 1G (analógico) e 2G (digital)

Característica	1G (Analógico) Ex.: AMPS (EUA), NMT (Europa), TACS (Reino Unido)	2G (Digital) Ex.: GSM (Global), IS-95 (CDMA), PDC (Japão)
Período de implantação	Década de 1980 (ex.: AMPS em 1983)	Década de 1990 (ex.: GSM em 1991)
Tecnologia	Analógica (FDMA)	Digital (TDMA, CDMA)
Faixa de frequência	800 MHz (ex.: 824-849 MHz / 869-894 MHz)	900 MHz, 1800 MHz, 1900 MHz (vários por região)
Largura de canal	25-30 kHz por canal (uma conversa por canal)	200 kHz por canal (GSM) 8 conversas simultâneas (TDMA)
Capacidade por canal	1 conversa (voz)	8 conversas (GSM - TDMA)
Serviços	Apenas voz (analógica)	Voz (digital), SMS, dados (GPRS/EDGE), roaming internacional
Qualidade de voz	Degrada com a distância e interferência	Qualidade constante (regeneração e correção de erro)
Segurança	Sem criptografia (fácil de interceptar)	Autenticação e criptografia (ex.: A5/1, A5/2 no GSM)
Eficiência espectral	Baixa (FDMA simples)	Alta (TDMA/CDMA, compressão de voz)
Padronização	Vários sistemas nacionais (incompatíveis)	Padrão global (GSM) e maior interoperabilidade
Terminais	Grandes e pesados (instalados em carros)	Menores e mais leves (portáteis)

2.2 Os primeiros passos digitais: GSM e IS-95

A digitalização das comunicações móveis não aconteceu de forma única e uniforme. Ela ocorreu em duas frentes paralelas e concorrentes, que representavam filosofias técnicas radicalmente diferentes: o GSM na Europa e o IS-95 nos Estados Unidos. Entender essa dualidade é fundamental, porque ela moldou toda a evolução subsequente das redes

móveis — e, em certa medida, a competição entre essas duas filosofias continua até hoje, no 5G e além.

2.2.1 O contexto político e técnico do GSM

O GSM nasceu de uma necessidade política antes de ser uma necessidade técnica. Nos anos 1980, a Europa tinha uma colcha de retalhos de sistemas analógicos incompatíveis: NMT nos países nórdicos, TACS no Reino Unido e na Itália, C-450 na Alemanha e em Portugal, Radiocom 2000 na França. Um executivo que viajasse de Estocolmo para Roma precisava de dois ou três aparelhos diferentes, ou simplesmente não conseguia usar o celular. Essa fragmentação era um obstáculo não apenas para os usuários, mas para a própria ideia de um mercado europeu integrado.

Em 1982, a Conferência Europeia de Administrações Postais e de Telecomunicações (CEPT) criou o grupo Groupe Spécial Mobile (GSM) — daí o nome original, depois rebatizado como Global System for Mobile Communications. O objetivo era ambicioso: criar um padrão único, pan-europeu, digital, que permitisse roaming automático entre todos os países signatários. Em 1987, treze operadoras de doze países assinaram um memorando de entendimento comprometendo-se a implantar o sistema. Em 1989, a responsabilidade pela especificação passou para o ETSI (European Telecommunications Standards Institute), recém-criado.

O primeiro sistema comercial entrou em operação em 1991, na Finlândia, pela operadora Radiolinja. Em 1992, havia redes

comerciais em vários países europeus. Em 1993, o GSM já tinha mais de 1 milhão de assinantes. Em 1995, ultrapassava 10 milhões. A partir daí, virou um fenômeno global: países da Ásia, África, América Latina e até os Estados Unidos (com o padrão PCS-1900, uma variante do GSM) adotaram o sistema. No auge, o GSM conectava mais de 5 bilhões de pessoas em mais de 200 países — o sistema de telecomunicações mais bem-sucedido da história humana.

2.2.2 A filosofia técnica do GSM

O GSM foi projetado com uma filosofia clara: **eficiência espectral e qualidade de voz em ambientes com alta interferência**. Para isso, adotou três decisões técnicas fundamentais.

A primeira foi a **digitalização da voz com compressão**. Em vez de transmitir a voz analógica diretamente, o GSM digitaliza a voz em amostras de 13 bits a 8 kHz, resultando em 104 kbps. Esse fluxo é então comprimido por um codec chamado RPE-LTP (Regular Pulse Excitation – Long Term Prediction), que reduz a taxa para 13 kbps. O codec é "lossy" — perde informação — mas a perda é projetada para ser imperceptível ao ouvido humano em condições normais. A grande vantagem é que 13 kbps ocupam muito menos espectro que 104 kbps, permitindo mais conversas simultâneas na mesma faixa.

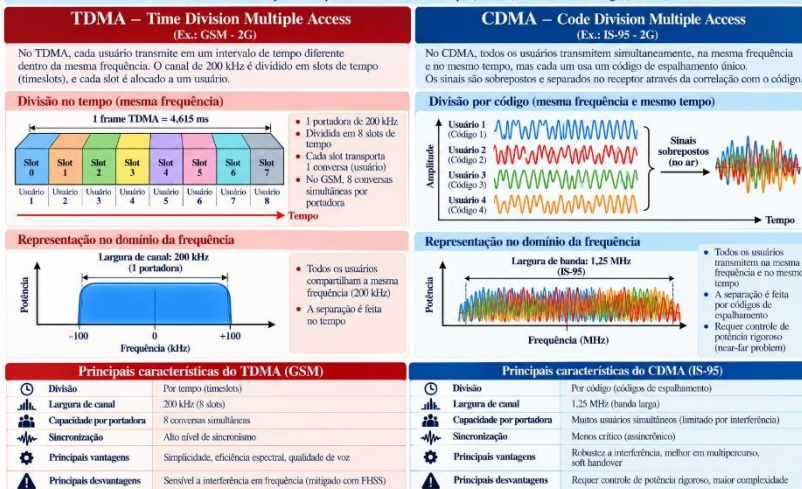
A segunda decisão foi o uso de **TDMA (Time Division Multiple Access)**. Cada portadora de 200 kHz é dividida em 8 slots de tempo (timeslots) de 577 microssegundos cada. Cada slot é

um canal físico que pode ser alocado a um usuário. Assim, uma única portadora de 200 kHz carrega 8 conversas simultâneas — ou seja, 25 kHz por conversa, uma eficiência espectral excelente para a época. A estrutura de frames é hierárquica e sincronizada com precisão de microssegundos, o que exige relógios atômicos nas estações base e algoritmos de sincronização sofisticados nos terminais.

A terceira decisão foi o uso de **FHSS (Frequency Hopping Spread Spectrum)**. A cada frame TDMA (4,615 ms), a portadora salta para uma frequência diferente, seguindo uma sequência pseudo-aleatória conhecida pelo terminal e pela estação base. Isso mitiga interferência seletiva em frequência e desvanecimento por multipercurso. Um sinal que sofre desvanecimento em uma frequência específica será transmitido em outra frequência no próximo frame, e a informação perdida pode ser recuperada por codificação de canal.

Figura 2.2.1 — Comparativo: TDMA (GSM) vs CDMA (IS-95)

Duas filosofias diferentes para múltiplo acesso: divisão do tempo (TDMA) vs divisão do código (CDMA)



2.2.3 A filosofia técnica do IS-95

Enquanto a Europa desenvolvia o GSM, os Estados Unidos seguiam um caminho diferente. A Qualcomm, fundada em 1985 por Irwin Jacobs e Andrew Viterbi, apostou em uma tecnologia radicalmente diferente: **CDMA (Code Division Multiple Access)**.

A ideia do CDMA é contraintuitiva. Em vez de separar os usuários no tempo (TDMA) ou na frequência (FDMA), o CDMA permite que **todos os usuários transmitam simultaneamente na mesma frequência**, separados apenas por códigos ortogonais. Cada usuário recebe um código único — uma sequência pseudo-aleatória de chips — que multiplica seu sinal. No receptor, o mesmo código é aplicado para "desespalhar" o sinal desejado, enquanto os sinais dos outros

usuários (com códigos diferentes) aparecem como ruído de fundo.

O princípio físico é o **espalhamento espectral**. Cada bit de informação é multiplicado por uma sequência de chips, resultando em uma largura de banda muito maior que a original. No IS-95, a largura de banda é de 1,25 MHz — seis vezes maior que os 200 kHz do GSM. O ganho de processamento (a relação entre a largura de banda espalhada e a taxa de informação) permite que o sinal seja recuperado mesmo quando a relação sinal-ruído é negativa.

O IS-95 entrou em operação comercial em 1995, nos Estados Unidos, pela operadora Sprint PCS. Apesar de começar depois do GSM, o CDMA tinha vantagens teóricas significativas: maior capacidade (o chamado "fator de reuso 1", em que todas as células usam a mesma frequência), melhor qualidade de voz em condições de desvanecimento, e transições suaves de handover (soft handover). Em contrapartida, era mais complexo, exigia controle de potência extremamente preciso, e tinha um ecossistema de fornecedores menor.

2.2.4 A batalha GSM vs CDMA

A competição entre GSM e CDMA moldou a indústria móvel nas décadas de 1990 e 2000. O GSM tinha a vantagem do primeiro movimento, do apoio europeu, e de um ecossistema de fornecedores mais amplo (Ericsson, Nokia, Siemens, Alcatel, Motorola). O CDMA tinha a vantagem tecnológica e o apoio da Qualcomm, que licenciava suas patentes e chipsets.

No final dos anos 1990, o GSM dominava a Europa, a Ásia e a África, enquanto o CDMA dominava os Estados Unidos e tinha presença significativa na Coreia do Sul e no Japão. A China adotou o GSM. A Índia adotou ambos. A América Latina dividiu-se entre os dois.

Essa divisão teve consequências profundas. Um usuário GSM não podia usar seu aparelho em uma rede CDMA, e vice-versa. O roaming internacional era limitado. Os fabricantes precisavam produzir aparelhos diferentes para cada mercado. A fragmentação persistiu até a chegada do LTE, que unificou o mundo em torno de uma única tecnologia (OFDMA) e um único padrão (3GPP).

2.2.5 A arquitetura GSM em detalhe: o BSS e o NSS

Para entender o GSM, é preciso entender sua arquitetura em camadas. O sistema é dividido em três grandes blocos: o **MS (Mobile Station)**, o **BSS (Base Station Subsystem)** e o **NSS (Network Subsystem)**.

O **MS** é o terminal do usuário. É composto por duas partes: o **ME (Mobile Equipment)**, que é o aparelho físico, identificado pelo IMEI (International Mobile Equipment Identity); e o **SIM (Subscriber Identity Module)**, que é o cartão inteligente que contém o IMSI (International Mobile Subscriber Identity), a chave de autenticação Ki, e outros dados do assinante. A separação entre ME e SIM foi uma das inovações mais importantes do GSM: permitiu que o usuário trocasse de aparelho sem trocar de número, e vice-versa. O SIM também é

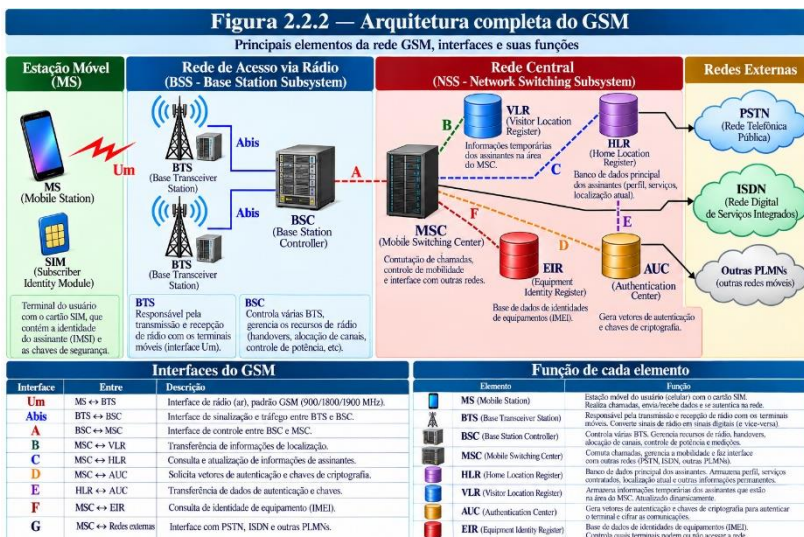
a base da segurança do GSM — a autenticação é feita pelo SIM, que nunca revela a chave Ki.

O **BSS** é a parte da rede que se comunica via rádio com o MS. É composto por dois elementos: a **BTS (Base Transceiver Station)**, que é a estação base propriamente dita, contendo os transceptores, antenas e equipamentos de rádio; e a **BSC (Base Station Controller)**, que é o controlador das BTSs, gerenciando a alocação de canais de rádio, o handover entre BTSs, e a interface com o NSS. Uma BSC tipicamente controla dezenas ou centenas de BTSs.

A interface entre MS e BTS é chamada de **Um** (ou Air Interface). A interface entre BTS e BSC é chamada de **Abis**. A interface entre BSC e MSC é chamada de **A**.

O **NSS** é o núcleo da rede. É composto por vários elementos. O **MSC (Mobile Switching Center)** é o coração do NSS: gerencia as chamadas, o handover entre BSCs, e a interface com outras redes (PSTN, ISDN, outras redes móveis). O **HLR (Home Location Register)** é o banco de dados central dos assinantes: contém o IMSI, o MSISDN (número de telefone), os serviços contratados, e a localização atual do assinante (qual VLR o está servindo). O **VLR (Visitor Location Register)** é um banco de dados temporário que armazena informações sobre os assinantes que estão na área de cobertura de um MSC. O **AUC (Authentication Center)** contém as chaves de autenticação (Ki) e gera os vetores de autenticação (RAND, SRES, Kc). O **EIR (Equipment Identity Register)** é o banco de dados dos IMEIs,

permitindo bloquear aparelhos roubados ou não homologados.



2.2.6 A interface aérea GSM: TDMA, FHSS e canais lógicos

A interface aérea do GSM é um dos sistemas mais complexos já projetados. Ela precisa gerenciar não apenas a voz, mas também a sinalização, a sincronização, o controle de potência, o handover, e a segurança. Para isso, define uma hierarquia de canais lógicos mapeados em canais físicos.

A estrutura física é baseada em **TDMA**. Cada portadora de 200 kHz é dividida em 8 timeslots de 577 microssegundos. Um frame TDMA completo dura 4,615 ms. Vários frames formam multiframe: o multiframe de tráfego tem 26 frames (120 ms), o multiframe de controle tem 51 frames (235,4 ms). Vários

multiframe formam superframes (1.326 frames, 6,12 s), e vários superframes formam hiperframes (2.048 superframes, 3h28min53s760ms). Essa hierarquia é necessária para sincronizar a rede e permitir o frequency hopping.

Os **canais lógicos** são divididos em duas categorias: canais de controle e canais de tráfego.

Os **canais de controle** incluem: o **BCCH (Broadcast Control Channel)**, que transmite informações da célula (identidade, frequências vizinhas, etc.); o **FCCH (Frequency Correction Channel)**, que transmite uma rajada de correção de frequência; o **SCH (Synchronization Channel)**, que transmite informações de sincronização (BSIC, frame number); o **PCH (Paging Channel)**, que transmite mensagens de paginação (chamadas recebidas); o **RACH (Random Access Channel)**, usado pelo MS para solicitar acesso à rede; o **AGCH (Access Grant Channel)**, que transmite a resposta ao RACH; e o **SDCCH (Standalone Dedicated Control Channel)**, usado para sinalização (autenticação, atualização de localização, SMS).

Os **canais de tráfego** incluem: o **TCH/F (Traffic Channel Full rate)**, com 22,8 kbps para voz; o **TCH/H (Traffic Channel Half rate)**, com 11,4 kbps para voz; o **SACCH (Slow Associated Control Channel)**, para sinalização associada ao TCH; e o **FACCH (Fast Associated Control Channel)**, para sinalização rápida (handover).

Cada canal lógico é mapeado em um ou mais timeslots, seguindo uma complexa tabela de alocação. O BCCH, por

exemplo, ocupa o timeslot 0 de uma portadora específica, em todos os frames. O TCH/F ocupa um timeslot dedicado durante a chamada.

2.2.7 O handover no GSM

O handover é o processo de transferir uma chamada de uma célula para outra sem interrupção perceptível. No GSM, o handover é controlado pela BSC (ou pelo MSC, no caso de handover entre BSCs). Existem vários tipos: **intra-BTS** (entre setores da mesma BTS), **inter-BTS intra-BSC** (entre BTSs do mesmo BSC), **inter-BSC intra-MSC** (entre BSCs do mesmo MSC), e **inter-MSC** (entre MSCs diferentes).

O handover é decidido com base em medições feitas pelo MS (nível de sinal da célula servidora e das células vizinhas) e pela BTS (qualidade do sinal recebido). O MS reporta essas medições ao BSC através do SACCH, a uma taxa de aproximadamente duas medições por segundo. O BSC aplica histerese e thresholds para evitar o "efeito ping-pong" (handovers repetidos entre duas células). Quando a decisão é tomada, o BSC aloca recursos na nova célula, transfere o contexto da chamada, e instrui o MS a mudar de frequência e timeslot. O processo leva de 100 a 200 ms, e é imperceptível para o usuário.

2.2.8 Segurança no GSM: autenticação e criptografia

O GSM foi o primeiro sistema móvel a levar segurança a sério. Os mecanismos principais são autenticação, criptografia e uso de identidades temporárias.

A **autenticação** é feita com a chave K_i , armazenada no SIM e no AUC. O processo é o seguinte: a rede envia um número aleatório (RAND) ao MS; o MS calcula $SRES = A_3(K_i, RAND)$ e envia de volta; a rede calcula SRES e compara; se iguais, o MS é autenticado. O algoritmo A_3 é mantido em segredo, mas versões vazaram ao longo dos anos.

A **criptografia** é feita com a chave K_c , derivada de K_i e RAND ($K_c = A_8(K_i, RAND)$). A criptografia é aplicada na interface aérea (algoritmo A_5). Existem várias versões do A_5 ($A_5/1$, $A_5/2$, $A_5/3$), com níveis diferentes de segurança. O $A_5/1$ foi quebrado em 2009; o $A_5/3$ é considerado seguro.

O **TMSI (Temporary Mobile Subscriber Identity)** é usado para proteger a privacidade: em vez de transmitir o IMSI constantemente, a rede atribui um TMSI temporário, que é atualizado periodicamente. O IMSI só é transmitido em situações específicas (primeira autenticação, mudança de VLR, etc.).

2.3 A evolução para 2.5G: GPRS e EDGE

2.3.1 Por que o GSM precisava evoluir

O GSM original era um sistema **circuit-switched**: uma chamada ocupava um canal dedicado durante toda a sua duração. Isso é

eficiente para voz, que é um fluxo contínuo, mas ineficiente para dados, que são naturalmente "bursty" — rajadas de informação separadas por longos períodos de silêncio. Se um usuário quisesse enviar um e-mail de 10 KB, ocuparia um canal inteiro por segundos, desperdiçando recursos. Se quisesse navegar na web, ocuparia um canal intermitentemente, mas a rede não conseguiria compartilhá-lo com outros usuários.

Além disso, o GSM original transmitia dados a 9,6 kbps — uma velocidade ridícula para os padrões do final dos anos 1990. A internet estava explodindo, e o GSM não conseguia acompanhar. Era preciso introduzir a **comutação por pacotes**, que permite que múltiplos usuários compartilhem os mesmos canais de rádio, alocando recursos sob demanda.

2.3.2 GPRS: a primeira rede de dados móvel

O **GPRS (General Packet Radio Service)** foi a resposta.

Introduzido comercialmente a partir de 2000, o GPRS adicionou uma rede de pacotes paralela à rede de circuito do GSM, permitindo acesso à internet em velocidades teóricas de até 114 kbps (na prática, 30-50 kbps).

A arquitetura GPRS adiciona dois novos elementos ao núcleo da rede: o **SGSN (Serving GPRS Support Node)** e o **GGSN (Gateway GPRS Support Node)**. O SGSN é o equivalente do MSC para pacotes: gerencia a mobilidade e a sessão dos usuários de dados. O GGSN é o equivalente do GMSC: faz a interface com redes externas (internet, redes corporativas). A

comunicação entre SGSN e GGSN é feita pela interface **Gn**, usando o protocolo **GTP (GPRS Tunneling Protocol)**.

O GPRS introduziu o conceito de **PDP Context (Packet Data Protocol Context)** — uma sessão de dados entre o MS e o GGSN. Cada PDP Context tem um endereço IP, um APN (Access Point Name), e parâmetros de QoS. Quando o MS quer acessar a internet, ativa um PDP Context; quando termina, desativa. O PDP Context é mantido mesmo durante o handover, permitindo mobilidade contínua.

O GPRS também introduziu **classes de QoS** (conversational, streaming, interactive, background) e **classes de multislot** (o MS pode usar múltiplos timeslots simultaneamente para aumentar a velocidade). Um MS classe 12, por exemplo, pode usar até 4 timeslots no downlink e 4 no uplink, simultaneamente.

2.3.3 EDGE: a evolução do GPRS

O **EDGE (Enhanced Data rates for GSM Evolution)** foi uma evolução do GPRS que introduziu três melhorias fundamentais.

A primeira foi a **modulação 8-PSK**. O GSM original usava GMSK (Gaussian Minimum Shift Keying), que transmite 1 bit por símbolo. O EDGE introduziu 8-PSK (8-Phase Shift Keying), que transmite 3 bits por símbolo, triplicando a taxa de dados por timeslot. A desvantagem é que 8-PSK é mais sensível a ruído e interferência, exigindo condições de canal melhores.

A segunda foi a **codificação adaptativa**. O EDGE define nove esquemas de codificação (MCS-1 a MCS-9), variando de altamente robusto (MCS-1, com muita redundância e baixa taxa) a altamente eficiente (MCS-9, com pouca redundância e alta taxa). O esquema é adaptado dinamicamente às condições do canal: em boas condições, usa MCS-9; em condições ruins, usa MCS-1.

A terceira foi o **Incremental Redundancy**. Em vez de retransmitir pacotes inteiros quando há erro, o EDGE retransmite apenas a redundância adicional, que é combinada com a transmissão original para recuperar a informação. Isso melhora a eficiência em condições de erro.

O EDGE permitiu velocidades teóricas de até 384 kbps, com médias de 100-200 kbps em condições reais. Tornou-se a "rede de fallback" quando o 3G não estava disponível, e ainda hoje é usado em algumas regiões como rede de voz e dados básicos.

2.3.4 O impacto do GPRS e do EDGE

O GPRS e o EDGE transformaram o celular de um telefone em um terminal de dados. Pela primeira vez, era possível navegar na web, enviar e receber e-mails, e usar aplicações de dados móveis — ainda que lentamente. O conceito de "sempre conectado" (always on) nasceu com o GPRS: o PDP Context podia ser mantido ativo indefinidamente, permitindo que aplicações recebessem dados sem intervenção do usuário.

O impacto social foi profundo. O GPRS viabilizou os primeiros serviços de mensagens instantâneas móveis (como o BlackBerry Messenger), os primeiros aplicativos de e-mail push, e os primeiros serviços de localização. O EDGE viabilizou a primeira geração de smartphones (como o Nokia N95 e o iPhone original, que usava EDGE nos primeiros modelos). Sem o GPRS e o EDGE, a revolução dos smartphones não teria acontecido.

2.4 O impacto social da digitalização

A digitalização das comunicações móveis não foi apenas uma mudança técnica — foi uma mudança social profunda, que transformou a forma como as pessoas se comunicam, trabalham, se informam e se relacionam.

2.4.1 O SMS: um fenômeno inesperado

O **SMS (Short Message Service)** foi originalmente concebido como um subproduto do GSM: um canal de sinalização (SDCCH) que podia transportar mensagens curtas de até 160 caracteres. Ninguém previu que se tornaria um fenômeno cultural. A primeira mensagem SMS foi enviada em 1992, por Neil Papworth, engenheiro da Sema Group, para o celular de Richard Jarvis, da Vodafone. Dizia simplesmente "Merry Christmas".

Nos anos 2000, o SMS explodiu. Em 2010, eram enviados mais de 6 trilhões de SMS por ano no mundo. O SMS tornou-se

essencial para tudo: comunicação pessoal, notificações bancárias, marketing, votação em programas de TV, campanhas políticas. Em muitos países em desenvolvimento, o SMS tornou-se a principal forma de comunicação escrita, superando até o e-mail.

O SMS também teve impacto econômico: as operadoras cobravam por mensagem, e o SMS tornou-se uma fonte significativa de receita. Em alguns países, o SMS era mais caro por megabyte do que o envio de dados por satélite — um dos maiores exemplos de precificação arbitrária da história das telecomunicações.

2.4.2 A democratização do acesso

A digitalização tornou o celular acessível a bilhões de pessoas. O GSM, em particular, foi projetado para ser barato e escalável. Os terminais GSM tornaram-se commodities, produzidos em massa por fabricantes como Nokia, Motorola, Siemens e Ericsson. O preço caiu de milhares de dólares nos anos 1980 para dezenas de dólares nos anos 2000.

Em países em desenvolvimento, o celular saltou a etapa do telefone fixo. Em vez de esperar anos por uma linha fixa, as pessoas compravam um celular pré-pago e tinham comunicação imediata. A África, em particular, tornou-se um laboratório de inovação móvel: o M-Pesa, no Quênia, revolucionou os pagamentos móveis; o Ushahidi, também no Quênia, usou SMS para mapear crises; o FrontlineSMS

permitiu que organizações não-governamentais se comunicassem com comunidades remotas.

2.4.3 A base para a revolução dos smartphones

A digitalização foi o alicerce para a revolução dos smartphones. Sem a comutação por pacotes do GPRS e do EDGE, não haveria acesso móvel à internet. Sem o acesso móvel à internet, não haveria aplicativos, redes sociais, streaming, economia de aplicativos. O iPhone, lançado em 2007, usava EDGE nos primeiros modelos — e foi o EDGE que permitiu que ele funcionasse minimamente antes do 3G.

A digitalização também criou a infraestrutura de autenticação e segurança que sustenta os smartphones modernos. O SIM, inventado para o GSM, evoluiu para o USIM do 3G, o ISIM do VoLTE, e o eSIM dos smartphones modernos. A autenticação mútua, a criptografia, e a gestão de identidade — tudo isso nasceu com o GSM.

2.5 Conclusão: a digitalização como ponto de inflexão

A transição do analógico para o digital foi o ponto de inflexão na história das comunicações móveis. Ela transformou o celular de um luxo para poucos em um serviço universal; de um telefone em um terminal de dados; de um sistema fragmentado em um padrão global. O GSM e o IS-95 foram os pioneiros, mas o legado vai muito além: a digitalização criou os

conceitos, as arquiteturas e os protocolos que sustentam todas as gerações subsequentes.

O 3G, o 4G e o 5G não seriam possíveis sem a base estabelecida pelo 2G. O SIM, o HLR, o VLR, o handover, a autenticação, a criptografia, a comutação por pacotes — todos nasceram ou foram consolidados na era 2G. Entender o 2G é entender a fundação sobre a qual o mundo móvel moderno foi construído.

Capítulo 3. 2G: GSM, GPRS e EDGE

3.1 A arquitetura GSM: uma visão detalhada

O GSM é, provavelmente, o sistema de telecomunicações mais bem-sucedido da história. Em seu auge, conectava mais de 5 bilhões de pessoas em mais de 200 países. Sua arquitetura introduziu conceitos que sobrevivem até hoje, e entendê-la é fundamental para compreender todas as gerações subsequentes.

A arquitetura GSM é dividida em três grandes blocos: **MS (Mobile Station)**, **BSS (Base Station Subsystem)** e **NSS (Network Subsystem)**. Cada bloco tem funções específicas e interfaces padronizadas, permitindo interoperabilidade entre equipamentos de diferentes fabricantes.

3.1.1 O Mobile Station (MS)

O MS é o terminal do usuário. É composto por duas partes distintas, mas inseparáveis na operação:

O **ME (Mobile Equipment)** é o aparelho físico, identificado pelo IMEI (International Mobile Equipment Identity), um número único de 15 dígitos que identifica o dispositivo. O IMEI é composto por: TAC (Type Allocation Code, 8 dígitos, identificando o modelo), FAC (Final Assembly Code, 2 dígitos, identificando o fabricante), SNR (Serial Number, 6 dígitos), e CD (Check Digit, 1 dígito). O IMEI é usado pelo EIR para bloquear aparelhos roubados ou não homologados.

O **SIM (Subscriber Identity Module)** é o cartão inteligente que contém o IMSI (International Mobile Subscriber Identity), a chave de autenticação Ki, e outros dados do assinante. O IMSI é composto por: MCC (Mobile Country Code, 3 dígitos, identificando o país), MNC (Mobile Network Code, 2 ou 3 dígitos, identificando a operadora), MSIN (Mobile Subscriber Identification Number, 9 ou 10 dígitos, identificando o assinante). O IMSI é armazenado no SIM e no HLR, e é usado para autenticação e roteamento.

O SIM também contém: a chave Ki (128 bits, usada para autenticação), os algoritmos A3 e A8 (implementados no chip), o PIN (Personal Identification Number, usado para desbloquear o SIM), o PUK (PIN Unblocking Key, usado para desbloquear o PIN), e espaço de armazenamento para contatos e SMS.

A separação entre ME e SIM foi uma das inovações mais importantes do GSM. Permitiu que o usuário trocasse de

aparelho sem trocar de número (bastava mover o SIM), e vice-versa (bastava inserir outro SIM). Também permitiu que as operadoras vendessem aparelhos subsidiados, com o SIM bloqueado à rede — um modelo de negócio que dominou a indústria por décadas.

3.1.2 O Base Station Subsystem (BSS)

O BSS é a parte da rede que se comunica via rádio com o MS. É composto por dois elementos:

A **BTS (Base Transceiver Station)** é a estação base propriamente dita. Contém os transceptores, antenas, e equipamentos de rádio. Uma BTS pode ter múltiplos setores (tipicamente 3, cobrindo 120° cada) e múltiplas portadoras por setor (tipicamente 1 a 4, dependendo da capacidade). Cada portadora é um canal de 200 kHz, dividido em 8 timeslots TDMA. A BTS é responsável pela camada física: modulação, demodulação, codificação de canal, e controle de potência.

O **BSC (Base Station Controller)** é o controlador das BTSs. Gerencia a alocação de canais de rádio, o handover entre BTSs, e a interface com o NSS. Uma BSC tipicamente controla dezenas ou centenas de BTSs, cobrindo uma área metropolitana ou uma região. O BSC é responsável pela camada de enlace: gerenciamento de recursos de rádio, controle de handover, e concentração de tráfego.

A interface entre MS e BTS é chamada de **Um** (ou Air Interface). A interface entre BTS e BSC é chamada de **Abis**. A

interface entre BSC e MSC é chamada de **A**. Cada interface tem protocolos específicos e requisitos de desempenho.

3.1.3 O Network Subsystem (NSS)

O NSS é o núcleo da rede GSM. É composto por vários elementos:

O **MSC (Mobile Switching Center)** é o coração do NSS. Gerencia as chamadas, o handover entre BSCs, e a interface com outras redes (PSTN, ISDN, outras redes móveis). O MSC também gerencia os serviços suplementares (chamada em espera, conferência, etc.). Um MSC tipicamente controla dezenas de BSCs, cobrindo uma região ou um país.

O **HLR (Home Location Register)** é o banco de dados central dos assinantes. Contém o IMSI, o MSISDN (número de telefone), os serviços contratados, e a localização atual do assinante (qual VLR o está servindo). O HLR é consultado em toda chamada recebida, para rotear a chamada ao MSC correto.

O **VLR (Visitor Location Register)** é um banco de dados temporário que armazena informações sobre os assinantes que estão na área de cobertura de um MSC. Quando um assinante entra em uma nova área, o VLR consulta o HLR para obter os dados e autenticar o assinante. O VLR também armazena o TMSI (Temporary Mobile Subscriber Identity), que é usado para proteger a privacidade.

O **AUC (Authentication Center)** contém as chaves de autenticação (Ki) dos assinantes. Gera os vetores de autenticação (RAND, SRES, Kc) usados no processo de autenticação. O AUC é fisicamente integrado ao HLR na maioria das implementações.

O **EIR (Equipment Identity Register)** é o banco de dados dos IMEIs. Permite bloquear aparelhos roubados ou não homologados. O EIR tem três listas: a lista branca (aparelhos permitidos), a lista cinza (aparelhos monitorados), e a lista negra (aparelhos bloqueados).

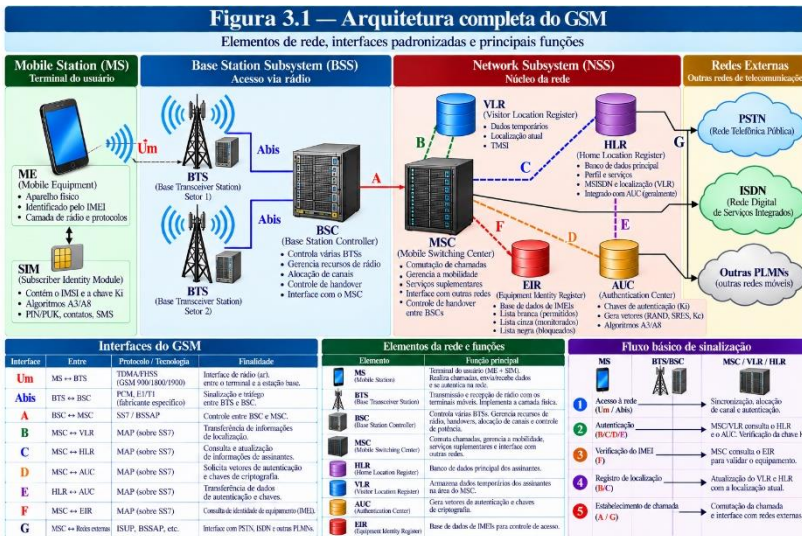
3.1.4 Interfaces e protocolos

As interfaces do GSM são padronizadas pelo 3GPP, permitindo interoperabilidade entre equipamentos de diferentes fabricantes. As principais interfaces são:

A interface **Um** (Air Interface) entre MS e BTS, baseada em TDMA/FHSS. A interface **Abis** entre BTS e BSC, baseada em PCM (Pulse Code Modulation) e protocolos proprietários (na prática, cada fabricante tem sua própria variante). A interface **A** entre BSC e MSC, baseada em SS7 (Signaling System No. 7) e protocolo BSSAP (Base Station Subsystem Application Part).

A interface **B** entre MSC e VLR, usada para consultas de localização. A interface **C** entre MSC e HLR, usada para consultas de roteamento. A interface **D** entre HLR e VLR, usada para atualização de localização. A interface **E** entre MSCs, usada para handover inter-MSC. A interface **F** entre MSC e EIR,

usada para verificação de IMEI. A interface **G** entre VLRs, usada para troca de informações.



3.2 A interface aérea GSM: TDMA e FHSS

A interface aérea do GSM é um dos sistemas mais complexos já projetados. Ela precisa gerenciar não apenas a voz, mas também a sinalização, a sincronização, o controle de potência, o handover, e a segurança. Para isso, define uma hierarquia de canais lógicos mapeados em canais físicos.

A estrutura física é baseada em **TDMA**. Cada portadora de 200 kHz é dividida em 8 timeslots de 577 microssegundos. Um frame TDMA completo dura 4,615 ms. Vários frames formam multiframe: o multiframe de tráfego tem 26 frames (120 ms), o multiframe de controle tem 51 frames (235,4 ms). Vários multiframe formam superframes (1.326 frames, 6,12 s), e

vários superframes formam hiperframes (2.048 superframes, 3h28min53s760ms). Essa hierarquia é necessária para sincronizar a rede e permitir o frequency hopping.

O **FHSS (Frequency Hopping Spread Spectrum)** é usado para mitigar interferência e desvanecimento. A cada frame TDMA (4,615 ms), a portadora salta para uma frequência diferente, seguindo uma sequência pseudo-aleatória conhecida pelo MS e pela BTS. A sequência é gerada por um algoritmo que usa o frame number e o BSIC (Base Station Identity Code) como entrada. O FHSS melhora a qualidade em ambientes com interferência seletiva em frequência: um sinal que sofre desvanecimento em uma frequência específica será transmitido em outra frequência no próximo frame, e a informação perdida pode ser recuperada por codificação de canal.

O FHSS também melhora a segurança: um interceptador que não conhece a sequência de hopping não consegue seguir a transmissão. No entanto, o FHSS não é uma forma de criptografia — é uma técnica de espalhamento espectral, e pode ser quebrado com equipamento adequado.

3.3 Canais lógicos e físicos

O GSM define uma variedade de canais lógicos, mapeados em canais físicos (timeslots). Os canais lógicos são divididos em duas categorias: canais de controle e canais de tráfego.

Os **canais de controle** incluem:

O **BCCH (Broadcast Control Channel)** transmite informações da célula: identidade da célula (Cell Identity), identidade da área de localização (LAI), frequências vizinhas, e parâmetros de controle. O BCCH é transmitido continuamente, em todos os frames, no timeslot 0 de uma portadora específica.

O **FCCH (Frequency Correction Channel)** transmite uma rajada de correção de frequência, permitindo que o MS sincronize sua frequência com a da BTS. O FCCH é transmitido periodicamente, no mesmo timeslot do BCCH.

O **SCH (Synchronization Channel)** transmite informações de sincronização: o BSIC (Base Station Identity Code) e o frame number. O SCH permite que o MS sincronize seu timing com o da BTS.

O **PCH (Paging Channel)** transmite mensagens de paginação, usadas para notificar o MS de uma chamada recebida. O PCH é transmitido em subcanais, e o MS monitora apenas o seu subcanal (paging group), economizando bateria.

O **RACH (Random Access Channel)** é usado pelo MS para solicitar acesso à rede. O MS transmite uma rajada curta, e a BTS responde com um AGCH.

O **AGCH (Access Grant Channel)** transmite a resposta ao RACH, alocando um SDCCH ou TCH ao MS.

O **SDCCH (Standalone Dedicated Control Channel)** é usado para sinalização: autenticação, atualização de localização, estabelecimento de chamada, SMS.

Os **canais de tráfego** incluem:

O **TCH/F (Traffic Channel Full rate)** é o canal de voz principal, com 22,8 kbps. O **TCH/H (Traffic Channel Half rate)** é uma versão de metade da taxa, com 11,4 kbps, permitindo duas conversas por timeslot.

O **SACCH (Slow Associated Control Channel)** é usado para sinalização associada ao TCH: medições de sinal, controle de potência, timing advance.

O **FACCH (Fast Associated Control Channel)** é usado para sinalização rápida, como handover. O FACCH "rouba" bits do TCH, substituindo temporariamente a voz por sinalização.

3.4 O handover no GSM

O handover é o processo de transferir uma chamada de uma célula para outra sem interrupção perceptível. No GSM, o handover é controlado pela BSC (ou pelo MSC, no caso de handover entre BSCs). Existem vários tipos: **intra-BTS** (entre setores da mesma BTS), **inter-BTS intra-BSC** (entre BTSs do mesmo BSC), **inter-BSC intra-MSC** (entre BSCs do mesmo MSC), e **inter-MSC** (entre MSCs diferentes).

O handover é decidido com base em medições feitas pelo MS (nível de sinal da célula servidora e das células vizinhas) e pela BTS (qualidade do sinal recebido). O MS reporta essas medições ao BSC através do SACCH, a uma taxa de aproximadamente duas medições por segundo. O BSC aplica

histerese e thresholds para evitar o "efeito ping-pong" (handovers repetidos entre duas células).

Quando a decisão é tomada, o BSC aloca recursos na nova célula, transfere o contexto da chamada, e instrui o MS a mudar de frequência e timeslot. O processo leva de 100 a 200 ms, e é imperceptível para o usuário. Em caso de falha, o MS retorna à célula original (handover fallback).

3.5 Segurança no GSM: autenticação e criptografia

O GSM foi o primeiro sistema móvel a levar segurança a sério. Os mecanismos principais são autenticação, criptografia e uso de identidades temporárias.

A **autenticação** é feita com a chave K_i , armazenada no SIM e no AUC. O processo é o seguinte: a rede envia um número aleatório (RAND) ao MS; o MS calcula $SRES = A3(K_i, RAND)$ e envia de volta; a rede calcula SRES e compara; se iguais, o MS é autenticado. O algoritmo A3 é mantido em segredo, mas versões vazaram ao longo dos anos.

A **criptografia** é feita com a chave K_c , derivada de K_i e RAND ($K_c = A8(K_i, RAND)$). A criptografia é aplicada na interface aérea (algoritmo A5). Existem várias versões do A5 (A5/1, A5/2, A5/3), com níveis diferentes de segurança. O A5/1 foi quebrado em 2009; o A5/3 é considerado seguro.

O **TMSI (Temporary Mobile Subscriber Identity)** é usado para proteger a privacidade: em vez de transmitir o IMSI constantemente, a rede atribui um TMSI temporário, que é

atualizado periodicamente. O IMSI só é transmitido em situações específicas (primeira autenticação, mudança de VLR, etc.).

3.6 GPRS: a introdução da comutação por pacotes

O GPRS (General Packet Radio Service) foi a primeira evolução significativa do GSM. Introduziu a comutação por pacotes, permitindo acesso à internet em velocidades de até 114 kbps (teóricas).

A arquitetura GPRS adiciona dois novos elementos:

O **SGSN (Serving GPRS Support Node)** gerencia a mobilidade e a sessão dos usuários de dados. É o equivalente do MSC para pacotes. O SGSN autentica o usuário, gerencia o PDP Context, e roteia os pacotes para o GGSN.

O **GGSN (Gateway GPRS Support Node)** faz a interface com redes externas (internet, redes corporativas). É o equivalente do GMSC para pacotes. O GGSN aloca endereços IP, aplica políticas de QoS, e coleta dados de tarifação.

O GPRS introduziu o conceito de **PDP Context** (Packet Data Protocol Context) — uma sessão de dados entre o MS e o GGSN. Cada PDP Context tem um endereço IP, um APN (Access Point Name), e parâmetros de QoS. Quando o MS quer acessar a internet, ativa um PDP Context; quando termina, desativa. O PDP Context é mantido mesmo durante o handover, permitindo mobilidade contínua.

O GPRS também introduziu **classes de QoS** (conversational, streaming, interactive, background) e **classes de multislot** (o MS pode usar múltiplos timeslots simultaneamente para aumentar a velocidade). Um MS classe 12, por exemplo, pode usar até 4 timeslots no downlink e 4 no uplink, simultaneamente.

3.7 EDGE: a evolução do GPRS

O EDGE (Enhanced Data rates for GSM Evolution) foi uma evolução do GPRS que introduziu três melhorias fundamentais.

A primeira foi a **modulação 8-PSK**. O GSM original usava GMSK (Gaussian Minimum Shift Keying), que transmite 1 bit por símbolo. O EDGE introduziu 8-PSK (8-Phase Shift Keying), que transmite 3 bits por símbolo, triplicando a taxa de dados por timeslot. A desvantagem é que 8-PSK é mais sensível a ruído e interferência, exigindo condições de canal melhores.

A segunda foi a **codificação adaptativa**. O EDGE define nove esquemas de codificação (MCS-1 a MCS-9), variando de altamente robusto (MCS-1, com muita redundância e baixa taxa) a altamente eficiente (MCS-9, com pouca redundância e alta taxa). O esquema é adaptado dinamicamente às condições do canal: em boas condições, usa MCS-9; em condições ruins, usa MCS-1.

A terceira foi o **Incremental Redundancy**. Em vez de retransmitir pacotes inteiros quando há erro, o EDGE

retransmite apenas a redundância adicional, que é combinada com a transmissão original para recuperar a informação. Isso melhora a eficiência em condições de erro.

O EDGE permitiu velocidades teóricas de até 384 kbps, com médias de 100-200 kbps em condições reais. Tornou-se a "rede de fallback" quando o 3G não estava disponível, e ainda hoje é usado em algumas regiões como rede de voz e dados básicos.

3.8 O legado do GSM

O GSM deixou um legado profundo:

- **Padronização global:** pela primeira vez, um sistema móvel funcionava em múltiplos países.
- **SIM:** o conceito de identidade separada do equipamento.
- **Roaming:** a capacidade de usar o celular em redes de outras operadoras.
- **SMS:** um serviço que ninguém previu, mas que se tornou essencial.
- **Segurança:** autenticação e criptografia desde o início.
- **Arquitetura:** BTS, BSC, MSC, HLR, VLR — conceitos que evoluíram para eNodeB, RNC, MME, HSS.

O GSM foi desligado em muitos países a partir de 2017 (Austrália foi o primeiro), mas ainda opera em algumas regiões. Seu legado, porém, é eterno.

Capítulo 4. 3G: UMTS, WCDMA e HSPA

4.1 A necessidade de banda larga móvel

No final dos anos 1990, a internet estava explodindo. O GSM, com suas velocidades de 9,6 kbps (ou 114 kbps com GPRS), era claramente insuficiente para acesso à web. A ITU (União Internacional de Telecomunicações) lançou o programa IMT-2000 (International Mobile Telecommunications-2000), definindo requisitos para a terceira geração: velocidades de pelo menos 144 kbps em ambientes móveis, 384 kbps em ambientes pedestres, e 2 Mbps em ambientes fixos.

O 3GPP (3rd Generation Partnership Project) foi formado em 1998 para desenvolver o padrão 3G baseado no GSM. O resultado foi o UMTS (Universal Mobile Telecommunications System), com WCDMA (Wideband Code Division Multiple Access) como tecnologia de acesso.

4.2 WCDMA: a revolução do código

O WCDMA é uma tecnologia de acesso baseada em **CDMA (Code Division Multiple Access)**. Em vez de dividir o tempo (TDMA) ou a frequência (FDMA), o WCDMA divide o código: todos os usuários transmitem simultaneamente na mesma

frequência (5 MHz), separados por códigos ortogonais (códigos de Walsh).

O princípio é o **espalhamento espectral**: cada bit de informação é multiplicado por uma sequência de chips (código de espalhamento), resultando em uma largura de banda muito maior que a original. O receptor, conhecendo o código, pode "desespalhar" o sinal e recuperar a informação. Sinais de outros usuários (com códigos diferentes) aparecem como ruído de fundo.

O WCDMA tem características únicas:

- **Largura de banda de 5 MHz**: muito maior que os 200 kHz do GSM.
- **Controle de potência rápido**: 1500 vezes por segundo (1,5 kHz), essencial para mitigar o problema near-far (usuários próximos à BTS "abafam" os distantes).
- **Soft handover**: o MS pode se comunicar com múltiplas BTSs simultaneamente durante o handover, garantindo transição suave.
- **Macrodiversidade**: o sinal de múltiplas BTSs é combinado no receptor, melhorando a qualidade.
- **Codecs AMR (Adaptive Multi-Rate)**: a taxa de codificação de voz é adaptada às condições do canal.

4.3 Arquitetura UMTS

A arquitetura UMTS é uma evolução da arquitetura GSM, com novos elementos:

- **UE (User Equipment):** o terminal do usuário (equivalente ao MS).
- **NodeB:** a estação base (equivalente à BTS).
- **RNC (Radio Network Controller):** o controlador das NodeBs (equivalente ao BSC).
- **CS Core:** o domínio de comutação de circuito (voz), herdado do GSM (MSC, GMSC, VLR).
- **PS Core:** o domínio de comutação de pacotes (dados), evoluído do GPRS (SGSN, GGSN).
- **HLR/AUC:** os bancos de dados de assinantes.

4.4 A interface aérea WCDMA

A interface aérea WCDMA (Uu) é baseada em:

- **Modulação QPSK** (downlink) e **HPSK** (uplink).
- **Espalhamento espectral** com fator de espalhamento (SF) variável.
- **Controle de potência** rápido (1500 Hz).
- **Soft handover** e **softer handover**.

4.4 A interface aérea WCDMA

A interface aérea do WCDMA, chamada de **Uu**, é um dos sistemas de rádio mais complexos já padronizados. Ela precisa gerenciar voz e dados simultaneamente, múltiplos usuários compartilhando a mesma frequência, controle de potência extremamente rápido, e mobilidade contínua. Entender seus fundamentos é essencial para compreender por que o 3G funcionou — e por que, mais tarde, foi substituído pelo LTE.

4.4.1 O princípio do espalhamento espectral

No centro do WCDMA está o conceito de **espalhamento espectral** (spread spectrum). A ideia é contraintuitiva: em vez de transmitir um sinal de banda estreita, como faz o GSM (200 kHz por portadora), o WCDMA transmite um sinal de banda larga (5 MHz) para cada usuário. À primeira vista, isso parece um desperdício de espectro. Mas não é.

O espalhamento funciona assim: cada bit de informação é multiplicado por uma sequência de **chips** — uma sequência pseudo-aleatória de pulsos muito mais rápidos que a taxa de bits. Se a taxa de bits é de 12,2 kbps (voz AMR) e a taxa de chips é de 3,84 Mcps (megachips por segundo), o **fator de espalhamento** (SF) é $3.840.000 / 12.200 \approx 384$. Cada bit é representado por 384 chips.

No receptor, o mesmo código é aplicado. O resultado é que o sinal desejado é "comprimido" de volta à sua banda original, enquanto os sinais de outros usuários (com códigos diferentes) permanecem espalhados e aparecem como ruído de fundo. Esse é o princípio do **ganho de processamento**: mesmo que a

relação sinal-ruído seja negativa (o sinal é mais fraco que o ruído), o receptor consegue recuperar a informação porque conhece o código.

O WCDMA usa dois tipos de códigos: os **códigos de canalização** (códigos de Walsh), que separam os usuários dentro de uma mesma célula, e os **códigos de embaralhamento** (scrambling codes), que separam as células entre si. Os códigos de Walsh são ortogonais entre si, o que significa que, em condições ideais, não há interferência entre usuários da mesma célula. Os códigos de embaralhamento são sequências pseudo-aleatórias (Gold codes), com baixa correlação cruzada, que permitem que o receptor distinga o sinal de uma célula do sinal de outra.

4.4.2 O problema near-far e o controle de potência

Um dos maiores desafios do WCDMA é o **problema near-far**. Imagine dois usuários: um está a 100 metros da estação base, outro a 1 quilômetro. O sinal do primeiro chega à base com potência muito maior que o do segundo. Como todos compartilham a mesma frequência, o sinal forte do primeiro "abafa" o sinal fraco do segundo — a menos que algo seja feito.

A solução é o **controle de potência rápido**. A estação base mede a potência recebida de cada usuário e envia comandos de controle (TPC — Transmit Power Control) 1.500 vezes por segundo (a cada slot de 0,667 ms). O usuário ajusta sua potência em passos de 1 dB, para cima ou para baixo,

conforme o comando. O objetivo é que todos os sinais cheguem à base com a mesma potência, independentemente da distância.

Esse controle é complementado pelo **controle de potência de laço externo** (outer loop), que ajusta a relação sinal-interferência (SIR) alvo com base na taxa de erro de bloco (BLER). Se a BLER está alta, o SIR alvo é aumentado; se está baixa, é reduzido. Isso garante que cada usuário receba a qualidade necessária com o mínimo de potência.

O controle de potência é, talvez, o aspecto mais crítico do WCDMA. Sem ele, a capacidade da rede colapsa. Com ele, a rede consegue acomodar dezenas de usuários por célula simultaneamente.

4.4.3 Soft handover e macrodiversidade

No GSM, o handover é "hard": o terminal corta a conexão com a célula antiga antes de estabelecer com a nova. Isso pode causar interrupções perceptíveis. No WCDMA, o handover é "soft": o terminal se conecta à nova célula antes de cortar a antiga. Durante a transição, o terminal se comunica com duas ou mais células simultaneamente.

Esse processo é chamado de **macrodiversidade**. O terminal envia o mesmo sinal para múltiplas células, e o RNC combina os sinais recebidos, escolhendo o melhor em cada instante (ou combinando-os). Isso melhora a qualidade e reduz a probabilidade de queda de chamada. O preço é o aumento do

consumo de recursos de rádio: durante o soft handover, o terminal ocupa canais em duas células ao mesmo tempo.

Existe também o **softer handover**, que ocorre entre setores da mesma estação base. Nesse caso, a combinação é feita na própria NodeB, sem envolver o RNC.

4.4.4 Estrutura de frames e canais

A interface aérea WCDMA é organizada em frames de 10 ms, divididos em 15 slots de 0,667 ms. Cada slot contém 2.560 chips. A estrutura é sincronizada com o **chip rate** de 3,84 Mcps, que é o "coração" da interface aérea.

Os canais lógicos do WCDMA são divididos em:

- **Canais de transporte:** definem como os dados são transmitidos pela interface aérea. Incluem o DCH (Dedicated Channel), o RACH (Random Access Channel), o FACH (Forward Access Channel), o HS-DSCH (High-Speed Downlink Shared Channel), e o E-DCH (Enhanced Dedicated Channel).
- **Canais físicos:** definem a modulação e o espalhamento. Incluem o DPCH (Dedicated Physical Channel), o P-CCPCH (Primary Common Control Physical Channel), o S-CCPCH (Secondary Common Control Physical Channel), o HS-PDSCH (High-Speed Physical Downlink Shared Channel), e o E-DPDCH (E-DCH Dedicated Physical Data Channel).

A relação entre canais de transporte e canais físicos é definida pelo **mapeamento**. Por exemplo, o DCH é mapeado no DPCH; o HS-DSCH é mapeado no HS-PDSCH.

4.4.5 HSPA: a evolução do 3G

O WCDMA original (Release 99) oferecia velocidades de até 384 kbps no downlink e 128 kbps no uplink — insuficientes para competir com o ADSL. O **HSPA (High-Speed Packet Access)** foi a resposta, introduzindo dois canais compartilhados de alta velocidade:

O **HSDPA (High-Speed Downlink Packet Access)**, introduzido no Release 5 (2005), adicionou o HS-DSCH, um canal compartilhado que aloca recursos dinamicamente entre os usuários. O HSDPA introduziu três inovações: **modulação adaptativa** (QPSK e 16-QAM), **codificação adaptativa** (taxas variáveis), e **HARQ (Hybrid Automatic Repeat Request)** — retransmissão rápida com combinação de pacotes. O HSDPA permitiu velocidades de até 14,4 Mbps (teóricas), com médias de 2-5 Mbps.

O **HSUPA (High-Speed Uplink Packet Access)**, introduzido no Release 6 (2007), adicionou o E-DCH, um canal dedicado de alta velocidade no uplink. O HSUPA permitiu velocidades de até 5,76 Mbps (teóricas), com médias de 1-3 Mbps.

A combinação de HSDPA e HSUPA é chamada de **HSPA**. O **HSPA+** (Release 7 e posteriores) adicionou MIMO (Multiple Input Multiple Output), modulação 64-QAM, e agregação de

portadoras, permitindo velocidades de até 42 Mbps (dual-carrier) e, mais tarde, 84 Mbps (triple-carrier) e 168 Mbps (quad-carrier).

[IMAGEM 4.1 — Arquitetura completa do UMTS/HSPA: UE, NodeB, RNC, CS Core, PS Core, HLR. Interfaces Uu, Iub, Iur, Iu-CS, Iu-PS. Diagrama detalhado com legenda explicando a função de cada elemento e a evolução para HSPA.]

4.5 A arquitetura UMTS em detalhe

A arquitetura UMTS é uma evolução da arquitetura GSM, com novos elementos e interfaces. Ela é dividida em três grandes blocos: o **UE (User Equipment)**, a **UTRAN (UMTS Terrestrial Radio Access Network)**, e o **CN (Core Network)**.

O **UE** é o terminal do usuário, composto pelo ME (Mobile Equipment) e pelo USIM (Universal Subscriber Identity Module). O USIM é uma evolução do SIM, com maior capacidade de armazenamento e suporte a novos serviços.

A **UTRAN** é a rede de acesso, composta por NodeBs e RNCs. A NodeB é a estação base, responsável pela camada física (modulação, demodulação, espalhamento, desespalhamento, controle de potência). O RNC é o controlador, responsável pela camada de enlace (gerenciamento de recursos de rádio, controle de handover, concentração de tráfego). A interface entre UE e NodeB é a **Uu**; entre NodeB e RNC é a **Iub**; entre RNCs é a **Iur**; entre RNC e CN é a **Iu**.

O **CN** é dividido em dois domínios: o **CS Core** (Circuit Switched), que gerencia voz e serviços de circuito, herdado do GSM (MSC, GMSC, VLR); e o **PS Core** (Packet Switched), que gerencia dados e serviços de pacote, evoluído do GPRS (SGSN, GGSN). O HLR e o AUC são compartilhados entre os dois domínios.

A grande inovação arquitetural do UMTS é a separação entre **controle** e **usuário**. O RNC tem funções de controle (RRC — Radio Resource Control) e de usuário (PDCP, RLC, MAC). Essa separação foi aprofundada no LTE e no 5G, com a introdução do conceito de **CU/DU split** (Central Unit / Distributed Unit).

4.6 O legado do 3G

O 3G deixou um legado profundo:

- **Banda larga móvel:** pela primeira vez, a internet móvel era viável.
- **Vídeo chamada:** um serviço que nunca decolou, mas que provou a viabilidade de serviços multimídia.
- **CDMA:** uma tecnologia que dominou o 3G e influenciou o 4G e o 5G.
- **Soft handover:** uma técnica que melhorou a qualidade e a confiabilidade.
- **HSPA:** uma evolução que manteve o 3G competitivo por mais de uma década.

- **Arquitetura:** NodeB, RNC, CS Core, PS Core — conceitos que evoluíram para eNodeB, MME, SGW, PGW.

O 3G foi desligado em muitos países a partir de 2020, mas ainda opera em algumas regiões. Seu legado, porém, é eterno.

Capítulo 5. 4G: LTE e LTE-Advanced

5.1 A necessidade de uma nova arquitetura

No final dos anos 2000, o 3G começava a mostrar suas limitações. O WCDMA, com sua largura de banda de 5 MHz e sua arquitetura complexa (NodeB, RNC, CS Core, PS Core), não conseguia escalar para atender à demanda crescente por dados. Os smartphones estavam explodindo, e a rede não aguentava. Era preciso uma nova arquitetura, mais simples, mais eficiente, e mais escalável.

O 3GPP lançou o projeto **LTE (Long Term Evolution)** em 2004, com objetivos ambiciosos: latência de 10 ms, velocidades de 100 Mbps no downlink e 50 Mbps no uplink, eficiência espectral três vezes maior que o HSPA, e arquitetura totalmente IP. O primeiro padrão foi congelado no Release 8 (2008), e as primeiras redes comerciais entraram em operação em 2009 (Estocolmo e Oslo, pela TeliaSonera).

5.2 A revolução do OFDMA

A grande inovação do LTE é o **OFDMA (Orthogonal Frequency Division Multiple Access)**. Em vez de transmitir em uma única portadora de banda larga, o OFDMA divide a banda em centenas ou milhares de subportadoras de banda estreita (15 kHz cada), ortogonais entre si. Cada subportadora é modulada independentemente, e os recursos são alocados em blocos de 180 kHz (12 subportadoras) por 0,5 ms (1 slot).

O OFDMA tem várias vantagens:

- **Robustez contra multipercurso:** como cada subportadora é de banda estreita, o desvanecimento seletivo em frequência afeta apenas algumas subportadoras, e a codificação de canal pode recuperar a informação perdida.
- **Flexibilidade de alocação:** os recursos podem ser alocados dinamicamente, subportadora por subportadora, slot por slot, permitindo adaptação às condições do canal e às necessidades dos usuários.
- **Eficiência espectral:** o OFDMA é muito mais eficiente que o CDMA, especialmente em canais com alta relação sinal-ruído.
- **Escalabilidade:** a largura de banda pode variar de 1,4 MHz a 20 MHz (e mais, com agregação de portadoras).

No uplink, o LTE usa **SC-FDMA (Single-Carrier Frequency Division Multiple Access)**, uma variante do OFDMA que reduz

a relação pico-média de potência (PAPR), economizando bateria do terminal.

5.3 A arquitetura EPC

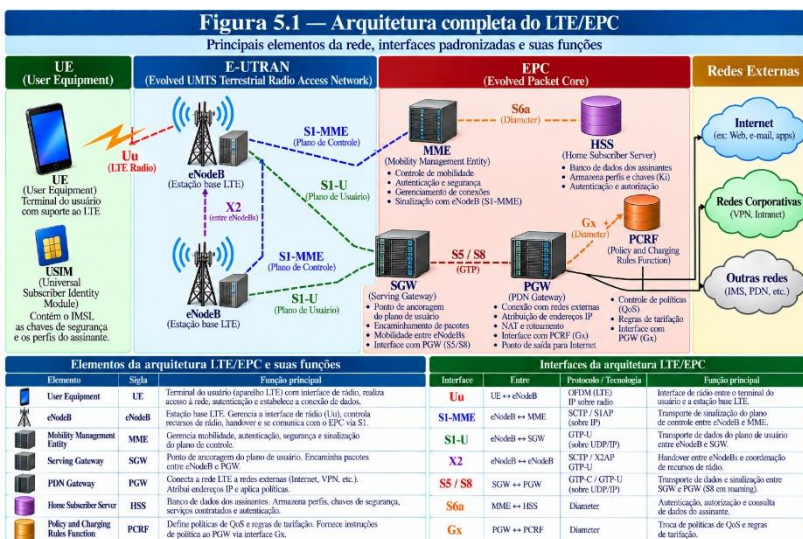
O LTE introduziu uma arquitetura totalmente nova, chamada **EPC (Evolved Packet Core)**. A grande mudança é a eliminação do RNC: o eNodeB se conecta diretamente ao core, simplificando a rede e reduzindo a latência.

Os principais elementos do EPC são:

- **eNodeB (evolved NodeB)**: a estação base, responsável pela camada física, pela camada de enlace, e por funções de controle de rádio (RRC). O eNodeB também faz a gestão de recursos de rádio (RRM), o controle de handover, e a compressão de cabeçalhos (ROHC).
- **MME (Mobility Management Entity)**: o elemento de controle, responsável pela autenticação, pela gestão de localização, pela gestão de portadoras, e pela sinalização NAS (Non-Access Stratum).
- **SGW (Serving Gateway)**: o elemento de usuário, responsável pelo roteamento de pacotes, pela ancoragem de mobilidade, e pela coleta de dados de tarifação.
- **PGW (Packet Data Network Gateway)**: o elemento de interconexão, responsável pela alocação de endereços IP, pela aplicação de políticas de QoS, e pela interface com redes externas (internet, IMS, redes corporativas).

- **HSS (Home Subscriber Server):** o banco de dados de assinantes, evolução do HLR/AUC.
- **PCRF (Policy and Charging Rules Function):** o elemento de políticas, responsável pela definição de regras de QoS e tarifação.

A interface entre eNodeB e MME é a **S1-MME**; entre eNodeB e SGW é a **S1-U**; entre eNodeBs é a **X2**; entre MME e HSS é a **S6a**; entre SGW e PGW é a **S5/S8**.



5.4 A interface aérea LTE

A interface aérea do LTE é baseada em OFDMA (downlink) e SC-FDMA (uplink). A estrutura de frames é hierárquica:

- **Frame de rádio:** 10 ms, dividido em 10 subframes de 1 ms.

- **Subframe:** dividido em 2 slots de 0,5 ms.
- **Slot:** dividido em 7 símbolos OFDM (em configuração normal) ou 6 símbolos (em configuração estendida).
- **Resource Block (RB):** 12 subportadoras de 15 kHz por 1 slot (0,5 ms), totalizando 180 kHz.

O LTE suporta dois modos de duplexação: **FDD (Frequency Division Duplex)**, em que downlink e uplink usam frequências diferentes; e **TDD (Time Division Duplex)**, em que downlink e uplink compartilham a mesma frequência, alternando no tempo. O TDD é mais eficiente para tráfego assimétrico, enquanto o FDD é mais simples e mais adequado para tráfego simétrico.

O LTE usa **MIMO (Multiple Input Multiple Output)** para aumentar a capacidade e a eficiência espectral. No downlink, suporta até 4x4 MIMO (Release 8) e 8x8 MIMO (Release 10). No uplink, suporta até 4x4 MIMO (Release 10). O MIMO explora a diversidade espacial e a multiplexação espacial para transmitir múltiplos fluxos de dados simultaneamente.

O LTE também usa **modulação adaptativa**: QPSK, 16-QAM, 64-QAM (e, no LTE-A, 256-QAM). A modulação é adaptada às condições do canal, com base no CQI (Channel Quality Indicator) reportado pelo terminal.

5.5 LTE-Advanced: a evolução do 4G

O **LTE-Advanced** (Release 10 e posteriores) foi a resposta do 3GPP aos requisitos do IMT-Advanced da ITU. Introduziu várias inovações:

- **Agregação de portadoras (Carrier Aggregation):** combinação de múltiplas portadoras (até 5, totalizando 100 MHz) para aumentar a largura de banda. As portadoras podem ser contíguas (intra-band) ou não contíguas (inter-band).
- **MIMO avançado:** até 8x8 no downlink e 4x4 no uplink.
- **Coordinated Multipoint (CoMP):** coordenação entre múltiplas células para melhorar a qualidade e reduzir a interferência.
- **Relay nodes:** nós intermediários que amplificam e retransmitem o sinal, melhorando a cobertura em áreas remotas.
- **Heterogeneous Networks (HetNet):** combinação de macrocélulas, picocélulas, femtocélulas e relays, para aumentar a capacidade e a cobertura.

O LTE-Advanced Pro (Release 13 e posteriores) introduziu ainda:

- **Licensed-Assisted Access (LAA):** uso de espectro não licenciado (5 GHz) em conjunto com espectro licenciado.

- **NB-IoT e eMTC:** tecnologias de baixo consumo para IoT.
- **V2X (Vehicle-to-Everything):** comunicação veicular.
- **Massive MIMO:** uso de dezenas ou centenas de antenas para aumentar a capacidade.

5.6 VoLTE: a voz sobre LTE

Uma das maiores mudanças do LTE foi a eliminação do domínio de circuito. No 3G, a voz era transmitida pelo CS Core; no LTE, não há CS Core. A voz precisa ser transmitida por VoIP, usando o **IMS (IP Multimedia Subsystem)**. Essa tecnologia é chamada de **VoLTE (Voice over LTE)**.

O VoLTE oferece várias vantagens: melhor qualidade de voz (AMR-WB, 16 kHz), estabelecimento de chamada mais rápido (1-2 segundos, contra 5-8 segundos no 3G), e integração com serviços de dados (vídeo chamada, compartilhamento de tela). Em contrapartida, exige cobertura LTE contínua e suporte do terminal.

5.7 O legado do 4G

O 4G deixou um legado profundo:

- **All-IP:** pela primeira vez, uma rede móvel é totalmente IP.
- **OFDMA:** uma tecnologia que dominou o 4G e influenciou o 5G.

- **Arquitetura simplificada:** eNodeB, MME, SGW, PGW — conceitos que evoluíram para gNB, AMF, SMF, UPF.
- **VoLTE:** uma tecnologia que viabilizou a voz sobre IP.
- **Agregação de portadoras:** uma técnica que aumentou a largura de banda.
- **MIMO:** uma técnica que aumentou a capacidade e a eficiência espectral.

O 4G ainda opera em todo o mundo, e continuará operando por muitos anos, mesmo com a chegada do 5G.

Capítulo 6. 5G: NSA, SA, Open RAN e evolução do ecossistema

6.1 A necessidade de uma nova geração

No início dos anos 2010, o 4G começava a mostrar suas limitações. A demanda por dados crescia exponencialmente, impulsionada por vídeo streaming, realidade virtual, IoT, e veículos autônomos. O 4G, com sua latência de 10-20 ms e sua arquitetura relativamente rígida, não conseguia atender a todos os casos de uso. Era preciso uma nova geração, com requisitos muito mais ambiciosos.

O 5G foi projetado para atender a três categorias de serviços:



SOBRE O AUTOR

Wagner R. Bomfim é autor brasileiro e profissional de Tecnologia e Telecomunicações, com mais de 20 anos de experiência em Infraestrutura de Redes e operações de redes móveis 2G, 3G, 4G e 5G, atuando em projetos de Rollout, Otimização e Operações para operadoras como TIM, VIVO e Claro.

Ao longo de sua trajetória, conciliou experiência de campo, conhecimento técnico e gestão de projetos. Atuou como Coordenador de Drive Test em projeto nacional da Huawei e na coordenação de operações de Rollout e Otimização, liderando equipes, acompanhando indicadores de desempenho, SLAs, cronogramas e padrões técnicos.

Sua experiência abrange infraestrutura de sites celulares, sistemas de energia AC/DC, climatização, transmissão, documentação técnica e análise de KPIs. Possui domínio de ferramentas como Genex Cloud, Genex Assistant, ISDP, XCal e Nemo, além de Excel Avançado.

Obras Técnicas Publicadas

É autor de diversas obras dedicadas à engenharia aplicada e às redes móveis, entre elas:

- Engenharia Completa de Redes Móveis
- Otimização de Redes Móveis
- Dominando as Redes 5G
- Implantação de Redes Celulares
- Impulsos Invisíveis

Seus livros abordam implantação, otimização multi-vendor, arquitetura 5G SA e NSA e fundamentos de infraestrutura Telecom, transformando conhecimentos técnicos e experiências práticas em conteúdo estruturado e didático.

Formação e Certificações

É Tecnólogo em Análise e Desenvolvimento de Sistemas pela Universidade Estácio de Sá, com certificações Cisco CCNA, Fortinet NSE 1 e 2, Gestão de Projetos (ENAP), Liderança Situacional (Solides) e Líder Coach (Sebrae).

Sua atuação é marcada pela visão sistêmica, liderança, organização e compromisso com a

ENGENHARIA POR TRÁS DO SINAL — Do Terreno ao Usuário Final reflete essa jornada: a perspectiva de quem vivenciou diferentes etapas do ciclo de vida de um site celular e transforma essa experiência em conhecimento compartilhado.

Wagner R. Bomfim

Autor - www.prosivasolutions.com