Alisson Stadler de Paula

Este trabalho foi inteiramente realizado em equipe, onde todos os integrantes pesquisaram, estudaram e discutiram todos os temas aqui abordados, contudo tive sólidas contribuições nos capítulos de Segurança em redes móveis 2G – GSM/GPRS/EDGE, Principais avanços de segurança do 2G, principais vulnerabilidades do 2G, Segurança em redes móveis 3G – UMTS, Principais avanços do 3G e Principais vulnerabilidades do 3G.

SEGURANÇA EM REDES MÓVEIS

Alisson Stadler de Paula
Marcos Artur Bressan
Takumi Abe

Pós Graduação em Redes e Segurança de Sistemas
Pontifícia Universidade Católica do Paraná

Resumo

Com a evolução e popularização dos sistemas de comunicação móvel, principalmente para acesso a serviços de dados, torna-se cada vez mais importante um olhar mais atento aos sistemas de segurança para estes usuários. Desde os sistemas analógicos, posteriormente GSM, passando pelo UMTS e mais recentemente com a quarta geração, o LTE, muitas modificações e evoluções ocorreram. Será que as redes móveis dispõem de sistemas suficientemente seguros? Quais são as vulnerabilidades em cada geração e como podemos nos precaver? No intuito de responder estes questionamentos é que desenvolvemos este estudo, explanando sobre os sistemas e comparando-os.

Palavras chave: Segurança; Redes Móveis; GSM; UMTS; LTE; WiMAX

Orientador: Prof. Marcelo E. Pellenz

Curitiba, fevereiro de 2013

1. Introdução

Desde o surgimento da primeira geração de tecnologia para comunicação móvel celular, em meados de 1980, muitos avanços e mudanças tecnológicas ocorreram. Conforme Harte e Bowler [15], na primeira geração várias tecnologias foram desenvolvidas, por exemplo, o TACS (*Total Access Communication System*), o NMT (*Nordic Mobile Telephone*), o MCS (*Japanese Mobile Cellular System*), o NAMPS (*Narrowband AMPS*) e o sistema AMPS (*Advanced Mobile Phone Service*) que foi utilizado inicialmente no Brasil. Todos estes sistemas são analógicos, transportam somente voz e sem criptografia.

Finalizando a primeira geração, sendo considerada a transição para a segunda geração de telefonia móvel, veio o D-AMPS (*Digital* AMPS), que utilizava canais de 30kHz mantendo a compatibilidade plena com o sistema analógico já implantado. Essa tecnologia ficou conhecida pelo nome da técnica de múltiplo acesso utilizada, o TDMA (*Time Division Multiple Access* ou Acesso Múltiplo por divisão de Tempo). Nela foi possível aumentar em 3 vezes a capacidade em relação ao sistema AMPS além de ofertar novos serviços, como identificador de chamadas e mensagens de texto (SMS - *Short Message Service*).

De acordo com Allan [7], com a segunda geração em ascendência surgiram as tecnologias digitais CDMA2000 (*Code Division Multiple Access*) e o GSM (*Global System for Mobile communication*), que trouxeram a criptografia sobre a voz e mecanismos para autenticação de usuários mais eficientes. Com o 2G, além de voz e serviços de SMS havia um serviço para transmissão de dados, o CSD/HSCSD (*Circuit Switch Data/High Speed CSD*) – que modulam dados em canais de voz. Com HSCSD a taxa de *download* típica é de 48kbps.

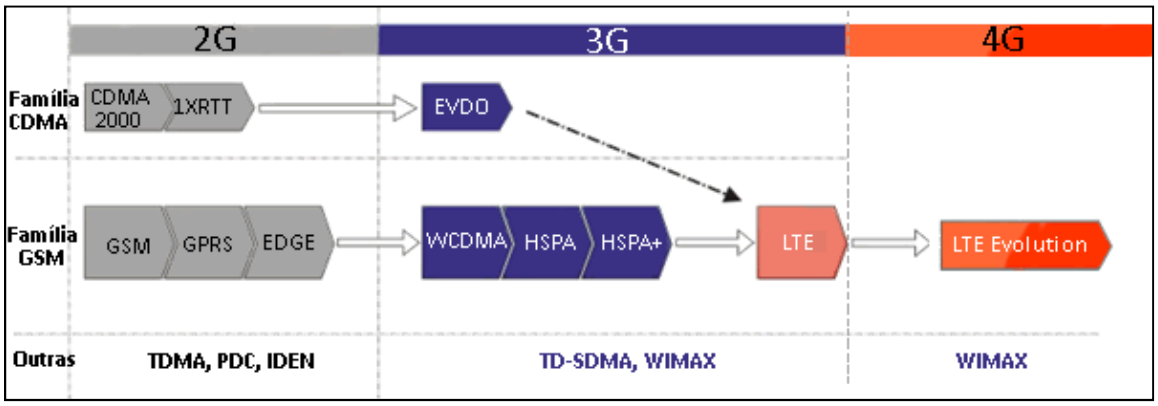
Na seqüência, Chang [9] mostra as tecnologias GPRS (*General Packet Radio Service* – 3GPP R97) e EDGE (*Enhanced Data rates for Global Evolution* – 3GPP R98) para transmissão de dados com modulação, canais e controles próprios e que foram agregadas a segunda geração. Com o GPRS e a utilização de vários canais simultaneamente, a taxa de transferência em *downlink* chegava a 65kbps; No sistema EDGE, que oferecia uma nova modulação na interface aérea - 8PSK - houve uma evolução significativa de taxa, atingindo 240kbps. Principalmente a partir desse momento houve um grande crescimento na transmissão de dados via redes móveis para as mais diversas aplicações, tais como máquinas de cartão de crédito e débito, controle de frotas (ônibus e caminhões), monitoramento de centrais de alarme, dentre outros.

Com a chegada da terceira geração, conforme Sverzut [30], o UMTS (*Universal Mobile Telecommunications System*), baseando no 3GPP R99 e R4 teve inicio a banda larga móvel, com taxa de aproximadamente 2 Mbps. As evoluções mais recentes, ainda dentro do 3G, permitem ao usuário atingir uma taxa de *download* de até 42 Mbps, com o uso da tecnologia HSPA+ (*High Speed Packet Access Plus* – 3GPP R7).

A vertente paralela, de acordo com Esteves e Swart [12], tem como terceira geração as tecnologias CDMA 1xEV-DO (*Evolution, Data-Optimized*) com otimizações que permitiram a transmissão de dados em taxas de até 2,4Mbps, porém portadoras distintas são necessárias para voz e dados; posteriormente com a tecnologia CDMA 1xEV-DV (*Evolution, Data and Voice*) voz e dados passaram a compartilhar a mesma portadora de freqüência.

A quarta geração enfim, 4G, conforme Sesia, Toufik, e Baker [27] é representada pelas tecnologias LTE (*Long Term Evolution* – 3GPP R8 e R9), também nomeado de eUMTS (*Evolved UMTS*) e WiMAX (*Worldwide Interoperability for Microwave Access* – IEEE 802.16) que oferecem taxas de *download* de até 150Mbps numa primeira fase, e de 300Mbps ou até 1 Gbps numa segunda etapa, denominada de *Trully 4G* (referentes ao 3GPP Release 10 - *LTE-Evolution* ou *LTE-Advance* e ao IEEE 802.16m para o WiMAX).

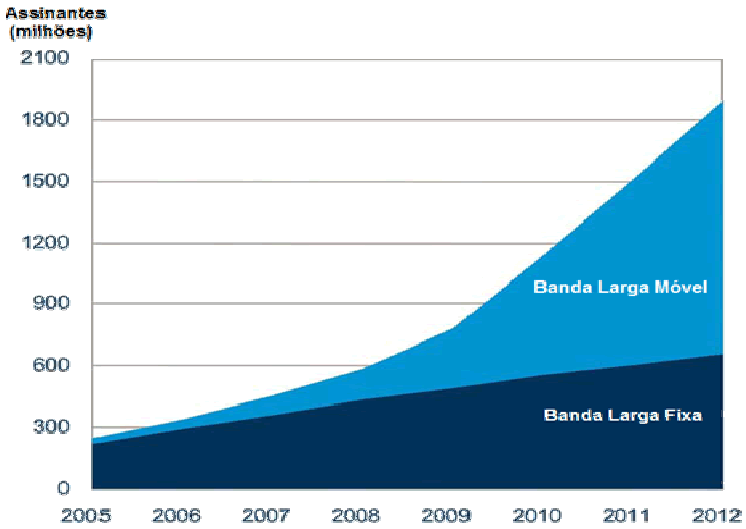
O quadro abaixo ilustra a evolução dos sistemas e as tecnologias envolvidas. A denominada "Família GSM" é que se faz presente na grande maioria das operadoras pelo mundo.



Evolução das tecnologias móveis
Fonte: TELECO [32]

Alguns autores indicam que o HSPA+ (3GPP *Release* 7) já é um sistema de quarta geração, assim como outros afirmam que o LTE (3GPP *Release* 8) ainda faz parte do 3G.

Com o aumento das taxas de *download* muitas aplicações que antes somente podiam ser utilizadas em bases fixas, passam a ser utilizadas também em equipamentos com acesso a redes móveis, como por exemplo, a navegação na internet, email, redes sociais, e principalmente as aplicações que necessitam de elevadas taxas de transmissão como, por exemplo, a transmissão de vídeos de alta definição e/ou em tempo real. Aliado a tudo isso, existe uma grande preocupação com a segurança dos dados transmitidos.



Crescimento da Banda Larga
Fonte: TELECO (OUVM, Strategy Analitics & Internal Ericsson) [32]

2. Principais ameaças de segurança em redes móveis

Em pouco mais de uma década houve um crescimento extraordinário associado à telefonia móvel tanto em número de usuários quanto em tecnologia, que saiu da primeira para a quarta geração. Devido a esse fenômeno os aparelhos celulares mudaram o seu *status*, se tornando cada vez menos telefones e mais computadores, e, portanto ficando gradativamente mais suscetíveis as diversas formas de ataques. Um celular desprotegido associado a uma rede "insegura" pode resultar numa invasão muitíssimo onerosa a privacidade individual, possibilitando fatos como adulteração de dados ou até mesmo um roubo via *Mobile Banking*, por exemplo. Em outras palavras significa que um invasor pode ouvir suas chamadas, ler suas mensagens de texto, acompanhar sua atividade na internet e não obstante apontar sua localização geográfica.

Para que uma rede seja considerada minimamente segura em padrões internacionais, de acordo com a norma ISO IEC 17799 [17], ela deve seguir alguns preceitos básicos de segurança:

- Confidencialidade: Garante que o acesso às informações esteja ligado somente a entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;

- Integridade: Garante que toda informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo mudanças, nascimento, manutenção e fim da informação;

- Disponibilidade: Garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

- Autenticidade: Garante que a informação foi produzida, modificada ou descartada por uma determinada pessoa física, órgão, entidade ou sistema com intuito de validar sua origem.

Os conceitos do quarteto acima não se referem apenas a sistemas computacionais, mas sim a todo e qualquer modelo de informações, dados e comunicações. Nesse contexto serão enfocados os seguintes tipos de ataques mais comuns em redes móveis:

- **Acesso não autorizado *(Unauthorized Access)***: Se um método de autenticação não é propriamente aplicado ou é mal configurado, então um invasor pode ter acesso livre a rede e usar seus serviços mesmo não sendo autorizado para isso;

- **Obstrução do meio *(Channel Jamming)***: É uma técnica usada pelos invasores cujo objetivo é destruir ou degradar o sinal da interface aérea, e dessa forma desabilitar o acesso dos usuários legítimos dessa rede deixando-os expostos a "outras" redes;

- **Negação de serviço *(Denial of Service)***: É causada pelo envio excessivo de dados na rede, mais do que ela pode suportar, deixando os usuários sem os recursos de rede disponíveis;

- **Espionagem *(Eavesdropping)***: Se o tráfego na interface aérea não for fortemente criptografado, um invasor pode espiar ou interceptar dados importantes ou ligações telefônicas confidenciais;

- **Mensagens Falsificadas *(Message Forgery)***: Se o canal de comunicação não for suficientemente seguro, um invasor pode mudar o conteúdo das mensagens em ambas as direções sem ao menos que os reais receptores perceberem isso;

- **Ataque Invasor-no-meio *(Man In The Middle Attack)***: Um atacante pode estar entre um telefone celular e um ponto de acesso da rede para interceptar mensagens;

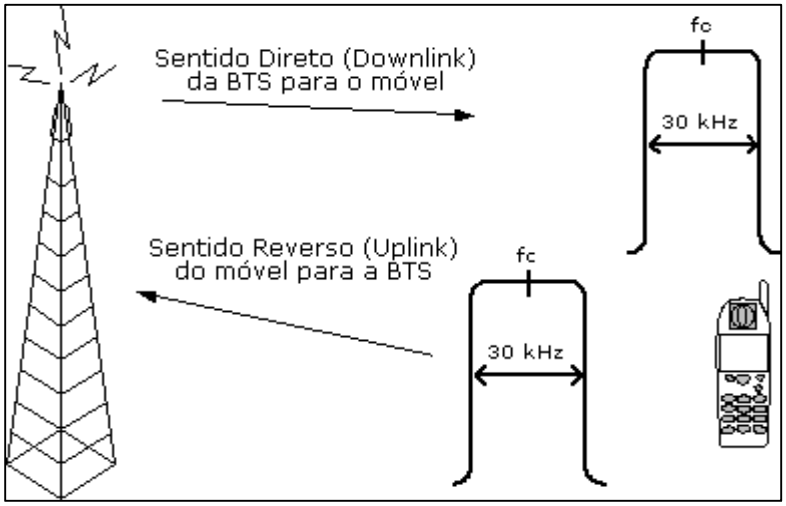
- **Sequestro de sessão *(Session Hijacking)***: Um usuário malicioso pode sequestrar uma sessão já estabelecida e atuar como um legítimo usuário de uma determinada *base station*.

Devido ao dinamismo da tecnologia e à natureza aérea de uma rede móvel, não há como oferecer qualquer tipo de "certeza de segurança definitiva" na solução destes problemas. Porém existem muitos métodos de minimizar ou em vários casos eliminar essas tentativas de quebra dos mecanismos de segurança das redes móveis.

3. Segurança em redes móveis 1G - AMPS

Baseando-se em Tude [34], o sistema AMPS (*Advanced Mobile Phone System*) foi desenvolvido pela *Bell Labs* em 1978 e padronizado pela ANSI EIA/TIA-553. Foi a primeira geração de telefonia celular adotada em larga escala no mundo e também no Brasil. Suas redes eram totalmente analógicas e somente transmitiam informação de voz usando canais de frequência separados para cada chamada.

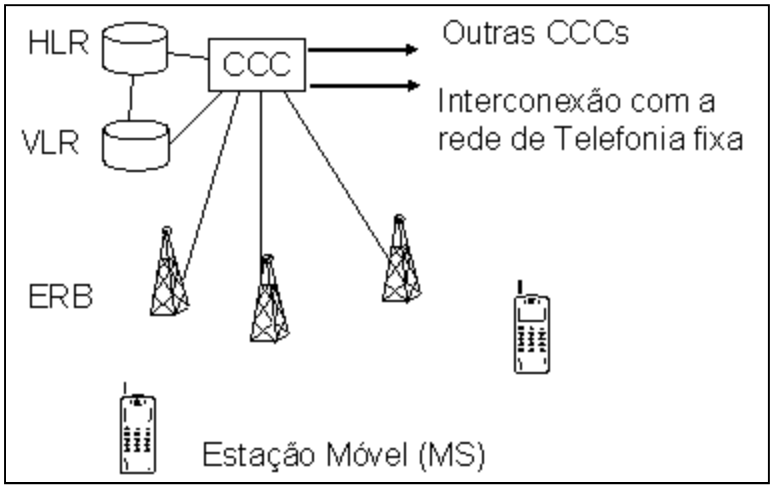
Tinha transmissão full-duplex e usava a faixa de frequência que variava de 800MHz a 900MHz, dependendo da localidade. O método de acesso aos canais de 30kHz (em cada sentido) era via FDMA (*Frequency Division Multiple Access*) utilizando modulação analógica FM. Isso trazia algumas desvantagens como exigência de largura de banda considerável para vários usuários simultâneos, linhas cruzadas (*cross talking*), interferências e principalmente problemas de segurança que serão mencionados na sequência.



Banda para Telefonia Celular: 850MHz e o sistema AMPS
Fonte: TELECO [32]

Tude [34] explica ainda que essa topologia de rede não oferecia sistemas de criptografia e, portanto qualquer pessoa que coletasse os dados na interface aérea poderia facilmente decodificar os dados. Nos anos 90 essa prática acabou se tornando cada vez mais comum. Um atacante com equipamentos especializados como um RF Scanner UHF que demodula sinais FM podia facilmente escutar ou reproduzir conversas particulares, quebrando o sigilo telefônico.

Além disso, era possível também capturar o ESN (*Electronic Serial Number*) e o MIN (*Mobile Identification Number*) que autenticavam o usuário ao sistema. O ESN era um número de 12 dígitos enviados pelo telefone celular para a rede *Core* da operadora para efeitos de tarifação e identificação de usuários. No entanto esses dados eram transmitidos em formato texto e caso alguém interceptasse o par ESN/MIN esses dados poderiam ser clonados para outro telefone gerando um enorme precedente de problemas e vulnerabilidades.



Arquitetura de rede móvel 1G
Fonte: TELECO [32]

De acordo com Engel [11] um exemplo de ataque pode ser descrito ou realizado em três partes. Primeiramente é preciso um receptor de RF, como por exemplo o Icom PCR-1000, que pode ser sintonizado num canal reverso, que é a frequência em que os telefones mandam os dados para a torre. O segundo item seria um computador com uma placa de som comum e um software chamado Banpaia instalado e por último um telefone fácil de ser configurado para ser clonado como o OKI 900. Sintonizando o receptor de RF na frequência apropriada, ele recebe o sinal transmitido pelo celular a ser clonado contendo o par ESN/MIN. Esse sinal deve ser introduzido na entrada de áudio do PC e o software Banpaia vai decodificar esse sinal contendo o ESN/MIN e mostrá-lo na tela. Por fim, esses dados revelados são configurados no celular OKI 900 e após um reset no aparelho a rede não distingue mais entre o verdadeiro e o clonado, dando ao impostor a chance de atuar como o assinante legítimo.

Principais vulnerabilidades do 1G

A fraca autenticação e a não existência de criptografia certamente eram os pontos mais fracos dessa rede. Mesmo para os padrões da época era relativamente fácil burlar os poucos mecanismos de confidencialidade, integridade e autenticidade adotados para o AMPS. Nota-se claramente que a rede era suscetível a quase todas as formas de ataque, como acesso não autorizado, espionagem, ataque invasor-no-meio, sequestro de sessão e clonagem.

Essas vulnerabilidades tomaram uma proporção tão grande que algumas operadoras começaram adotar um sistema de *PIN Code* antes de se efetuar uma chamada. De qualquer forma os problemas foram apenas minimizados e não totalmente sanados. Então, a solução mais plausível seria converter as redes analógicas para redes digitais. Diante disso a organização norte-americana FCC (*Federal Communications Commission*) decidiu em 2002 que não iria mais conceder portadoras de banda A e B para suportar o serviço AMPS a partir de 18 de fevereiro de 2008. Nesse cenário as operadoras se viram

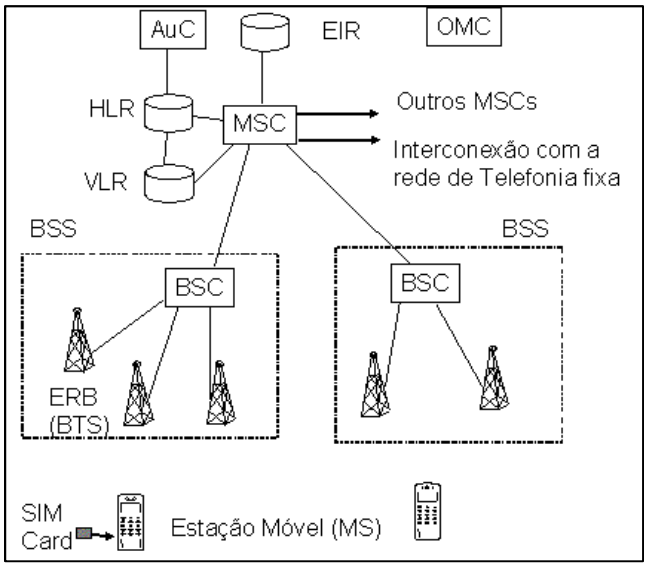
forçadas a evoluir suas redes para D-AMPS (*Digital* AMPS - mais conhecida como TDMA) ou para tecnologias concorrentes e mais bem sucedidas como o CDMA2000, GSM, entre outras. Assim se iniciou a segunda geração das redes móveis celulares.

4. Segurança em redes móveis 2G – GSM/GPRS/EDGE

Segundo Tude [35] e Silva [28], a segunda geração de telefonia celular encontrou no GSM (*Global System for Mobile Communications*) o padrão de maior sucesso, sendo ainda hoje o sistema mais utilizado mundialmente. Para a implantação do GSM no Brasil foram licitadas as bandas C, D e E que trabalham na faixa de 1800MHz de frequência. Esse espectro foi divido em 373 canais com banda de 200kHz para o par de frequências de transmissão e recepção, conhecidos como ARFCN (*Absolute Radio Frequency Channel Number*) que são utilizados tanto como canais de tráfego quanto canais de controle. A modulação digital utilizada é o GMSK (*Gaussian Minimum Shift Keying*) operando com divisão de 8 *timeslots* através de TDMA.

Foi com esta tecnologia que pela primeira vez dados começaram a ser transmitidos na interface aérea de forma digital. Além disso, novos serviços começaram a ser ofertados, como SMS (*Short Message Service*), transmissões de pacotes de dados, identificador de chamadas, além de melhor eficiência na utilização do espectro de frequências. Finalmente ganhou-se facilidade e flexibilidade de utilização de recursos convenientes para aperfeiçoar a segurança das informações, pois todo e qualquer dado transmitido tem criptografia digital. Essa nova forma de transmitir dados foi revolucionária em termos de segurança se comparado à tecnologia anterior, porém ainda não foi o suficiente para evitar outras formas de ataques.

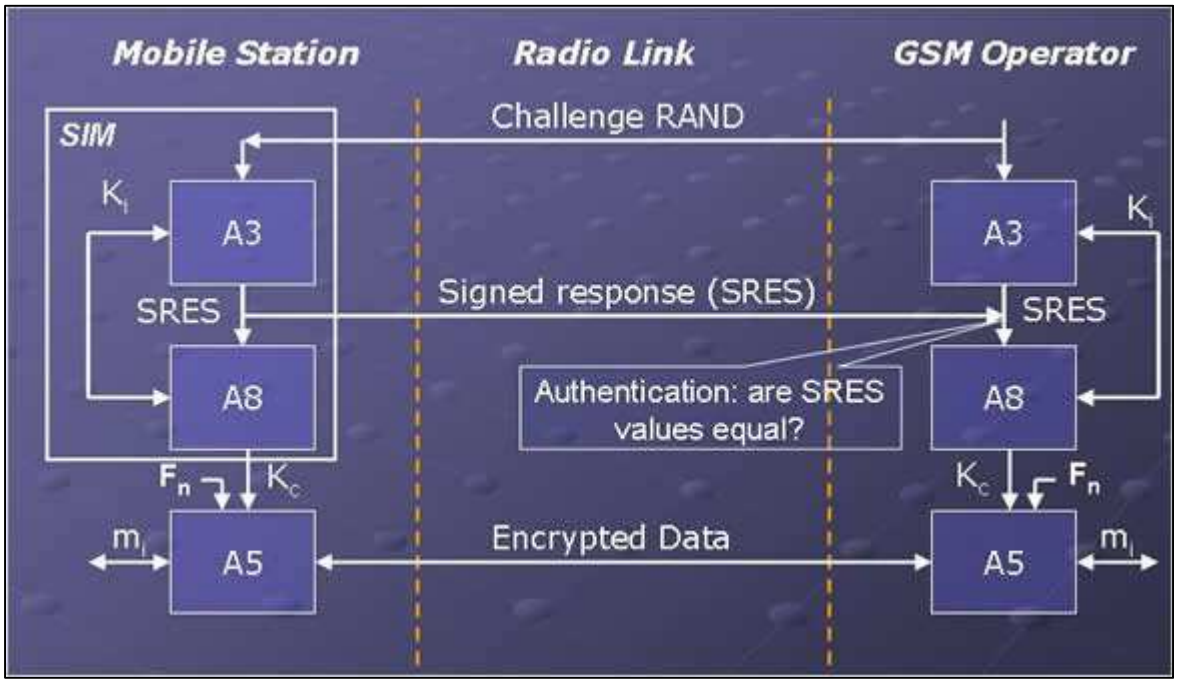
A estrutura de uma rede móvel 2G está ilustrada na figura abaixo:



Arquitetura de rede GSM
Fonte: TELECO [32]

Em termos de segurança, segundo Chang [9], os primeiros itens a serem pensados numa rede 2G são a identificação e autenticação do usuário, por isso foi criado o SIM (*Subscriber Identity Module*). No SIM *Card* está registrado o IMSI (*International Mobile Subscriber Identity*), que é único na rede e a partir dele que são iniciados os processos de segurança.

Molva [16] descreve que a rede GSM realiza o processo de autenticação do assinante através do SIM usando um mecanismo tipo desafio/resposta. O processo se inicia quando a *Base Station* envia ao móvel um número aleatório de 128 bits, chamado *Challenge RAND.* Para poder responder ao *RAND*, o *SIM Card* estando ligado ao telefone utiliza o algoritmo A3 e a *Individual Subscriber Authentication Key*, conhecida como Ki (única para cada *SIM card*) e dessa forma pode criar o *Signed Response* de 32bits (ou SRES) e o manda de volta para a rede. Caso o SRES corresponda com o valor pré-calculado pela *Base Station*, então o próximo passo é dado. Na segunda etapa, o SIM utiliza um algoritmo diferente, o A8, juntamente com o Ki e o *Challenge RAND* original para calcular a *Session Key* (Kc); e novamente envia ao *Core* da rede. Por fim essa chave de sessão (Kc) é utilizada junto ao algoritmo A5 para criptografar e descriptografar os dados que serão enviados na interface aérea, conforme o diagrama abaixo:



GSM Security

Fonte: Networks and Telecommunications Research Group [18]

No lado da rede o responsável pela verificação, cálculo e autenticação dos *Triplets* (RAND, SRES e Kc) é o AuC (*Authentication Center*) e todo o processo é feito num sistema de *handshake*, ou seja, caso algum dos valores não coincidam em ambos os lados (rede e terminal), a conexão é interrompida e a falha de autenticação é reportada. Adicionalmente, está previsto a troca da chave de criptografia de tempos em tempos. Também é utilizado o parâmetro TMSI (*Temporary Mobile Subscriber Identity*),

evitando que o IMSI seja divulgado na interface aérea. O TMSI, gerenciado pela MSC (*Mobile Switching Center*) é enviado para o terminal depois que os procedimentos de autenticação e cifragem estiverem concluídos tornando o sistema ainda mais resistente a ataques.

Nas redes GPRS/EDGE, segundo Chang [9], o processo é semelhante, porém ao invés do TMSI, associa-se ao usuário um TLLI (*Temporary Logical Link Identity*) tratado pelo SGSN (*Serving GPRS Support Node*). A autenticação do usuário em GPRS é similar ao procedimento usado em GSM. Adicionalmente a chave de cifragem é gerada com o algoritmo GEA (*GPRS Encryption Algorithm*), ao invés do algoritmo A5, usado para voz.

Principais avanços de segurança do 2G

Gardezi [14] discorre que pela primeira vez as redes móveis tiveram um nível de segurança moderado. Se comparado com os métodos das redes da geração anterior, houve uma significativa melhora no processo de autenticação e confidencialidade dos usuários. Além do *SIM Card* agora também se utilizam os algoritmos A3/A8 junto ao AuC, e devido a isso a clonagem de telefones ficou reduzida a um valor quase inexpressivo. Outro avanço importante foi a adoção de algoritmos de cifragem A5.1, A5.2 e A5.3 na interface aérea, garantindo maior segurança das informações.

Principais vulnerabilidades do 2G

Com o passar do tempo todos os algoritmos de criptografia e autenticação mencionados acima acabaram se mostrando fracos e já foram quebrados, tendo no A5 (tanto na versão 1 quanto a 2) os pontos de vulnerabilidade mais explorados. Dentre os principais pontos fracos de uma rede GSM estão:

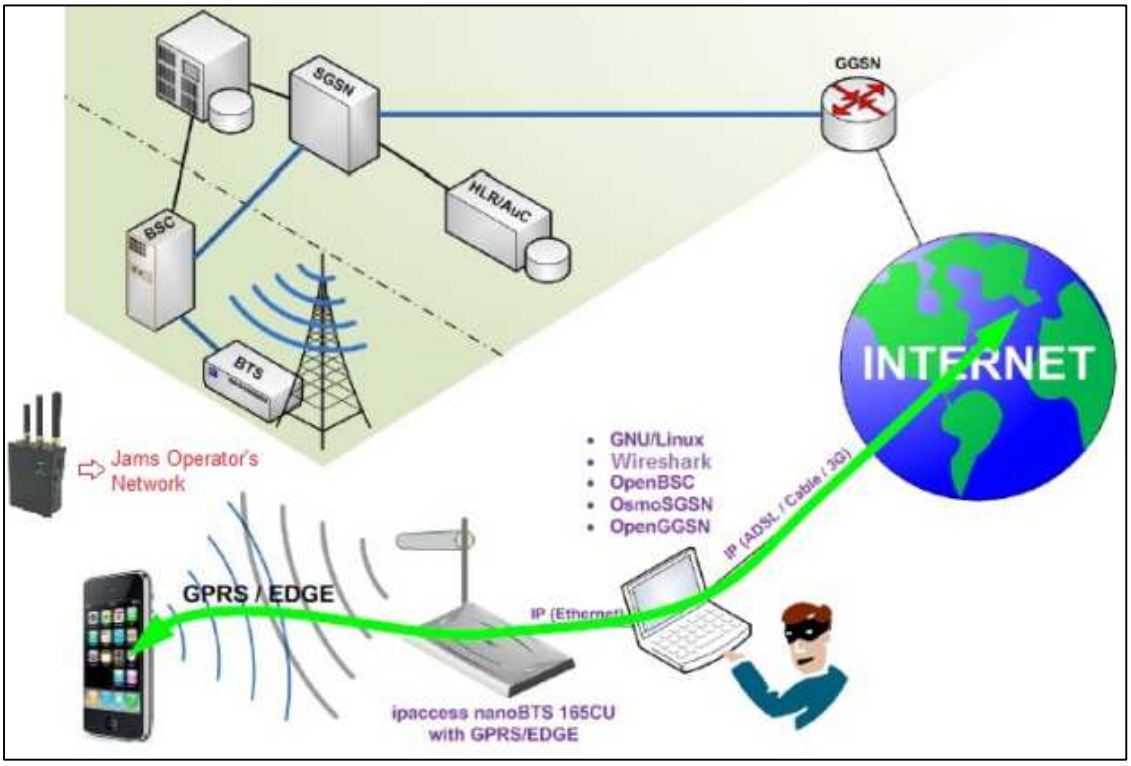
- Chaves de tamanho pequeno (64bits);
- Apenas o usuário se autentica na rede e não vice-versa;
- Não possui verificação na integridade de dados;
- Transmissão de chaves de forma insegura, entre outros.

Diante dessas vulnerabilidades, mais uma vez a rede celular móvel se encontrou diante de problemas já enfrentados no passado, como acesso não autorizado, negação de serviço, espionagem, ataque invasor-no-meio, sequestro de sessão, etc. Existem algumas formas de burlar os mecanismos de segurança de uma rede 2G, até mesmo via força bruta devido a velocidade dos processadores dos computadores de hoje em dia.

Um dos ataques mais comuns, explicitados por Perez e Picó [21], acontece através do método “Rogue BTS”, que explora o fato do aparelho móvel não autenticar a rede onde ele se conecta e a possibilidade que os aparelhos possuem de operarem sem cifragem. O exemplo pode ser considerado um ataque *Man-in-the-Middle* numa rede GPRS/EDGE. Para isso, utiliza-se um bloqueador de sinal (*channel jammer*), uma nanoBTS comercial (*Rogue BTS*) e um computador com os seguintes softwares

livres instalados: Wireshark, OpenBSC, OsmoSGSN, OpenGGSN (esses três últimos rodando em máquinas virtuais) para emular o *packet core* da rede.

Primeiramente se obstrui o sinal da operadora com *channel jammer*, e paralelo a isso se inicia a transmissão da *Rogue BTS* (falsa). O celular irá perceber a piora súbita do sinal da rede onde ele está conectado e automaticamente irá procurar um sinal melhor. Como a BTS falsa estará com nível de sinal maior, o celular irá tentar se conectar a ela. O celular executa um *cell re-selection*, um *location update request* e *attach request*, com isso a falsa rede obtém seus parâmetros de entrada. Obviamente os emuladores da falsa rede trabalharão sem cifragem (A5.0 ou GEA.0) e propositalmente autenticam esse usuário, que conseqüentemente, se conecta na *Rogue BTS*. Com o Wireshark (em especial na versão 1.8.3) se monitora toda a transmissão de pacotes provenientes do móvel, tendo assim um bem sucedido ataque *man-in-the-middle*, como ilustrado na figura a seguir.



Ataque prático contra comunicações móveis
Fonte: Perez e Picó [21]

Medidas de segurança em qualquer sistema tem uma validade limitada e obviamente que os sistemas de segurança das redes 2G já estão ultrapassados, permitindo os mais variados tipos de ataques. Com a evolução para os sistemas 3G muitas destas vulnerabilidades foram sanadas, conforme exposto na seqüência.

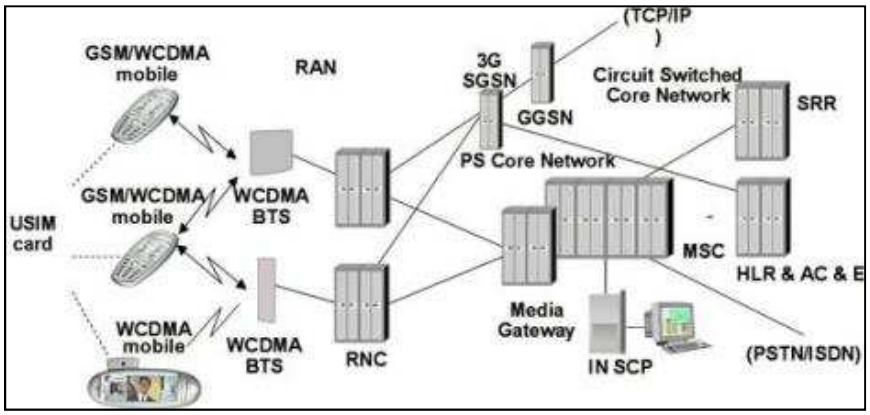
5. Segurança em redes móveis 3G – UMTS

Sverzut [30] mostra que nas redes UMTS muitas características foram herdadas da rede GSM, toda a parte de *Switching Core* e *Packet Core* da rede foram mantidos, no entanto se diferenciam totalmente na parte de acesso (*Radio Access*). Em termos de segurança o processo de uso do TMSI e TLLI é idêntico as redes GSM/GPRS/EDGE e isso facilita bastante para que se tenha uma migração suave ou interoperabilidade entre redes 2G e 3G.

Para proteção dos dados na interface aérea, Pütz, Schmitz e Martin [25] demonstram que o UMTS adiciona como camada de segurança de proteção, o UEA (*UMTS Encryption Algorithm*), que possui uma grande vantagem sobre os modelos utilizados nas redes 2G, A5.x e GEAx, pois ele não é secreto, fazendo com que sua força não esteja em seu desconhecimento e sim na sua própria robustez, tornando-se eficaz contra ataques de engenharia reversa.

Straccialano [29] demonstra o modelo de *stream cipher* aplicado no UEA, tanto para sinalização como para dados de usuário, denominado F8, possui como referência o algoritmo KASUMI. O F8 possui chave de 128 bits, tornando ataques como o *Birthday Attacks* e força bruta inviáveis. O algoritmo de integridade (*UIA – UMTS Integraty Algorithm*), denominado F9, é implementado no terminal e na RNC (*Radio Network Controller*). No 3G também foi implementado um novo cartão SIM, denominado uSIM (UMTS/UTRAN SIM) e com ele as novas técnicas de autenticação e cifragem puderam ser aplicadas. O método de autenticação e troca de chaves, AKA (*Authentication and Key Agreement*), utiliza o mecanismo de desafio/resposta (*Challenge/Response*) semelhante ao utilizado no GSM, porém com 5 elementos (*quintuplets*) ao invés de 3 (*triplets*). Atualmente a recomendação 3GPP para AKA é a chamada *MILLENAGE*, que se baseia no compartilhamento popular de algoritmos de chaves secretas, chamadas AES ou Rijndael. O algoritmo AKA fornece autenticação mútua para o usuário e a rede, além disso, o usuário e a rede combinam uma chave de cifragem (*Chiper Key – CK*) e uma chave para integridade (*Integraty key – IK*).

A arquitetura básica de uma rede UMTS é mostrada na figura abaixo:



Arquitetura de rede UMTS
Fonte: DriveTestBr [10]

Principais avanços do 3G

Com o uso do uSIM novas técnicas de autenticação se tornaram possíveis, e então, não mais 3 elementos são usados, mas 5 (RAND, XRES, Ck, Ik e AUTN). Além disso, o tamanho das chaves foi aumentado de 64 para 128bits, dificultando bastante ou até inviabilizando ataques por força bruta.

Foi criada também uma camada de segurança, o UEA, e nela os algoritmos de autenticação, cifragem e integridade são aplicados. Para aumentar a confidencialidade, somente o algoritmo UEA1 (AES) é utilizado, por ser o mais forte.

Através do algoritmo AKA (*Authentication and Key Agreement*) é feita a autenticação do terminal com a rede, assim como nos sistemas 2G, mas também a autenticação da rede ao terminal. Desta forma os ataques por falsa estação rádio base se tornam inviáveis.

Principais vulnerabilidades do 3G

Um dos tipos de ataque contra as redes 3G utiliza a técnica de estação rádio base falsa, porém como na rede 3G ocorre a autenticação mútua, faz-se necessário inibir o sinal 3G com o uso de bloqueadores de sinal para que o terminal busque uma outra rede, e desta forma a estação rádio base falsa, em 2G, poderá ser utilizada para o ataque.

Ataques oriundos de interfaces IP, tais como negação de serviço - DOS, *SYN-flood* ou *smurf*, são possíveis, porém bastante controlados pelas ferramentas de segurança da rede de pacotes.

6. Segurança em redes móveis 4G - LTE

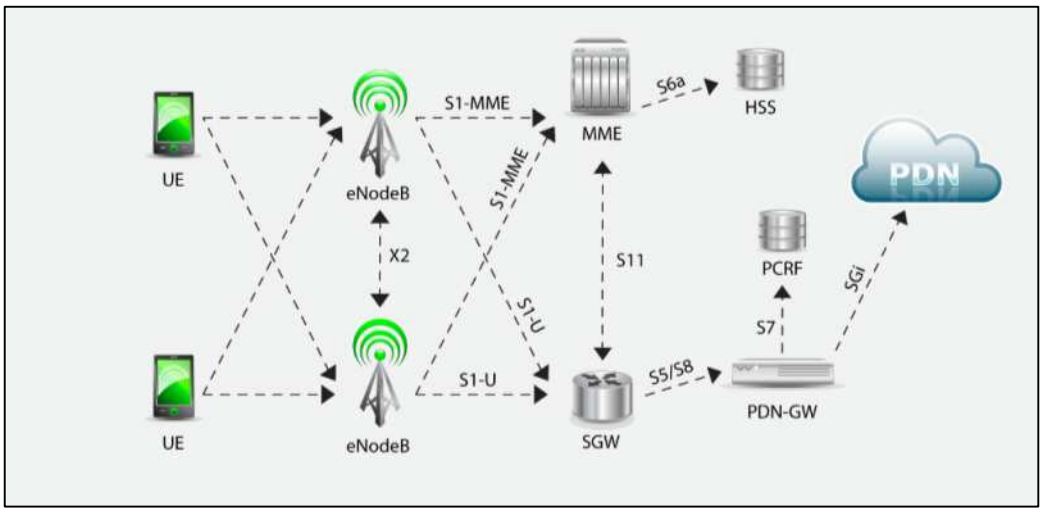
A quarta geração dos sistemas de comunicação móvel teve como princípio de desenvolvimento ser totalmente IP, isto é, todos os elementos, com exceção do terminal, devem se comunicar por interfaces puramente IP. Com isso, várias técnicas de autenticação, integridade e confidencialidade já existentes e utilizadas nas redes IP são empregadas no 4G, como por exemplo, o IPSec, o CMP (*Certificate Management Protocol*) e o TLS (*Transport Layer Security*).

De acordo com Poole [23] e Niemi [20] uma rede de quarta geração utiliza menos elementos físicos, equipamentos, porém cada um com mais funções. É previsto ainda a utilização de células para cobertura de pequenas áreas, tais como residências ou escritórios, denominadas Femto Cells (HeNB – Home eNB). No LTE a cifragem é aplicada para os dados de usuário e de controle, e a proteção de integridade é aplicada somente para os dados de controle, através do protocolo PDCP (*Packet Data Convergence Protocol*).

Com o PDCP ocorre o controle da quantidade de pacotes enviados e recebidos (*COUNT*) e o controle da seqüência dos pacotes (*SN – sequence number*). Com esse procedimento os ataques do tipo *replay attack*, onde o invasor tenta reenviar um pacote capturado anteriormente, é bastante dificultado. O uso do valor *COUNT* também previne o sistema de ataques contra as chaves de autenticação e cifragem; neste caso o sistema usa chaves incorrelacionáveis entre dois pacotes transmitidos.

A integridade é garantida através do campo MAC-I (*Message Authentication Code for Integrity*) para cada pacote, calculado com base nas chaves AS (*Access Stratum*), na mensagem em si, no RBI (*Radio Bearer ID*), na direção (*Uplink* ou *Downlink*) e no valor do *COUNT*.

A arquitetura básica de uma rede LTE é ilustrada na figura abaixo.



Arquitetura de rede LTE
Fonte: Breaking point Systems [8]

Cada vez mais os sistemas de comunicação móvel são utilizados para transmissão de dados e com isso alguns requisitos básicos de segurança precisam ser seguidos:

- A segurança em LTE deve oferecer pelo menos o mesmo nível de segurança que foi fornecido pelos serviços 3G;
- As medidas de segurança não devem afetar a conveniência do usuário;
- Deverão fornecer defesa de ataques vindos da Internet;
- As medidas de segurança devem ser compatíveis e permitir a transição com 3G.

Niemi [20] mostra que para garantir esses requisitos básicos de segurança, um novo sistema hierárquico de chaves foi introduzido, permitindo a renovação das chaves por diversas razões. Funções de segurança distintas são aplicadas para *Non-Access Stratum* (NAS) que envolve elementos na rede LTE, e *Access Stratum* (AS) que envolve elementos de redes 3G e 2G.

Com a transição 2G - GSM para 3G - UMTS, a idéia do *SIM card* foi atualizada para o cartão USIM – *UMTS SIM card*. Para o LTE apenas o cartão USIM pode ser usado e os antigos cartões SIM não são mais compatíveis.

Principais avanços do 4G

Todas as interfaces, exceto a de rádio, são IP e isto facilita e flexibiliza bastante a instalação e manutenção das redes.

Os sistemas de autenticação e troca de chaves foram melhorados, se comparados com os sistemas aplicados às redes 2G e 3G, utilizando chaves HMAC-SHA-256. A criptografia utiliza vetores de autenticação incompatíveis com os utilizados em redes 3G e para se manter a compatibilidade dos usuários, o USIM deve verificar o bit de separação (*separation bit*). Os algoritmos utilizados são o *AES* e o *SNOW 3G*, que utilizam chaves de 128 bits, e com capacidade de processar chaves de 256 bits, num próximo *release*.

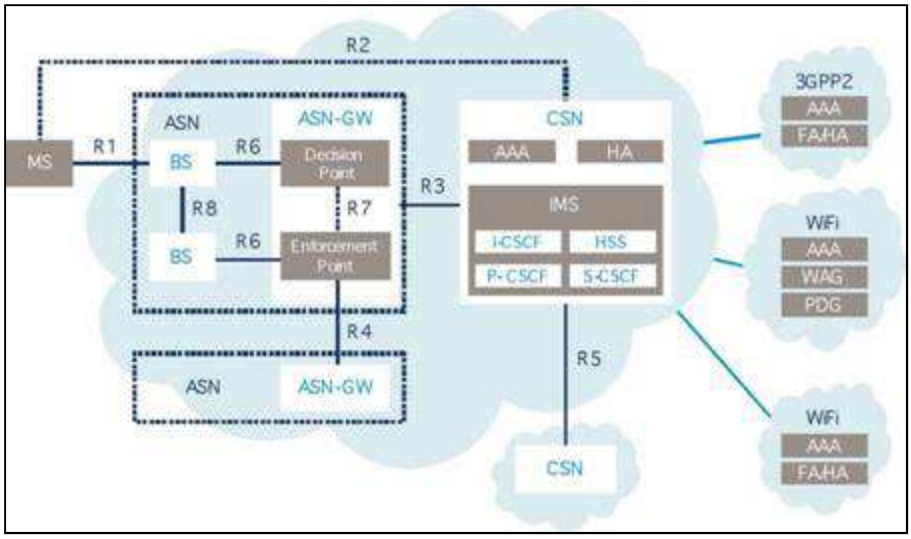
Nas interfaces S1-U e S1-MME podem, opcionalmente, ser aplicados mecanismos de segurança baseados em IPSec.

Principais vulnerabilidades do 4G

Existem vulnerabilidades devido à operação conjunta com redes 2G e 3G e ataques oriundos das interfaces IP (negação de serviço - DOS, *SYN-flood* ou *smurf*). Assim como nas redes 3G, onde muitos usuários utilizam *smart phones*, ataques podem explorar vulnerabilidades dos sistemas operacionais através de códigos maliciosos escondidos em aplicativos, mensagens de texto ou mensagens multimídia.

7. Segurança em redes móveis 4G - WiMAX

Teixeira [31] disserta sobre o padrão IEEE 802.16, finalizado em 2001 e publicado em 2002, que especifica uma interface sem fio para redes metropolitanas (WMAN). Foi atribuído a este padrão o nome WiMAX (*Worldwide Interoperability for Microwave*) criado por um grupo de indústrias cujo objetivo é promover a compatibilidade e interoperabilidade entre equipamentos baseados no padrão IEEE 802.16. Este padrão é similar ao padrão Wi-Fi (IEEE 802.11), que já é bastante difundido, porém agrega novos recursos, visando um melhor desempenho de comunicação permitindo velocidades de até 1 Gbps.



Arquitetura de rede WiMAX móvel
Fonte: Teleco [32]

O padrão WiMAX objetiva estabelecer a parte final da infra-estrutura de conexão de banda larga (*last mile*) oferecendo conectividade para uso doméstico, empresarial e em *hotspots*, com possibilidade de taxa de transmissão de 1 a 75Mbps.

Reconhecendo a importância da segurança, os grupos de trabalho destinados a especificação do padrão 802.16 desenvolveram vários mecanismos para proteção do prestador de serviço contra roubo de serviço e para proteger o cliente de divulgação de informações não autorizadas.

Principais avanços de segurança do WIMAX

Yang [37] descreve que o WiMAX utiliza o RSA (*Rivest Shamir Adleman*), o DES-CBC (*Data Encryption Standard- Cipher Block Chaining*) e AES-CCM (*Advanced Encryption Standard in Counter with CBC-MAC*) como algoritmos de criptografia. Para cifragem, o HMAC (*Hashed Message Authentication Code*) e o CMAC (*Cipher-based Message Authentication Code*) são utilizados.

O padrão 802.16 ainda especifica que cada estação de assinante (*Subscriber Station - SS*) deve utilizar o certificado X.509 para identificá-lo. O uso de certificados X.509 torna difícil um atacante falsificar a identidade dos assinantes legítimos, oferecendo ampla proteção contra roubo de serviço. A emenda 802.16**e** adicionou suporte para o *Extensible Authentication Protocol* (EAP) para redes WiMAX, que é atualmente opcional para prestadores de serviços.

Principais vulnerabilidades do WIMAX

Apesar das boas intenções para a segurança no WiMAX, existem vulnerabilidades exploradas principalmente por ataques por estações base falsas (*Rogue Base Stations*), ataques de negação de serviço (*DoS Attacks*), ataques *man-in-the-middle* e manipulação de rede com quadros de gerenciamento (*Network manipulation with spoofed management frames*).

Na especificação 802.11 (Wifi), os quadros de gerenciamento não são criptografados, permitindo ao invasor coletar informações sobre os assinantes e outras características da rede potencialmente sensíveis. Com a alteração 802.16e, permitindo a cifragem AES, houve uma grande melhoria na confidencialidade dos dados.

Nguyen [19] ressalta que muitas vulnerabilidades foram encontradas no padrão 802.16, principalmente com a adição de mobilidade (802.16e). Uma das falhas mais sérias é a falta de autenticação da rede pelo usuário, permitindo ataques *man-in-the-middle* e ataques de disponibilidade. O protocolo de gerenciamento de chaves PKM (*Privacy Key Management*) é utilizado para compartilhamento de informações de autenticação e até o 802.16 o PKMv1 é utilizado; no 802.16e foi introduzido o PKMv2, onde ocorre a autenticação mútua entre BS (*base station*) e SS.

8. Tabela Comparativa

Abaixo é disposta uma tabela comparativa entre as gerações de comunicação móvel com relação aos critérios de segurança de sistemas.

	Confidencialidade	**Integridade**	**Disponibilidade**	**Autenticidade**	**Tamanho das Chaves**	**Possíveis Proteções**
1G (AMPS)	Não tem	Não tem	Não tem	ESN/MIN (fraco)	Não tem	Adoção de PIN Code
2G (GSM/EDGE)	A5.1, A5.2 e A5.3.	Não tem	Não tem	Triplets para autenticar o usuário apenas.	64 bits	Adoção da cifragem A5.3
3G (UMTS)	UEA1 ou UEA2 (f8)	UIA1 ou UIA2 (f9)	Não tem	Quintuplets e autenticação mútua	128 bits	Fixar o terminal para operar somente em redes 3G
4G (LTE)	EEA1 (AES) ou EEA2 (SNOW)	EIA1 (AES) ou EIA2 (SNOW)	Não tem	Quintuplets e autenticação mútua	128/256 bits	Cuidados na camada de aplicação e emprego de IPSEC entre a BTS e Core
4G (WiMAX)	RSA, DES-CBC ou AES-CCM	CBC-MAC	Não tem	Certificado X.509	160 bits	Cuidados na camada de aplicação e emprego de EAP

9. Considerações Finais

Com a evolução das tecnologias nota-se claramente o emprego de técnicas cada vez mais elaboradas para prevenção de ataques e aumento do nível de segurança em redes móveis. No entando, todas as tecnologias têm vulnerabilidades que podem ser exploradas, com maior ou menor complexidade.

As redes de primeira geração praticamente não possuem dispositivos de segurança, e que na segunda geração ganharam maior atenção dos desenvolvedores, criando sistemas de autenticação e confidencialidade, até então inexistentes.

As redes 3G trouxeram técnicas de integridade além de avanços nos quesitos de segurança já existentes, como o aumento do tamanho das chaves de segurança para 128 bits. Atualmente as redes de quarta geração, predominantemente baseadas em IP, agregam técnicas de segurança até então utilizadas somente no *core* da rede.

Perez e Picó [21] ressaltam que os usuários podem tomar ações práticas afim de aumentar a segurança do sistema, como por exemplo, fixar o terminal somente em redes 3G, evitanto assim o ataque de *rogue BTS*.

Além disso, os *smartphones* devem ser tratados como computadores pessoais, com necessidade de constantes atualizações do sistema operacional e uso de antivirus.

Poole [24] fomenta algumas idéias e iniciativas para a quinta geração de comunicação móvel, e termos como o “wwww” (*World WideWireless Web*), tecnologias de rádio cognitivo, redes universais (*Pervasive Networks*), *smart antennas*, entre outros.

O estudo realizado envidenciou que a evolução dos sistemas de segurança empregados visam corrigir e minimizar as vulnerabilidades, assim como aplicar técnicas para dificultar os ataques. Da mesma forma os *hackers* também aprimoram suas técnicas criando um círculo vicioso.

10. Referências

[1] 3rd Generation Partnership Project. **3GPP TS33.102 – UMTS security.** Disponível em: <http://www.3gpp.org>. Acesso em: 22/08/2012.

[2] 3rd Generation Partnership Project. **3GPP TS33.210 – 3G security; Network Domain Security (NDS); IP network layer security.** Disponível em: <http://www.3gpp.org>. Acesso em: 21/10/2012.

[3] 3rd Generation Partnership Project. **3GPP TS33.310 – Network Domain Security (NDS); Authentication Framework (AF).** Disponível em: <http://www.3gpp.org>. Acesso em: 21/10/2012.

[4] 3rd Generation Partnership Project. **3GPP TS33.401 – 3GPP System Architecture Evolution (SAE); Security architecture.** Disponível em: <http://www.3gpp.org>. Acesso em: 22/10/2012.

[5] 3rd Generation Partnership Project. **3GPP TS33.402 – Architecture enhancements for non-3GPP accesses.** Disponível em: <http://www.3gpp.org>. Acesso em 22/10/2012.

[6] **4Gamericas**. Disponível em: <http://www.4gamericas.org>. Acesso em: 28/08/2012.

[7] Allan, T., **CDMA, GSM and AMPS mobile network Technologies.** 1998. Disponível em: <http://www.apms.com.au/papers/cdma.html>. Acesso em: 26/08/2012.

[8] **Breaking point Systems** Disponível em: <http://www.breakingpointsystems.com>. Acesso em: 28/08/2012.

[9] Chang, D. **Security Along the Path Through GPRS Towards 3G Mobile Telephone Network Data Services.** SANS Institute – InfoSec Reading Room, 2002.

[10] **DriveTestBR** Disponível em: < http://drivetestbr.wordpress.com/>. Acesso em: 26/08/2012.

[11] Engel, J. Stanley **Advanced Mobile Phone System** Disponível em: <http://en.wikipedia.org/wiki/Advanced_Mobile_Phone_System>. Acesso em: 10/10/2012.

[12] Esteves, E., Swart H. **1x EV-DO (cdma2000).** 2004. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialcdma2000/default.asp>. Acesso em: 26/08/2012.

[13] Felix, Jose A. **Instrução Normativa GSI/PR nº 1.** 2008 Disponível em: <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. Acesso em: 27/08/2012.

[14] Gardezi, Ali I. **Security in Wireless Cellular Networls**. 2006. Disponível em: <http://cse.wustl.edu/~jain/cse574-06/ftp/CellularSecurity/index.html>. Acesso em: 14/09/2012.

[15] Harte, L., Bowler, D. **Introduction To Mobile Telephone Systems: 1G, 2G, 2.5G, and 3G Wireless Technologies and Services**. Ed. ALTHOS, 2004.

[16] Molva, R. **Mobile Network Security**. Institut Eurécom – France, 2005.

[17] **NBR ISO IEC 17799-2005**. Disponível em: <http://portal.cjf.jus.br/sigjus/arquivos-diversos/NBR-ISO-IEC-17799-2005.PDF/view>. Acesso em: 27/08/2012.

[18] **Networks and Telecommunications Research Group.** Disponível em: <http://ntrg.cs.tcd.ie>. Acesso em: 06/12/2012.

[19] Nguyen, T. **A survey of WiMAX security threats**, 2009. Disponível em: <http://www.cse.wustl.edu/~jain/cse571-09/ftp/wimax2/index.html>. Acesso em: 17/12/2012.

[20] Niemi, V. **LTE Security Architeture**. Nokia Research Center – Eurolab, Lausanne, Switzerland, 2010.

[21] Perez, D., Picó, J. **A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications.** 2011. Disponível em: <http://taddong.org>. Acesso em: 21/09/2012.

[22] Pizzol, A., Feltes, F., Hoescher, G., Voltz, J. **Segurança de Redes Sem Fio** 2011. Disponível em: <http://professor.unisinos.br/fkarl/arquivos/Apresentacao%20GA%20Seg%20Red%20Sem%20fio%20%281%29.ppt>. Acesso em: 03/07/2012.

[23] Poole, I. **LTE Security Authentication**. 2011. Disponível em: <http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/lte-security-authentication.php>. Acesso em: 06/12/2012.

[24] Poole, I. **5G Mobile Cellular Tecnology**. 2012. Disponível em: <http://www.radio-electronics.com/info/cellulartelecomms/5g-mobile-cellular/technology-basics.php>. Acesso em: 06/12/2012.

[25] Pütz, S., Schmitz, R., Martin T., **Security Mechanisms in UMTS.** 2001. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.6356&rep=rep1&type=pdf>. Acesso em: 12/10/2012.

[26] Rose, G**. A precis of the new attacks on GSM encryption** 2003. Disponível em: <https://opensource.qualcomm.com/assets/pdf/GSM_Attacks.pdf>. Acesso em: 14/11/2012.

[27] Sesia, S., Toufik, I., Baker, M. **LTE – the UMTS long term evolution: from teory to practice**. Segunda edição. Editora John Wiley & Sons Ltd, 2011.

[28] Silva, Erick F. R. **Rede GSM: Conceitos.** 2008. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredegsm/Default.asp>. Acesso em: 26/08/2012.

[29] Straccialano, André L. **Segurança em redes 3G – UMTS** 2008 Artigo CPQD. Disponível em: <www.wirelessbrasil.org/wirelessbr/artigos/seguranca-umts-geral.pdf>. Acesso em: 05/10/2012.

[30] Sverzut, José Umberto. **Redes GSM, GPRS, EDGE e UMTS: Evolução a caminho da terceira geração (3G)**. Primeira edição. São Paulo. Editora Érica, 2005.

[31] Teixeira, Edson R. D. **WiMAX** 2004. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialwimax/default.asp>. Acesso em: 29/10/2012.

[32] TELECO - **Tutoriais**. Disponível em: <http://www.teleco.com.br/tutoriais.asp>. Acesso em: 26/08/2012.

[33] **Telecommunications UK Fraud Forum**. Disponível em: <http://www.tuff.co.uk/home.asp>. Acesso em: 28/08/2012.

[34] Tude, E**. AMPS/TDMA (IS-136).** 2003. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialtdma/Default.asp>. Acesso em: 26/08/2012.

[35] Tude, E**. GSM.** 2003. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgsm/default.asp>. Acesso em: 26/08/2012.

[36] **WirelessBR**. Disponível em: <http://www.wirelessbrasil.org>. Acesso em: 25/08/2012.

[37] Yang, E. **A Survey of WiMAX and Mobile Broadband Security** 2009. Disponível em: <http://www.cse.wustl.edu/~jain/cse571-09/ftp/wimax1/index.html>. Acesso em: 21/01/2013.