UNIVERSIDADE ESTADUAL DO MARANHÃO
CENTRO DE CIÊNCIAS TECNOLÓGICAS
CURSO DE ENGENHARIA DE COMPUTAÇÃO

THIARLLESON SANTOS DE SOUSA

ANÁLISE DE VULNERABILIDADES DA REDE DE TELEFONIA MÓVEL GSM

SÃO LUÍS - MA
2018

THIARLLESON SANTOS DE SOUSA

ANÁLISE DE VULNERABILIDADES DA REDE DE TELEFONIA MÓVEL GSM

Monografia apresentada ao curso de Engenharia de Computação, como pré-requisito para a obtenção do Título de Bacharel em Engenharia de Computação, Centro de Ciências Tecnológicas - CCT, da Universidade Estadual do Maranhão - UEMA.

Orientador: Prof. Dr. Rogério Moreira Lima Silva

SÃO LUÍS - MA

2018

Sousa, Thiarlleson Santos de.
Análise de vulnerabilidades da rede de telefonia móvel GSM / Thiarlleson Santos de Sousa. – São Luís, 2018.
94 f.

Monografia (Graduação) – Curso de Engenharia de Computação, Universidade Estadual do Maranhão, 2018.

Orientador: Prof. Dr. Rogério Moreira Lima Silva.

1. GSM. 2. Segurança. 3. Vulnerabilidade. 4. Criptografia. I. Título.

CDU 004.056.55

THIARLLESON SANTOS DE SOUSA

ANÁLISE DE VULNERABILIDADES DA REDE DE TELEFONIA MÓVEL GSM

Monografia apresentada ao curso de Engenharia de Computação, como pré-requisito para a obtenção do Título de Bacharel em Engenharia de Computação, Centro de Ciências Tecnológicas - CCT, da Universidade Estadual do Maranhão - UEMA.

Trabalho aprovado. São Luís, 19 de Março de 2018:

Prof. Dr. Rogério Moreira Lima Silva
Orientador

Prof. Me. Jorge de Jesus Passinho e Silva
Avaliador

Prof. Dr. Leonardo Henrique Gonsioroski Furtado da Silva
Avaliador

SÃO LUÍS - MA

2018

Dedico a Deus primeiramente por me ter tirado do mau caminho e ter confiado em mim, quando ninguém o fazia. A minha família pela imensurável ajuda emocional, financeira, compreensão e incentivo a educação.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado forças para chegar onde estou e até onde chegarei futuramente. Aos meus familiares: meu pai, minha mãe e meu irmão por toda a ajuda imensurável, ao professor Passinho por me ajudar na realização deste trabalho, ao meu orientador por ter tido muita compreensão e paciência, e finalmente ao grupo de amigos "suricates" pelos momentos de descontração e por me ajudar a crescer profissionalmente e pessoalmente, tenho certeza que se não fosse por este grupo, eu não estaria aqui.

“Quando estiver no fundo do poço, lembre-se que há uma mola que te levará para cima, onde ninguém jamais foi.” (Autor Desconhecido)

RESUMO

Este trabalho faz uma análise acerca das vulnerabilidades da rede de telefonia móvel GSM (Sistemas Global para Comunicações Móveis), as quais estão amplamente documentadas e conhecidas pela comunidade segurança. Neste estudo, utilizou-se a pesquisa bibliográfica, contemplando uma breve história da telefonia móvel, principais conceitos de funcionamento, interfaces, protocolos, modelo de segurança, *softwares* e *hardwares* específicos para exploração, contexto histórico em que este padrão foi concebido e os motivos que fizeram a segurança do mesmo encontrar-se vulnerável atualmente. Por conseguinte, essa temática viabilizará formas de prevenir ou mitigar os ataques as redes GSM.

Palavras-chave: GSM. Segurança. Vulnerabilidade. Criptografia.

ABSTRACT

This work makes an analysis about the vulnerabilities of mobile network GSM (Global Systems for mobile communications), which are widely documented and known by the security community. In this study, we used a literature search, including a brief history of mobile telephony, core concepts, interfaces, protocols, security model, software and hardware specific to exploration, context history in which this pattern is designed and the reasons that have made safety meet vulnerable currently. Therefore, this theme will enable ways to prevent or mitigate the attacks the GSM networks

Keywords: GSM. Security. Vulnerability. Encryption.

LISTAS DE ILUSTRAÇÕES

LISTAS DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AMPS	*Advanced Mobile Phone System*
AuC	*Authentication Center*
ARFCN	*Absolute Radio Frequency Channel Numbers*
BSS	*Base Station System*
BTS	Estação Transceptora Base
CBC	*Cipher Block Chaining*
CC	*Call Control*
CDMA	*Code Division Multiple Access*
CM	*Call Management*
ECB	*Electronic CodeBook*
EIR	*Equipment Identity Register*
ESN	*Eletronic Serial Number*
ETSI	*European Telecommunications Standards Institute*
FDD	*Frequency Division Duplex*
FDMA	Múltiplo Acesso por Divisão de Frequência
FHMA	*Frequency Hopped Multiple Access*
GMSK	*Gaussian Minimum Shift Keying*
GPRS	*General Packet Radio Service*
GSM	Sistema Global para Comunicações Móveis
HLR	*Home Location Register*
IMEI	*International Mobile Equipment Identity*
IMSI	*International Mobile Subscriber Identity*

LAC	*Location Area Code*
LAI	*Location Area Identification*
LCH	*Logical Channel*
MCC	*Mobile Country Code*
ME	Equipamento Móvel
MIN	Identidade do Aparelho
MNC	*Mobile Network Code*
MS	Estação Móvel
MSC	*Mobile Switching Center*
NSS	*Network Switching System*
OTP	*One-time pad*
PABX	*Private Automatic Branch Exchange*
PHC	*Physical Channel*
PIN	*Personal Identity Number*
PUK PIN	*Unblocking Key*
SIM	*Subscriber Identity Module*
SMS	*Short Message Service*
SS	*Supplementary Services*
TDMA	Acesso Múltiplo por Divisão de Tempo
TMSI	*Temporary Mobile Subscriber Identity*
UIT	União Internacional de Telecomunicações
USRP	*Universal Software Radio Peripheral*
VLR	*Visitor Location Register*
VoIP	*Voice over Internet Protocol*

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

Com o advento da telefonia móvel em 1979 nos Estados Unidos e posteriormente na Europa, constatamos uma grande revolução no mundo, as pessoas foram adquirindo aparelhos móveis (celulares) e realizando chamadas de voz com uma qualidade razoável, tanto para telefones fixos e celulares. Sendo internacionalmente conhecida como a 1ª geração (1G), esta tecnologia utilizava a comutação por circuito e FDMA[1], sua padronização oficial foi chamada de AMPS[2].

No Brasil , segundo o relatório da (ANATEL, 2006) o AMPS em 2006 possuía apenas 61.462 acessos, o que equivale a 0,06% do total de acessos de todo o Brasil, sendo que esta tecnologia chegou em 1991 trabalhando na frequência de 800 MHZ, contudo as operadoras que trabalham com a tecnologia AMPS no Brasil teriam que migrar para as gerações 2G e 3G até o dia 31 de junho de 2008 pressionadas pela Anatel. Desativando obrigatoriamente as redes AMPS, o espectro de frequência após isso, seria utilizado em outras tecnologias mais modernas tal como o 2G ou 3G.

O padrão AMPS mesmo sendo um padrão pioneiro, já implementava o *handoff*[3] e *roaming*[4] (pouco funcional), todavia a rede apresentava várias limitações que não permitiam a sua massificação: era essencialmente analógico, incompatibilidade de sistemas entre os países, nenhum tipo de criptografia, pouca escalabilidade e só servia para trafegar voz. A evolução era algo natural e imprescindível, e assim entraríamos na 2ª geração das redes móveis (2G).

Uma nova geração da telefonia móvel deveria suprir a falta de padronização e incompatibilidade da geração anterior. O aparelho celular além de ser demasiadamente grande só funcionava no seu país de origem e o *roaming* parecia está longe de ser plenamente funcional. Como os sistemas eram todos isolados e a demanda por estes serviços só aumentava, isto começou a preocupar a todos os envolvidos, conscientes dos problemas que

---

[1] FDMA - Acesso múltiplo por divisão de frequência.

[2] AMPS - *Advanced Mobile Phone System*.

[3] *Handoff* - É o procedimento empregado em redes sem fio para tratar a transição de uma célula para outra de forma transparente ao utilizador.

[4] *Roaming* - Designa a capacidade de um usuário de uma rede para obter conectividade em áreas fora da localidade geográfica onde está registrado.

viriam a seguir. A rede móvel era muito limitada devido à circunstância de ser analógica e logo viria a não suportar mais o crescente número de usuários.

Os custos para a pesquisa e desenvolvimento desta nova geração de rede móvel eram exorbitantes, desencadeando assim a cooperação entre fabricantes e operadores a criar um sistema global e bem padronizado. Expandir a produção deste sistema único e assim reduzir os custos seria a única saída. Em 1982 foi criada a CEPT (*Conférence des Administrations Européenes des Postes et Télécommunications*), uma organização composta pelas operadoras públicas de 26 países europeus. Os membros que compunham esta organização eram empresas estatais, que tinham posição de monopólio. A CEPT criou o GSM (*Group Spéciale Mobile*), o que mais tarde iria se tornar *Global System For Mobile Communications* sem nenhuma mudança na sigla) com o intuito de criar um sistema único com *roaming* internacional, capaz de operar com milhões de usuários em toda a Europa. Este grupo enfrentou o ceticismo da indústria, problemas políticos, técnicos e econômicos. Eles consideravam de extrema relevância os seguintes requisitos:

- Boa qualidade de serviço;
- Terminais e serviços baratos;
- Roaming internacional;
- Possibilidade de utilização de terminais portáteis;
- Poder suportar futuros novos serviços;
- Eficiência de espectro.

A proposta inicial era que esse padrão operasse na frequência de 900 MHz, utilizando de modo eficiente o espectro de frequência com uma alta qualidade de transmissão assim possibilitando mais chamadas. O sistema também deveria fornecer chamadas seguras e a transmissão de dados.

Apesar desta evolução das redes móveis serem de extrema relevância, ainda dependia da boa vontade política, somente em 1984 depois do inicio do congestionamento das redes analógicas é que a **Comissão Europeia** deu o apoio formal ao GSM, e isto foi muito importante e decisivo para os próximos passos.

Alemanha, Itália e França assinaram um tratado de desenvolvimento do GSM. No evento Telecom, ocorrido em 1991, realizado pela UIT[5] em Genebra, foi lançado a primeira versão do novo padrão e demonstrada com sucesso. Era compatível com a rede fixa digital européia (ISDN), oferecia resistência a interferências e era capaz de prover o *roaming* internacional (um dos requisitos mais importantes), possibilitando o livre trânsito dos cidadãos entre todos os países europeus, como discorre (TELECO, 2017). O sistema seria totalmente aberto, não proprietário, de forma a prevenir o monopólio dos fabricantes em função do fornecimento. Serviços de dados (como o SMS) poderiam ser implementados pelas operadoras já na primeira versão do GSM e posteriormente o MMS também (TELECO, 2017).

A Europa começou a aprimorar as suas redes GSM no final do ano de 1992, quando um grande número de aparelhos celulares chegou ao mercado e antiga geração já estava congestionada, assegurando o funcionamento totalmente compatível, continental e sem prejudicar a rede. Novas faixas de frequências foram definidas em 1800 MHz para realizar um maior número de operações GSM em cada país, o que fez o GSM operar em duas frequências não conflitantes, isso acabou dando um impulso ainda maior ao uso da tecnologia. O GSM logo percorreu o mundo, sendo implementado progressivamente na Austrália, no Oriente Médio, na África e em grande parte da Ásia entre outros.

O GSM deixara de ser um padrão europeu, para se tornar, de fato, um padrão internacional o qual foi projetado, tamanho foi o sucesso que em 2000 já tinham mais de 4 milhões e 930 mil assinantes segundo (ANACOM, 2000). As grandes exceções na adoção do GSM ficaram por conta do Japão e da Coréia do Sul. (TELECO, 2017) O Japão decidiu incentivar a sua própria indústria, adotando o padrão doméstico PDC[6]. A Coréia do Sul escolheu o CDMA[7] pois era uma oportunidade de desenvolver a sua indústria de comunicações móveis nacional (seguindo o mesmo rumo protecionista do Japão).

Vale ressaltar que o GSM apresenta um grau muito maior de segurança do que o sistema anterior, pois com o advento do cartão SIM[8], o supracitado ficou responsável pela autenticação e criptografia utilizada entre o MS[9] e a BTS[10], em contrapartida o AMPS não

[5] UIT - União Internacional de Telecomunicações.
[6] PDC - *Personal Digital Cellular*.
[7] CDMA - Tecnologia do 2G concorrente ao GSM, *Code Division Multiple Access*.
[8] SIM - São pequenos chips que guardam todas as informações do proprietário do telefone.
[9] MS - Estação Móvel refere-se ao aparelho celular com cartão SIM.

tem nenhum sistema de criptografia, então todos os dados eram expostos em texto claro e bastava um equipamento específico para operar a recepção e demodular os sinais FM e assim quebrar o sigilo de qualquer ligação (PAULA; BRESSAN; ABE, 2013, p. 7).

Outro problema a ser abordado e mitigado pelo GSM era a clonagem de aparelhos:

> Os celulares possuem uma senha única, composta pelo número da linha somada a mais um código do aparelho. Essa combinação é chamada de ESN. Quando o celular é ligado, a senha é transmitida para autenticar o celular na rede. Dessa forma, o celular saberá qual a ERB será utilizada para se comunicar. Para a busca por aparelhos que estejam utilizando a rede AMPS é utilizado o scanner de frequência. Dessa forma, irá conseguir a senha única (ESN[11]) do aparelho e irá transferir os dados para um aparelho celular (geralmente roubado) para completar o ataque. A clonagem de números se mostra mais bem-sucedida em aparelhos que contam com a tecnologia CDMA, e, embora também afete dispositivos com a tecnologia GSM, se mostra muito mais rara nesse caso. A tecnologia digital, utilizada nos três sistemas (TDMA, GSM e CDMA), possui mais recursos para garantir a privacidade do usuário. Enquanto os aparelhos CDMA contam com um número serial eletrônico (ESN) e um número de identificação móvel (MIN[12]), aqueles com a tecnologia GSM são identificados somente pelo IMEI (Identificação Internacional de Equipamento Móvel), número de identificação global e único para cada celular, que se mostra um grande obstáculo aos falsários. (ANATEL, 2007).

Enfim, a segunda geração da rede de telefonia, nasceu de uma grande ambição mundial e foi considerada um sucesso em todo mundo, praticamente alavancou vários progressos. Aparelhos menores, ligações de alta qualidade de voz, introdução da tecnologia SMS e a utilização de criptografia, revolucionaram o mundo de uma forma até então nunca vista antes.

1.2 Motivação

Diante dos fatos que afirmam que no Brasil o número de usuários que utilizam a rede 2G ainda é muito alto, mesmo registrando quedas a cada ano, vide a Tabela 1 e Tabela 2, se relaciona por diversos fatores enumerados a seguir: o país tem uma grande extensão territorial e uma grande burocracia como afirma (PAIVA, 2009), ademais há muitos celulares antigos ainda em uso que não suportam tecnologias mais atuais como 3G ou 4G como disse (NOHL, 2009), falhas de operação nas BTSs que suportam os padrões 3G ou 4G fazem o aparelho móvel operar em 2G, a configuração errada nos aparelhos também podem fazer o aparelho operar na supracitada, e por fim quando o usuário está em *roaming* ele poderá estar vulnerável

---

[10] BTS - Estação Transceptora Base.

[11] ESN - *Eletronic Serial Number*, ou seja, Número Serial Eletrônico. É um número atribuído a cada estação móvel no momento de sua fabricação.

[12] MIN - A MIN é a identidade do aparelho, possui 34 *bits* binários para 10 números decimais de telefone ou 24 *bits* para telefone com 8 dígitos, como é no Brasil.

pelo seguinte motivo: um usuário apto para utilizar o 3G está fora de sua rede, então a operadora visitante pode forçar o usuário a utilizar a rede em um padrão inferior como o 2G.

Tabela 1- Cobertura das operadoras e suas tecnologias oferecidas

Ago/17	Municípios			% População Coberta		
	2G	**3G**	**4G**	**2G**	**3G**	**4G**
Vivo	**4.179**	**3.974**	1.762	93,8%	**92,2%**	74,1%
TIM	3.461	2.926	**2.186**	91,5%	85,1%	**77,1%**
Claro	4.162	3.296	1.221	**95,4%**	90,5%	73,1%
Oi	3.410	1.198	284	89,0%	72,2%	55,1%
Nextel	-	410	10	-	47,2%	5,1%
Algar	106	87	14	2,1%	1,5%	1,0%
Sercomtel	2	2	-	0,3%	0,3%	-
Total	**5.570**	**5.091**	**3.039**	**100,0%**	**98,7%**	**87,5%**

Fonte : (TELECO, 2017)

Tabela 2 - Crescimento de tecnologias móveis

Milhares	Dez/16	Agosto de 2017			
		Nº Celulares		Cresc. mês	Cresc. ano
GSM	**47.627**	37.545	15,5%	-1.501	-10.082
3G (WCDMA)	**119.101**	98.442	40,7%	-2.822	-20.659
LTE	**60.104**	88.504	36,5%	4.391	28.399
CDMA	**0,919**	0,507	-	0	-0,412
Total Terminais de Dados	**17.234**	17.677	7,3%	88	443
- Term. Dados Banda Larga	4.499	3.455	1,4%	-144	-1.044
- Term. Dados M2M	12.735	14.222	5,9%	232	1.487
M2M Especial	5.447	5.923	2,4%	-309	476
M2M Padrão	7.288	8.299	3,4%	541	1.011
Total	**244.067**	**242.168**	**100,0%**	**156**	**-1.899**

Fonte : (TELECO, 2017)

Em contrapartida a essa evolução das redes móveis, também houve progressos no *software* e *hardware* aos longos dos anos, por exemplo: CPUs cada vez mais potentes, as GPUs que começaram a serem utilizadas como fonte de processamento chegando até ser superior a CPU e o crescimento cada vez maior da computação em nuvem que fornecem um processamento gigantesco, alta disponibilidade de largura de banda e redundância, tudo isso a

preços acessíveis. Estes servidores foram sendo utilizados em muitas das vezes para fins nada éticos como a "quebra" da criptografia por meio de ataques de força bruta e dicionários.

Outro fator preocupante é a segurança do GSM, que utiliza a família de criptografia denominada **A5** que utiliza uma chave de sessão de 64 *bits* (considerada pequena para os padrões atuais) e tem como principal segurança a **obscuridade** (um método ineficiente de segurança) e para piorar ainda mais, vários testes de exploração foram bem sucedidos há muito tempo, por exemplo, (NOHL, 2009) conseguiu com um *hardware* de baixo custo o **USRP**[13] executar vários tipos de ataques à rede GSM como: homem do meio, quebra da criptografia, falsificação de BTS e negação de serviços em BTS.

Além do fato de que o algoritmo de criptografia A5 foi explorado e armazenado todas as informações sobre as transformações do algoritmo, em *Rainbow Tables*[14] de 2 TB, que são utilizadas para diminuir o fator computacional requerido e descobrir a chave de sessão (NOHL, 2010).

(NOHL, 2009), diretor do *Security Research Labs*, na Alemanha, um dos mais conhecidos especialistas em segurança de celulares, fez um alerta bastante preocupante:

> Hackers podem invadir celulares que possuem a tecnologia usada por cerca de 80% dos aparelhos móveis do mundo, a GSM. Os criminosos virtuais podem programar o telefone para que ele faça ligações ou envie SMS para números que cobram tarifas adicionais, embolsadas pelos próprios hackers. Assim que o ataque é realizado, os *hackers* eliminam o número do ataque para que não haja interceptação. Esse problema, muito comum em países da Europa Ocidental, África e Ásia, só é detectado quando o proprietário do celular vai efetuar o pagamento da conta. E, quem tem que bancar o prejuízo são as operadoras de telefonia, mesmo que seja apenas parcialmente.

Constatamos então, a fragilidade do modelo de segurança do GSM que apesar de inovar com a utilização de criptografia, com o passar dos anos ficou obsoleta e vulnerável já em 2009. E esta insegurança na telefonia móvel vem sendo bastante negligenciada por organizações de telecomunicações, governos e usuários apesar das inúmeras demonstrações de exploração. E ainda possuímos o agravante que o custo de *hardware* necessário para a exploração ficou mais barato e muito mais acessível.

As operadoras também não demonstram preocupação com a segurança posto que historicamente as empresas não investem o suficiente em segurança da informação

---

[13] USRP - *Universal Software Radio Peripheral*.
[14] *Rainbow Tables* - Tabela que armazena uma grande quantidade de *hashes*.

(SANT'ANNA, 2017) e ainda tem o fator custo, devido ao investimento para transferir todas as redes para 3G seria praticamente inviável para um país de tamanho continental como o Brasil e por conseguinte os aparelhos antigos se tornariam obsoletos fazendo com que muitos usuários comprassem telefones compatíveis com as novas gerações das redes móveis.

Embora autores como (CASAROTTO, 2000, p. 89) afirmam que seria menos custoso investir em equipamentos ou tecnologia melhores do que retardar e procrastinar o investimento a novas tecnologias. Vejamos em detalhes o que foi dito:

> Constatou-se que muitas empresas brasileiras (provavelmente a maioria) têm o costume de manter os equipamentos velhos em funcionamento, mesmo quando sua operação não é mais economicamente viável. As despesas de manutenção em geral superam em muito o valor dos investimentos. Acredita-se que existe atualmente no Brasil um potencial enorme de redução de custos simplesmente desfazendo-se de equipamentos obsoletos com tempos de operação muito elevados ou produzindo fora das especificações. Acredita-se que as empresas não fazem as substituições que deveriam fazer por causa de um comodismo administrativo: as decisões de substituição não chegam a ser cogitadas, pois o estilo administrativo dominante ainda é o de resolver os problemas só em último caso, e não se antecipar a eles. As empresas preferem os bombeiros às soluções mais racionais.

Diante dos vários motivos citados anteriormente este trabalho tem como a motivação demonstrar perante a sociedade e conscientizá-la sobre as vulnerabilidades da rede GSM, pois já foram feitos inúmeros testes por vários profissionais já citados, relatando a fragilidade da segurança da supracitada. Então advém dos motivos citados que este presente trabalho identificou a seguinte formulação da questão de pesquisa:

Quais são as vulnerabilidades existentes da rede móvel GSM, como analisá-las e preveni-las?

1.3 Os Objetivos

O objetivo primordial deste trabalho resume-se a explicar o funcionamento da rede GSM, seu modelo de segurança, as vulnerabilidades existentes, seus protocolos e apresentar meios de mitigação ou prevenção dos ataques. A partir do objetivo geral foram elaborados os seguintes objetivos específicos:

- Entender o funcionamento básico da infraestrutura do GSM;
- Estudar o modelo de segurança do sistema GSM;

- Refletir sobre as causas que fizeram a segurança do mesmo, apresentar-se atualmente obsoleta;
- Analisar as principais vulnerabilidades da rede GSM e os meios de exploração;
- Apresentar meios de mitigação e prevenção dos ataques conhecidos.

1.4 Metodologia

A metodologia deste trabalho foi elaborada por meio da pesquisa bibliográfica, que se fundamenta no intuito de levantar um conhecimento disponível sobre teorias, a fim de analisar, produzir ou explicar um objeto sendo investigado. A pesquisa bibliográfica visa então analisar as principais teorias de um tema, e pode ser realizada com diferentes finalidades (CHIARA, 2008).

O referencial teórico foi obtido por meio de artigos, monografias, estatísticas da ANATEL, congressos de segurança da informação, relatórios de profissionais de segurança especialistas na área, relatórios técnicos da organização responsável pela padronização do GSM (ETSI, 2017), entre muitos outros.

Para o desenvolvimento do trabalho foram consideradas as seguintes etapas:

- Estudo da literatura da rede GSM;
- Estudo da segurança (autenticação e criptografia);
- Estudo dos ataques documentados por diversos profissionais de segurança, que foram bem sucedidos ao explorar as vulnerabilidades da rede GSM;
- Apresentar meios de mitigação e de prevenção das vulnerabilidades.

1.5 Organização do TCC

Este presente TCC é composto por 4 capítulos. Organizado de forma a promover uma sequência lógica, o capítulo 1 trata da contextualização, motivação, objetivos e a metodologia do cerne da questão deste trabalho.

A seguir no capítulo 2, a fundamentação teórica fornece todo o embasamento teórico para a compreensão do objetivo central do TCC. O capítulo 3 apresentou a parte mais técnica,

apresentando as vulnerabilidades existentes no sistema GSM. Neste mesmo capítulo, os meios de mitigação tiveram ênfase.

O capítulo 4 apresentou as conclusões no tocante ao sistema GSM. E por fim os trabalhos futuros foram apresentados.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Sistema Global para Comunicações Móveis

O GSM continua sendo um dos sistemas de telefonia mais utilizados no mundo (MIRO, 2006) e no Brasil (vide a Tabela 1), e é o padrão vencedor da 2ª geração da telefonia móvel superando o TDMA e o CDMA por diversos fatores como:

Em suma o GSM trouxe diversas novidades como:

- Maior eficiência na utilização do espectro;
- Melhora significativa na ligação de voz;
- Possibilidade de envio de SMS;
- *Roaming* internacional;
- Identificação de chamadas;
- Serviços de mensagem multimídia;
- Melhor atendimento das futuras necessidades de espectro;
- Maior segurança com o cartão SIM que ficara responsável pela autenticação e encriptação na rede;
- Conveniência, pois permite que o chip do celular possa ser usado em qualquer outro aparelho GSM, exceto aos que estão bloqueados;
- Dificuldade na clonagem de aparelhos.

Inicialmente a sua frequência foi definida em 900 MHz, porém com o crescimento rápido, outras bandas foram utilizadas para a alocação como 1800 MHz, destacamos abaixo as fases do desenvolvimento do GSM:

- Na primeira fase foi dado ênfase nos serviços básicos de telefonia móvel, por exemplo: voz, *roaming* internacional, serviços básicos de dados, bloqueio de chamada, encaminhamento de chamadas e SMS;
- Na segunda fase alguns serviços novos foram implementados na tecnologia, como: aviso de cobrança, chamada retida, identificador de

chamadas, chamada em espera e comunicação de dados adicional o GPRS[15];

- Na terceira e última fase os serviços de plano de números privados e serviços fax foram incorporados à tecnologia, além de iniciar a utilização da banda de 1800 MHz.

Sendo administrado pelo ETSI (*European Telecommunications Standards Institute*) o GSM possui grande parte de suas especificações e tecnologias divulgadas no próprio site (ETSI, 2017). Contudo informações referentes á segurança foram omitidas e seus respectivos algoritmos criptográficos foram desenvolvidos e mantidos em segredo, o que se demonstrou ser um dos piores tipos de segurança para prevenir o vazamento dos algoritmos. (WYKES, 2016, p. 89) disse em seu livro.

> Infelizmente a história dessa cifra é um exemplo clássico de como não fazer um produto seguro. O projeto dessa cifra foi classificado como secreto, sendo liberado apenas para os fabricantes de equipamentos ou componentes para celulares. No entanto, após uma série de vazamentos parciais e um excelente trabalho de engenharia reversa, foi identificado um número de fraquezas criptográficas na cifra. Com certeza não existiriam tantas vulnerabilidades no GSM se o projeto das cifras estivesse sido publicado e submetido ao escrutínio criterioso da comunidade criptológica internacional. Por outro lado, há de se reconhecer que a inclusão de uma cifra fraca no padrão GSM pode ter auxiliado, em muito, o trabalho das organizações de segurança e inteligência.

Apesar de problemas na segurança, o padrão era considerado o mais seguro e eficiente naquele contexto. O GSM inovou com o padrão digital que veio para substituir o analógico e resolver o problema mundial de conectividade e realmente foi um marco na história. Com a sua especificação aberta, o GSM rompeu barreiras, foi implementado em quase todo mundo e serviu de precedente para as redes móveis mais modernas.

2.1.1 Arquitetura da Rede GSM

A arquitetura do GSM divide-se na prática em duas camadas, respectivamente: *Switching System* (SS) ou *network Switching System* (NSS), e *Base Station System* (BSS) ou *access network* (rede de acesso) como está demostrado na Figura 1, vale ressaltar que alguns

[15] GPRS - *General Packet Radio Service*.

autores como (CARLÉSIMO, 2013, p. 24) define como a divisão em três partes: a MS, o BSS e o NSS.

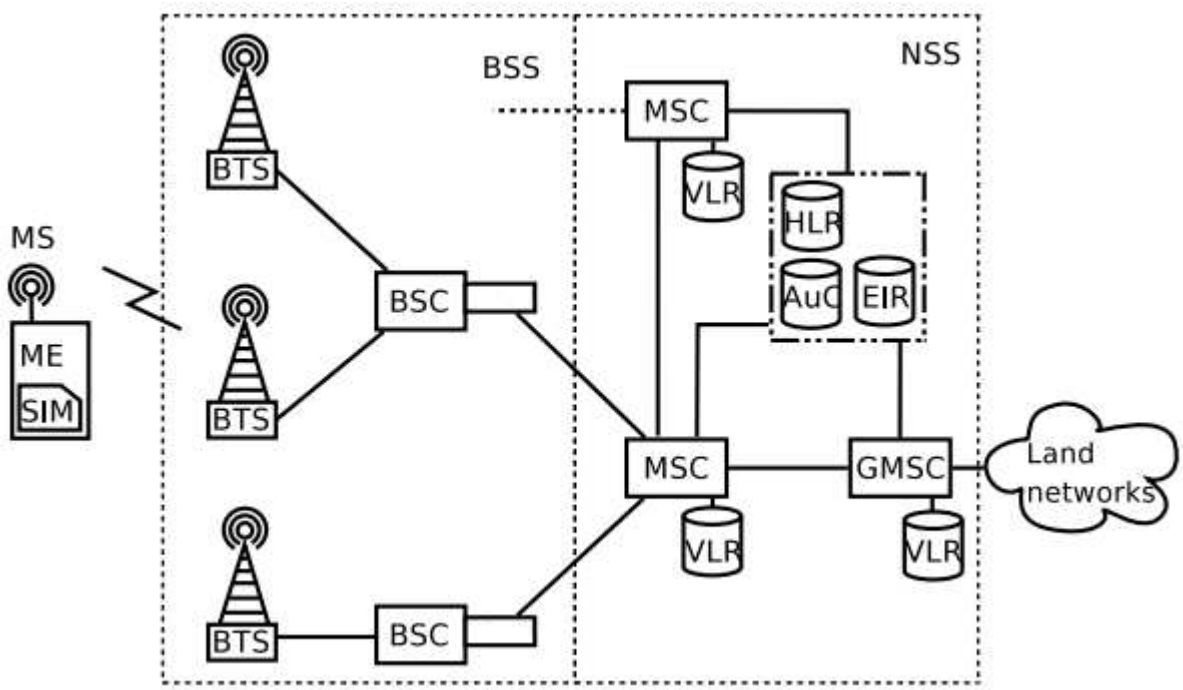

Figura 1 - Arquitetura simplificada GSM
Fonte: (BROEK, 2010)

Nos próximos subcapítulos, vamos entrar em especifico sobre a definição do componente e sua função exercida.

2.1.2 Identificação do Usuário na Rede GSM

O padrão GSM utiliza conceitos importantes para a identificação de usuários na rede, como mostra a seguir.

***Mobile Service ISDN Number* (MSISDN)**

Trata-se do número real e discado do assinante. É concedido na hora da compra e gravado no cartão SIM. É composto pelos seguintes elementos:

$$\mathrm{MSISDN} = \mathrm{CN} + \mathrm{NDC} + \mathrm{SN}$$

Onde os elementos são:

- CC, *Country Code* (código do país), no BRASIL é 55;
- NDC, *National Destination Code* (código nacional de destino);
- SN, *Subscriber Number* (número de assinante), é o número propriamente discado.

***International Mobile Subscriber Identity* (IMSI)**

Quando o assinante móvel, contrata o serviço de uma operadora uma identificação de 15 dígitos única e sigilosa é fornecida, e essa identificação é gravada no cartão SIM e também no HLR[16]. É composto pelos seguintes elementos:

$$\mathrm{IMSI} = \mathrm{MCC} + \mathrm{MNC} + \mathrm{MSIN}$$

Onde os elementos são:

- MCC, Mobile Country Code (código do país do celular);
- MNC, *Mobile Network Code* (código da rede celular);
- MSIN,*Mobile Subscriber Identification Number* (número de identificação do assinante móvel).

***Temporary Mobile Subscriber Identity* (TMSI)**

A Identidade Temporária de Assinante Móvel (TMSI) é a identidade que realmente trafega entre o celular e a rede. TMSI é atribuído aleatoriamente pelo VLR a cada celular na área, no momento em que é ligado, e armazenado no SIM, dentro da memória volátil. O número depende da área de localização e por este motivo, o TMSI está sempre associado a uma determinada LAI[17], portanto, deve ser atualizado sempre que o celular se move para uma nova área geográfica[18] (CARLÉSIMO, 2013, p. 26).

---

[16] HLR - Base de dados de assinantes na operadora.
[17] LAI - *Location Area Identification*.
[18] MSC - *Mobile Switching Center*.

Isso dificulta o rastreamento do celular, contudo só é eficiente caso o atacante não tenha escutado o processo inicial de associação de um TMSI ao IMSI, o qual ocorre quando o MS é ligado pela primeira vez. A rede também pode alterar o TMSI do celular a qualquer momento. E normalmente faz isso, para evitar que o assinante seja identificado e rastreado por “espiões” na interface de rádio.

2.1.3 Estrutura Geográfica da Rede

“O sistema de telefonia móvel celular é baseado na divisão de áreas geográficas, denominadas células. Cada célula pode ser representada pela área que a ERB opera, a qual provê a cobertura propriamente dita e utiliza o reuso de frequências, técnica aplicada para transmissão de sinais com a mesma frequência em estações distintas” (RODRIGUES; COSTA, 2000).

A célula é um dos pilares da rede de celular, ela é delimitada pela capacidade física da ERB. A primeira ideia concebida sobre células é que elas são circulares, mas na verdade estas são representadas por hexágonos, o que elimina a área de sombra quando sobrepostas umas às outras e aperfeiçoa a área de cobertura.

A Figura 2 abaixo mostra o formato hexagonal das células e como são alocadas e também o reuso de frequências de fator 7 (sete), embora a GSM utilize normalmente fator de reuso 9 e 12 (SANTOS, 2008).

Formando um conjunto de células, cada célula com uma frequência diferente, mas que podem ser repetidas em outros conjuntos sem interferências ou outro tipo de prejuízo (se for bem planejado). Isto economiza recursos de banda da rede, porém pode causar interferências se não for disposto de maneira correta, portanto um bom planejamento de frequências pode diminuir bastante estes problemas que possam acontecer (FOROUZAN, 2008).

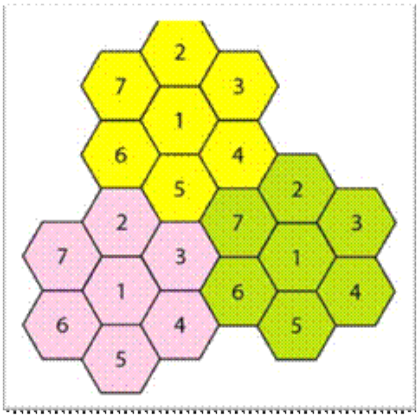

Figura 2 - Células e reuso de frequência fator 7
Fonte: (FOROUZAN, 2008)

Identificação da Área de Localização - *Location Area Identity* (LAI)

Cada rede GSM é subdividida em áreas de localização identificadas por um LAI exclusivo dentro da rede. LAI é o nome dado a um conjunto de células, tipicamente, ela contém 30 células. Este número consiste no MCC, MNC e um *Location Area Code* (LAC).

$$\mathrm{LAI} = \mathrm{MCC} + \mathrm{MNC} + \mathrm{LAC}$$

Onde os elementos são:

- MCC, *Mobile Country Code* (código do país do celular);
- MNC, *Mobile Network Code* (código da rede celular);
- LAC, *Location Area Code* (código local da operadora).

A LAC é um número de comprimento máximo de cinco dígitos que identifica uma área de localização dentro de um PLMN. Isso é usado como uma referência única para a localização atual de um assinante. A área de localização é ainda dividido em células, sendo cada uma identificada de maneira exclusiva por um identificador de célula (***Cell ID***).

Uma estação móvel (por exemplo, telefone celular) reconhece o LAI e o armazena no cartão SIM. Se a estação móvel estiver em movimento e perceber uma mudança de LAI, ela emitirá uma solicitação de atualização de localização, informando desse modo o provedor móvel de seu novo LAI. Isso permite que o provedor localize a estação móvel em caso de uma chamada recebida.

Rede PLMN

Um PLMN é identificado pelo *Mobile Country Code* (MCC) e pelo *Mobile Network Code* (MNC). Os PLMNs se interconectam com outros PLMNs e redes telefônicas públicas comutadas (PSTN[19]) para comunicações telefônicas ou com provedores de serviços de internet para dados e acesso à Internet.

O objetivo geral de um PLMN é facilitar a comunicação sem fio e interligar a rede sem fio com a rede fixa com fio. O PLMN foi especificado pelo ETSI seguindo suas especificações GSM.

Rede GSM

"É o conjunto de todas as PLMN's espalhadas no mundo, ou seja, é a área total onde existe cobertura GSM. Desta forma, pode-se dizer que todas as PLMN's compõem a rede GSM" (SILVA, 2013).

2.2 Estação Móvel - *Mobile Station* (MS)

A estação móvel (MS) é o equipamento do usuário na rede. A estação é composta por duas entidades, o Equipamento Móvel (ME) que representa o telefone em si e o *Subscriber Identity Module* (SIM), na forma de um cartão inteligente contido dentro do telefone.

2.2.1 Equipamento Móvel (ME)

Os ME's são independentes dos provedores de redes. A identidade do assinante é obtido a partir do SIM que deve ser inserido no MS para fazê-lo funcionar. No caso da MS estar desprovida do Cartão SIM não estará associada a nenhum usuário, não podendo efetuar nem receber chamadas. Apenas chamadas de emergência são possíveis.

Cada equipamento móvel tem um número de identificação chamado identidade internacional do equipamento móvel (*International Mobile Equipment Identity* - IMEI), para obter esta identificação do ME basta discar o seguinte código ***#06#**. Estas identificações são

[19] PSTN - É o termo usado para identificar a rede telefônica mundial comutada por circuitos destinada ao serviço telefônico. Inicialmente foi projetada como uma rede de linhas fixas e analógicas porém atualmente é digital e inclui também dispositivos móveis como os telefones celulares.

armazenadas no (*Equipment Identity Register* - EIR) que será estudado em breve, todavia informamos que com este número é possível bloquear as funções de rede do aparelho gravando o IMEI numa ***blacklist*** compartilhada entre as operadoras.

O IMEI é composto por 15 dígitos decimais com os seguintes elementos:

$$\text{IMEI} = \text{TAC} + \text{FAC} + \text{SNR} + \text{DIGITO VERIFICADOR}$$

Onde os elementos são:

- TAC (*Type Approval Code*), um código de 6 dígitos;
- FAC (*Final Assembly Code*), com 2 dígitos, identificando o local de fabricação;
- SNR (*Serial Number*), com 6 dígitos, representando cada equipamento produzido em um TAC e FAC;
- Digito para a verificação.

2.2.2 Módulo de Identidade do Assinante (SIM)

Uma das inovações que o GSM trouxe para a segurança é justamente o SIM, responsável pela autenticação, métodos de bloqueio entre outros. A definição segundo (SANTOS, 2008):

> Esse módulo consiste em um cartão inteligente (*smart card*) que carrega informações essenciais para a identificação do assinante. É um chip que se conecta ao telefone celular. O processamento dos serviços e suas tarifações são realizados a partir das informações contidas nesse chip, e não no aparelho celular. Sendo assim, o assinante pode retirar seu chip, encaixar em outro aparelho e realizar uma chamada com seu próprio número, o que será tarifado em nome do dono do chip e não o do aparelho.

Caso o usuário queira uma maior segurança em casos como o roubo do SIM, poderá usar o PIN (*Personal Identity Number*) que é uma senha de quatro a oito dígitos. O PIN é armazenado no cartão SIM e serve como senha pessoal. O PIN vem desabilitado para que o usuário utilize normalmente o aparelho. Antes de ser personalizada essa senha geralmente é a mesma para todos os chips de uma mesma operadora, por isso é recomendável que esta senha seja alterada (UFF TELECOM, 2012).

Se um PIN incorreto for introduzido três vezes consecutivas, o cartão fica bloqueado, e só pode ser utilizado o *reset* com um código de oito dígitos denominado PUK (*PIN*

Unblocking Key) que também fica armazenado no SIM. Caso este número também seja digitado de forma errada por 10 vezes, o SIM será inutilizado e o único jeito é a ida do usuário à operadora para resgatar o número em um novo chip (CARLÉSIMO, 2013, p. 28) (TIM, 2014).

Os Chips GSM também implementam o PIN2 em conjunto com o PUK2. Através do PIN2 é possível configurar o cartão SIM para desbloquear o PIN e efetuar funções específicas definidas pela operadora móvel, como efetuar ligações somente para os números pré-definidos pelo usuário. O PUK2 funciona para o PIN2 da mesma maneira que o PUK funciona para o PIN (UFF TELECOM, 2012).

O SIM contém um sistema operacional, arquivos de sistema e aplicativos. O *hardware* inclui uma CPU de 8 *bits*, 16K de memória ROM[20], 256 *bytes* de RAM[21] e 4K de EEPROM[22] (STEPANOV, 2013). Suas demais características são padronizadas segundo (ISO/IEC, 2013).

De acordo com o artigo de (WILLASSEN, 2003) o qual foi feito uma análise forense e verificado que o SIM armazena várias informações, dentre as quais destacamos:

- IMSI;
- TMSI;
- PIN;
- LAI;
- MSISDN;
- Os algoritmos A3 e A8 (em breve serão vistos);
- A chave de autenticação K_i, com 128 bits;
- A chave de encriptação K_c de 64 bits gerada pelo algoritmo A5.

[20] ROM - *Read Only Memory*.
[21] RAM - *Random Access Memory*.
[22] EEPROM - *Electrically Erasable Programmable Read-Only Memory*.

A Figura 3 abaixo ilustra o ME e o SIM.

Figura 3 - Estação móvel
Fonte: (PAULA; BRESSAN; ABE, 2013)

2.3 *Base Station Subsystem* (BSS)

A BSS é o subsistema que garante o acesso do assinante à rede. É através dessa camada que o usuário se conecta para poder realizar a ligação telefônica. Os componentes da BSS são responsáveis pela conectividade entre a central e a estação móvel (celular). Dividem-se, portanto em dois: *Base Transceiver Station* (BTS) e a *Base Station Controller* (BSC) (SILVA, 2013).

2.3.1 *Base Transceiver Station* (BTS)

É o ponto de acesso da estação móvel para a rede. É responsável pela realização de comunicações de rádio entre a rede e o MS. Ele gerencia a codificação, criptografia, multiplexação (TDMA), modulação e demodulação dos sinais de rádio. Um BTS geralmente cobre um único setor de 120 graus de uma área. Normalmente, uma torre com 3 BTSs acomodará todos os 360 graus em torno da torre (Figura 4).

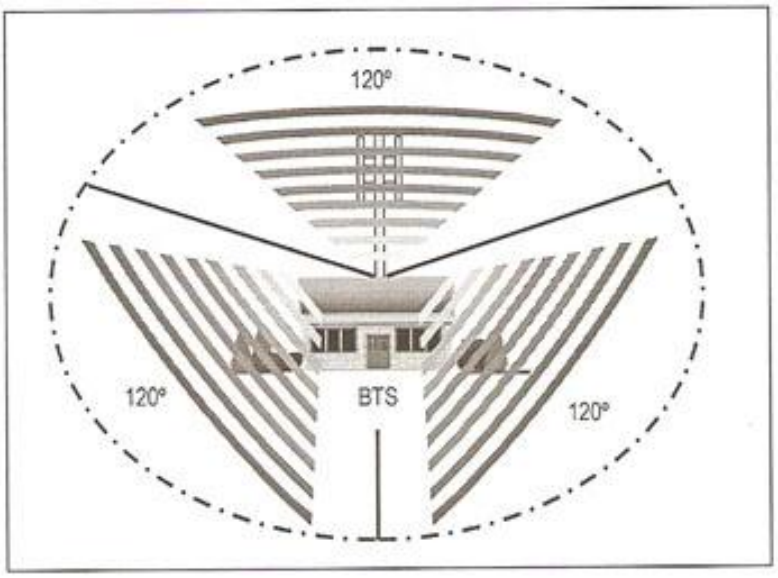

Figura 4 - Setores de 120º
Fonte: (SANTOS, 2008)

2.3.2 *Base Station Controller* (BSC)

Conectam o terminal móvel ao NSS, via MSCs. Cada BSC controla várias estações transceptoras base (BTS) conforme a Figura 5. Os *handoffs* (também denominados *handovers* no GSM) entre duas BTSs sob o controle do mesmo BSC são gerenciadas pelo BSS. Isso reduz consideravelmente o processamento da comutação da MSC (BRANQUINHO, 2016, p. 14) (UFF TELECOM, 2012, p. 4).

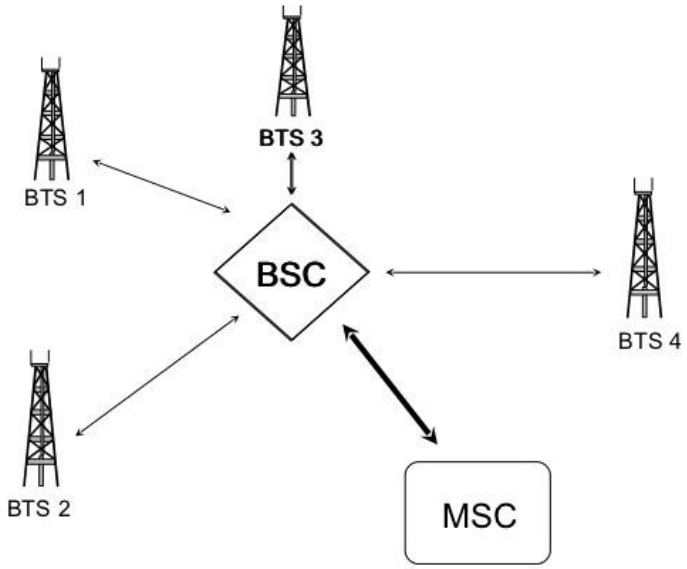

Figura 5 - Controlador de Estação Base (BSC)
Fonte: (UFF TELECOM, 2012)

2.4 *Network and Switching Subsystem* (NSS)

"A SS é a camada da rede que cuida da comutação de chamadas, do encaminhamento de mensagens e da sinalização. Os componentes do mesmo são: *Mobile Switching System* (MSC), *Home Location Register* (HLR), *Visitor Location Register* (VLR), *Authentication Center* (AUC), *Equipment Identity Register* (EIR) e *Gateway Mobile Switching Center* (GMSC)" (SILVA, 2013), a Figura 6 fornece a representação gráfica dos componentes.

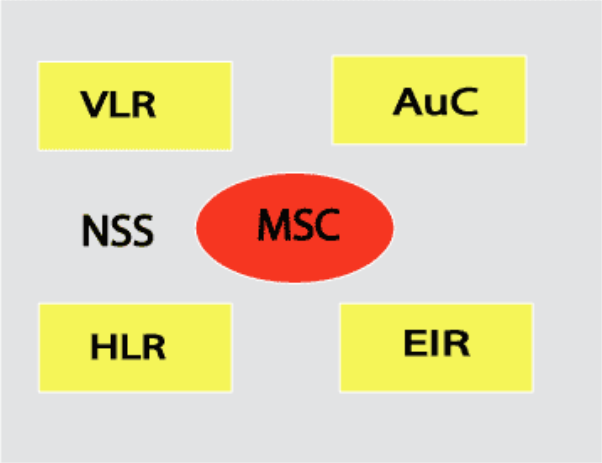

Figura 6 - NSS
Fonte: (POINT, 2016)

2.4.1 *Mobile Switching Center* (MSC)

O MSC é o coração da rede GSM. O MSC executa as chamadas entre o celular e outros usuários da rede fixa ou móvel, bem como o gerenciamento de serviços móveis, como registro, autenticação, atualização de local, transferências e roteamento de chamadas para um assinante de *roaming*. Ele também lida com *handoffs*, bem como as coordenadas com outros MSCs para transferências entre MSC, e trabalha integrado com 4 bases de dados que serão apresentadas a seguir.

2.4.2 *Home Location Register* (HLR)

O HLR é uma grande base de dados que armazena dados sobre assinantes. O HLR mantém informações específicas para assinantes, como a MSISDN, IMSI, localização atual do MS, restrições de *roaming*, tipo de plano assinado pelo usuário e serviços suplementares do assinante. A ativação e a desativação de planos de serviços é sempre implementado no

HLR, então para o assinante se registrar na rede, o HLR deve ser consultado para verificar se o assinante possui permissão para usar os serviços oferecidos (SILVA, 2013).

2.4.3 *Visitor Location Register* (VLR)

O VLR é um banco de dados que contém um subconjunto de informações localizadas no HLR. Contém informações semelhantes ao HLR, mas apenas para atender assinantes visitantes, ou seja, quando estão em *roaming*. Existe uma VLR para cada área de localização. O VLR reduz o número total de consultas ao HLR e, assim, reduz o tráfego de rede. Os VLRs geralmente são identificados pelo Código de Área de Localização (LAC) para a área que eles atendem.

2.4.4 *Equipment Identity Register* (EIR)

O Registro de Identidade do Equipamento (EIR) é um banco de dados que contém uma lista de todos os equipamentos móveis válidos na rede, o VLR é conectado com o MS. Onde a Identidade Internacional de Equipamentos Móveis (IMEI) identifica cada MS.

Um IMEI é marcado como inválido se for denunciado como roubado. O EIR é hoje o principal mecanismo de combate ao roubo de celulares. No mundo todo há grandes bases de dados que alimentam os bancos de dados das operadoras com o IMEI de aparelhos roubados, algo como um **SPC/SERASA** dos celulares roubados.

O EIR por sua vez é padronizado por 3 listas:

- Lista Branca: contendo os IMEIs sem restrições;
- Lista Cinza: contendo os IMEIs sob suspeita;
- Lista Negra: contendo somente os IMEIs dos aparelhos roubados.

2.4.5 *Authentication Center* (AuC)

O Centro de Autenticação é um banco de dados que armazena uma cópia da chave de autenticação assinante individual armazenada no cartão SIM de cada assinante (K_i), esta chave é utilizada para autenticação e a geração da chave de sessão (K_c), que criptografa o tráfego entre MS e BTS.

A AuC é o componente da rede que fica localizado com o HLR e provê a pela segurança dos assinantes, sendo responsável por autenticar os usuários da rede a fim de prevenir fraudes como a clonagem. Seu sistema de autenticação é simples e eficaz, utilizando chaves e algoritmos de autenticação e de criptografia.

2.4.6 *Gateway Mobile Switching Center* (GMSC)

O GMSC basicamente é a porta de entrada e saída para outras redes. Assim como funciona o *gateway* de uma rede local, semelhantemente o GMSC se comporta, pois é através dele que o usuário se comunica com outras redes, sejam elas redes móveis (PLMN) ou redes fixas (**PSTN**).

Por exemplo, um usuário que esteja em *roaming* em outra rede poderá se comunicar com a sua rede *home* através do GMSC. O supracitado tem a função de obter informações do HLR dos usuários para assim poder encaminhar as chamadas para seu devido destino.

2.5 Interfaces da Arquitetura da Rede GSM

As interfaces da arquitetura de uma rede GSM foram padronizadas de modo a permitir a interoperabilidade com outras redes, inclusive *roaming* internacional, e permitir a utilização de diversos fornecedores na sua implantação. Em uma rede GSM, diferentes interfaces são utilizadas entre os subsistemas e seus componentes propiciando que os protocolos necessários para habilitar o fluxo de dados e sinalização possam operar.

Por exemplo: A interface Um é utilizada entre MS e BTS, a interface Abis entre BTS e BSC, seguido pela interface A entre BSC e MSC. A Figura 7 abaixo mostra todas as interfaces.

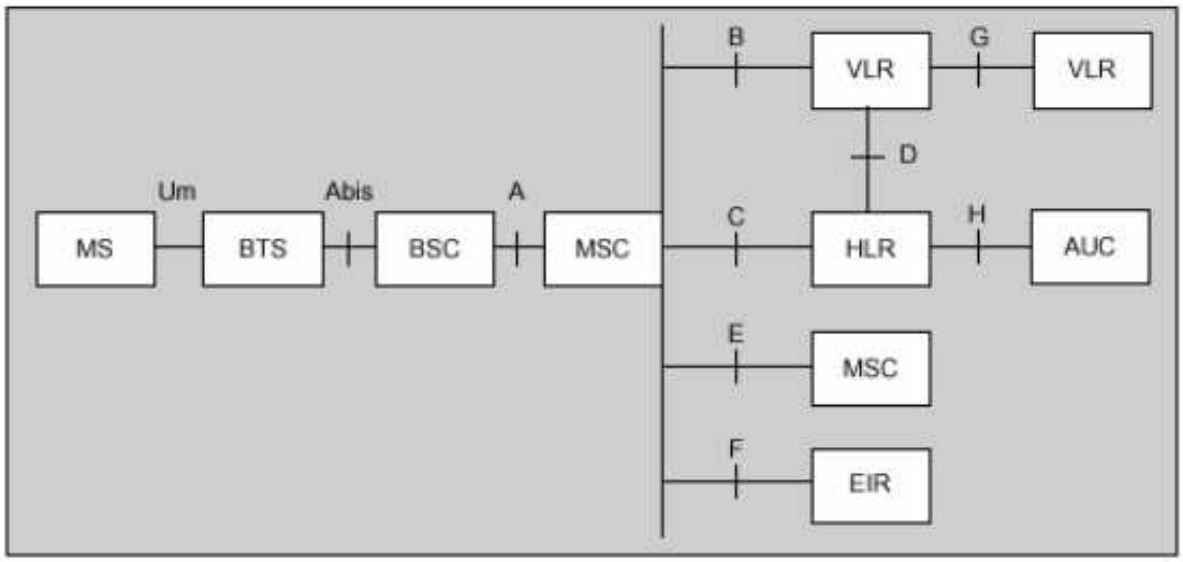

Figura 7 - Interfaces da Rede GSM
Fonte: (UFF TELECOM, 2012)

- **Interface Um:** interface aérea que é responsável por disponibilizar os canais físicos e lógicos aos assinantes móveis para viabilizar o processamento de chamadas, em breve será descrita com maiores detalhes;

- **Interface Abis:** responsável por interligar a BTS e BSC, tais como a transmissão de canais de tráfego e o gerenciamento dos canais de rádio;

- **Interface A:** interface de comunicação entre o BSC e MSC, suas tarefas consistem em: gerenciamento do BSS, tratamentos de chamadas, alocação de recursos terrestres e gerenciamento de mobilidade;

- **Interface B:** interface entre MSC e VLR, sendo utilizada sempre que o MSC precisa acessar os dados sobre uma MS localizada em sua área de cobertura. Como a maioria dos VLRs compõe a estrutura de *hardware* do MSC, isto faz com que a interface seja considerada uma interface interna;

- **Interface C:** Interface que conecta MSC e HLR. É usado quando a MSC precisa de informações necessárias ao roteamento de chamadas ou ao envio de SMS;

- **Interface D:** interface que interliga o HLR e VLR. É usada para a troca de dados sobre a localização da MS. Provê a capacidade de um assinante realizar chamadas dentro de uma determinada área de serviço;

- **Interface E:** interface de comunicação entre duas MSCs. Quando uma MS move-se da área de uma MSC para outra de outra MSC, durante uma chamada, um processo chamado *handover* permite que chamada não seja interrompida;

- **Interface F:** interface de ligação entre o MSC e EIR. Verifica se a MS está apta para utilizar a rede de telefonia móvel GSM, através do IMEI da MS previamente guardado no EIR, que consiste em três tipos: sem restrições, sob suspeitas e roubado;

- **Interface G:** interliga duas VLRs. É usado quando uma MS move-se de um VLR para outro, recuperando o IMEI e os parâmetros de autenticação guardados no VLR de origem;

- **Interface H:** interconexão entre a HLR e AuC. Assim como a interface B a interface H também não é padronizada oficialmente, pois geralmente são componentes internos.

2.5.1 Interface Um Detalhada

Conforme foi descrito acima, a interface Um refere-se á interface utilizada para comunicar o MS e BTS. A interface Um engloba as três camadas inferiores referenciadas no **modelo OSI** a física, enlace e a rede. A Figura 8 abaixo descreve as camadas do OSI da Interface Um entre outras.

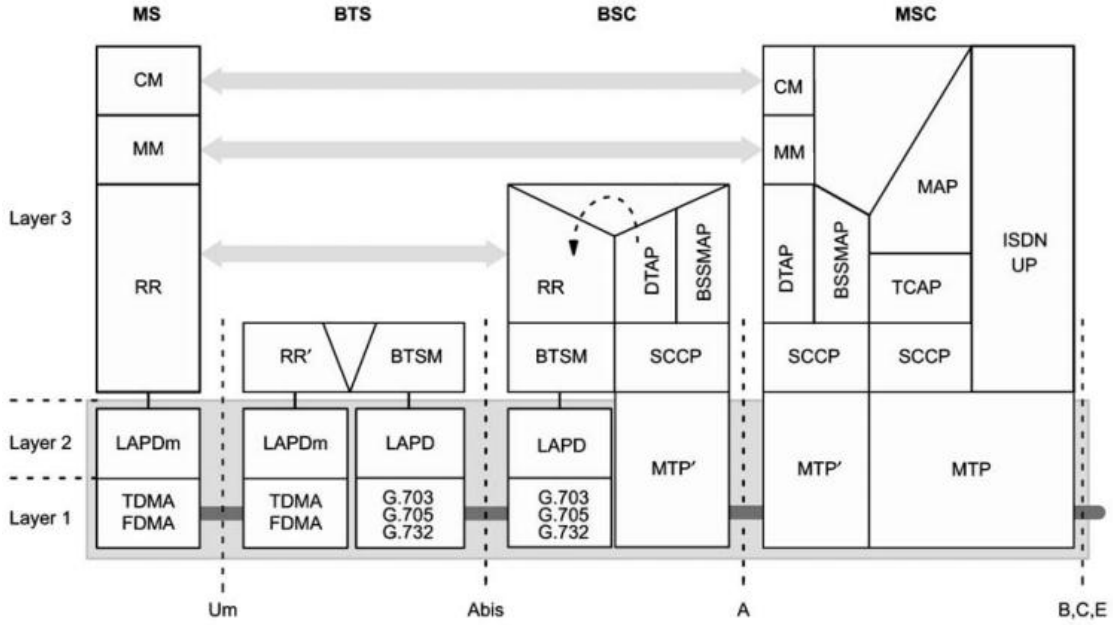

Figura 8 - Camada OSI da Interface Um
Fonte: (GLENDRANGE; HOVE; HVIDEBERG, 2010)

Com base nas camadas OSI apresentadas, os protocolos utilizados nas três camadas são os seguintes:

- **Camada 1: Física.** É o mais importante em qualquer sistema de rádio móvel, na medida em que aborda as características exigentes do ambiente de interface aérea e responsável por transmitir os bits da comunicação.

- **Camada 2: Enlace.** O LAPDm (*Link Access Procedures on the D-channel modified*) é usado para transportar as mensagens da interface aérea. LAPDm forma a camada 2 da interface Um.

- **Camada 3: Rede.** Esta camada está dividida em três subcamadas:
  - A subcamada de *Radio Resource* (RR);
  - A subcamada de *Mobility Management* (MM);
  - Na subcamada *Call Management* (CM), o nível mais alto desta camada se divide em três camadas:
    - *Call Control* (CC): tem a função de controle de chamadas;

- *Supplementary Services* (SS): fornece a gestão de serviços suplementares;

- *Short Message Service* (SMS): gerenciamento de SMS.

***Radio Resource* (RR)**

É a mais baixa na camada de rede e gerencia os canais de rádio, incluindo o estabelecimento do canal físico para os canais lógicos de tráfego e de controle. A camada RR também é usada no BCCH para transmitir informações de sistema, pedidos de paginação, pedidos de acesso e o acesso aos canais de controle comuns (CCCH).

Além disso, a camada RR também lida com o gerenciamento de entrega e controla a cifragem, embora a cifragem ocorra realmente na primeira camada da interface Um. Algumas das mensagens RR frequentemente usadas são definidas na Tabela 3.

Tabela 3 - Exemplos de mensagens RR

Nome	Direção	Descrição
Channel Request	MS→BTS	Esta mensagem requisita um canal de controle dedicado (SDCCH) para a sinalização entre o móvel e o sistema, por meio do RACH.
Cipher Mode Command	BTS→MS	Comando para a MS iniciar a criptografia na interface Um. Este comando contém o algoritmo (A5/X) que deve ser usado.
Immediate Assignment Command	BTS→MS	Esta mensagem é sempre transmitida no AGCH. A finalidade é atribuir um canal dedicado ao MS e contêm alguns parâmetros como: a referência aleatória tirada de uma mensagem de solicitação de canal (RACH), ARFCN e o *timeslot*.

Fonte: Autor

***Mobility Management* (MM)**

É a camada que fica acima de um nível da RR e trata das funções de suporte de atualização da localização para que o roteamentos de chamadas seja possível, autenticação e gerenciamento de criptografia. Algumas mensagens MM e suas respectivas definições estão na Tabela 4.

Tabela 4 - Exemplos de mensagens MM

Nome	Direção	Descrição
Locate Update Request	MS→BTS	Esta solicitação contém um parâmetro que identifica se esta é uma atualização de localização periódica normal ou se é um procedimento de *logon*. Este pedido também contém o antigo LAI e parâmetros como o IMSI/TMSI e o suporte de cifras.
Authetication Request	BTS→MS	Comando de autenticação que contém o desafio aleatório (RAND) e um CKSN (identificador para a chave de sessão resultante).
TMSI Realocation Command	BTS→MS	Ao final do *Locate Update Request*, deve ser atribuído um novo TMSI ao MS. Este comando atribui este novo valor, embora a especificação permite que o comando de reatribuição TMSI contenha o IMSI, em vez de um novo TMSI.

Fonte: Autor

***Call Control* (CC)**

A subcamada Controle de chamadas gerencia as chamadas feitas na rede GSM. E também utiliza o MM para gerenciar estabelecimentos de chamadas e desvios. Esta subcamada é muito similar ao protocolo de controle de conexão ISDN. Algumas das mensagens de CC frequentemente usadas são mostradas na Tabela 5.

Tabela 5 - Exemplos de mensagens CC

Nome	Direção	Descrição
Alerting	MS↔BTS	A mensagem de alerta é transmitida para o MS para indicar, que o celular do usuário da chamada recebida está sendo alertado (toque).
Setup	MS↔BTS	Esta mensagem é transmitida do MS para o BTS ou o inverso. Ela contém o número de quem chamou (MSISDN) e o tipo de conexão TCH solicitada, entre outras informações.
Connect	MS↔BTS	Esta mensagem é transmitida pelo MS para indicar que o usuário aceitou a chamada. Ou é transmitida pelo BTS para indicar que a conexão foi estabelecida com sucesso.

Fonte: Autor

2.5.2 Canais Físicos do GSM

Modulação

A modulação usada no GSM é a **GMSK** (*Gaussian Minimum Shift Keying*), os detalhes técnicos serão mostrados a seguir:

> [...] é um tipo de modulação FSK (*Frequency Shift Keying*) em que a modulação em frequência é o resultado de uma modulação em fase com sinais adequados e amplitude constante, tornando-o apropriado para uso com amplificadores de alta frequência. Baseado na modulação MSK (*Minimum Shift Keying*) os bits "1" e "0" são representados pelo deslocamento da portadora em aproximadamente 68 Hz e no GSM são representados por 270 MHz por ser quatro vezes a frequência no MSK, minimizando o espectro da modulação e aumentando a eficiência do canal. Um filtro gaussiano é usado na fase de pré-modulação reduzindo a velocidade de transferência de frequências que do contrário espalharia energia pelos canais adjacentes (TELECO, 2017).

FDD

O padrão GSM utiliza a FDD (divisão de frequência *duplex*), isto significa que o transmissor e receptor operam em diferentes frequências. Por exemplo, a faixa 890-915 MHz é utilizada para o link reverso ou *uplink* (do MS para a ERB) e a faixa 935-960 MHz é utilizada para o link direto ou *downlink* (da ERB para o MS), tendo então um *offset* de 45

MHz entre as duas faixas. Em seguida as bandas disponíveis para os links diretos e reversos são divididas em canais de banda larga de 200 kHz denominadas **ARFCNs** e adicionalmente há também a utilização da técnica de **FHMA** caso a operadora opte, os detalhes completos estão resumidos na Tabela 6 abaixo.

Tabela 6 - Especificações da interface aérea do padrão GSM 900

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

Fonte: (BRANQUINHO, 2016)

Os dados apresentados na Tabela 6 dizem respeito ao sistema GSM 900. O sistema DCS 1800 utiliza os mesmos princípios do GSM 900. No entanto, a banda alocada em cada sentido é três vezes maior (75 MHz para cada ligação) (SCHILLER *et al.*, 2016), abaixo a Figura 9 mostrando como o *downlink* e *uplink* operam em frequências diferentes.

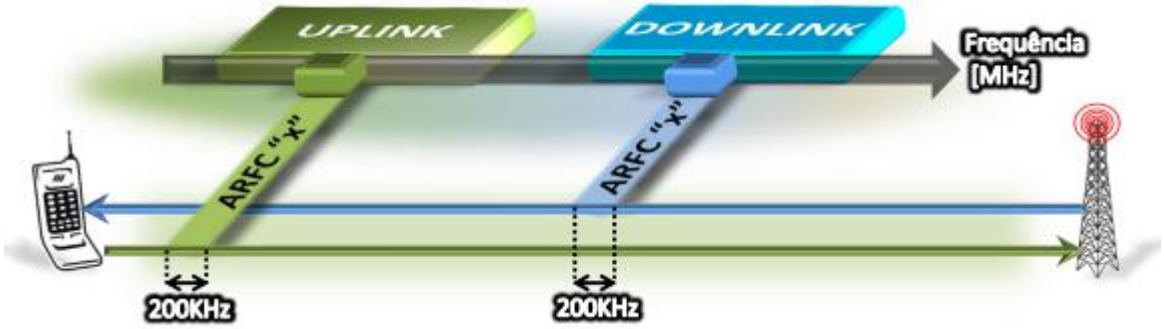

Figura 9 - Frequência de *uplink* e *downlink* segundo o FDD
Fonte: (CARLÉSIMO, 2013, p. 35)

Frequency Division Multiple Access (FDMA)

É um método de acesso ao canal que baseia-se na divisão da banda de frequência disponibilizada em faixas de frequência previamente denominados ARFCNs, cada um com uma largura de 200 kHz conforme adotado no padrão GSM, veja a Figura 10 abaixo.

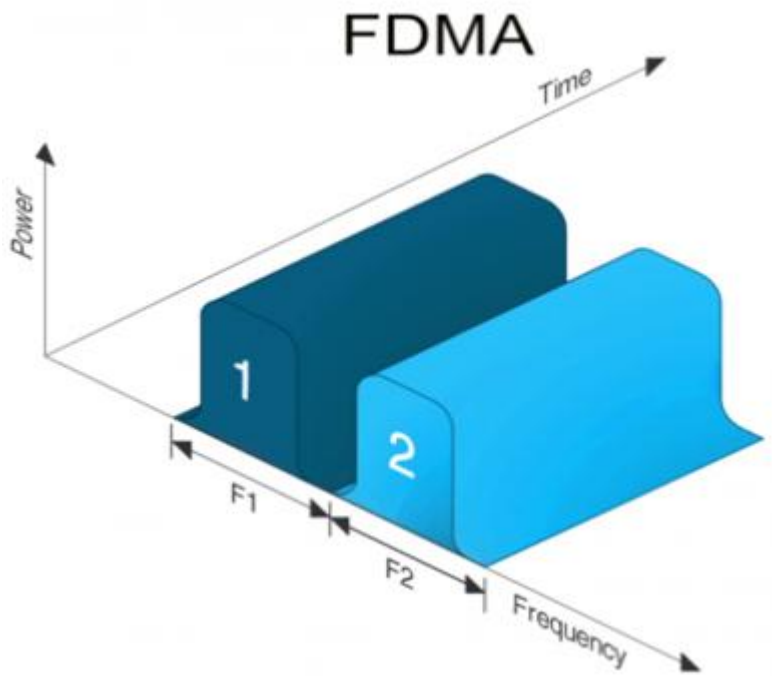

Figura 10 - FDMA
Fonte: (ACADEMY, 2012)

***Time Division Multiple Access* (TDMA)**

O TDMA é uma técnica que dividi cada canal de RF em 8 intervalos de tempo (*timeslots*), sendo que cada um dos 8 intervalos corresponderá a um assinante, um exemplo genérico é ilustrado na Figura 11. No caso das redes móveis o conteúdo de cada intervalo de tempo é denominado "*burst*".

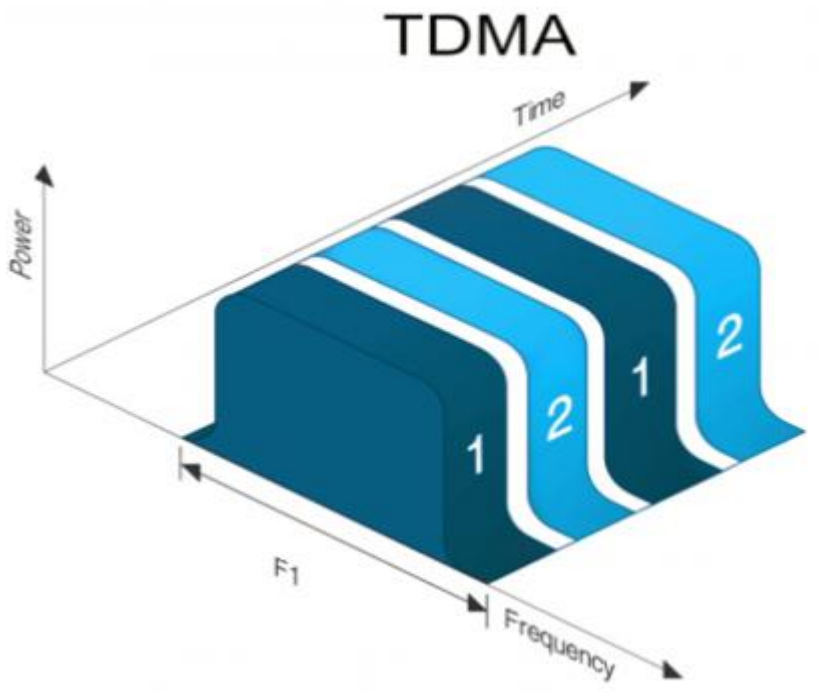

Figura 11 - TDMA
Fonte: (ACADEMY, 2012)

TDMA e FDMA

Esta técnica é a utilizada no sistema GSM. O método de acesso combina a divisão da banda em faixas menores (portadora) que por sua vez é subdivida no tempo (*timeslots*), consequentemente tem-se uma melhor utilização do espectro, vide a Figura 12.

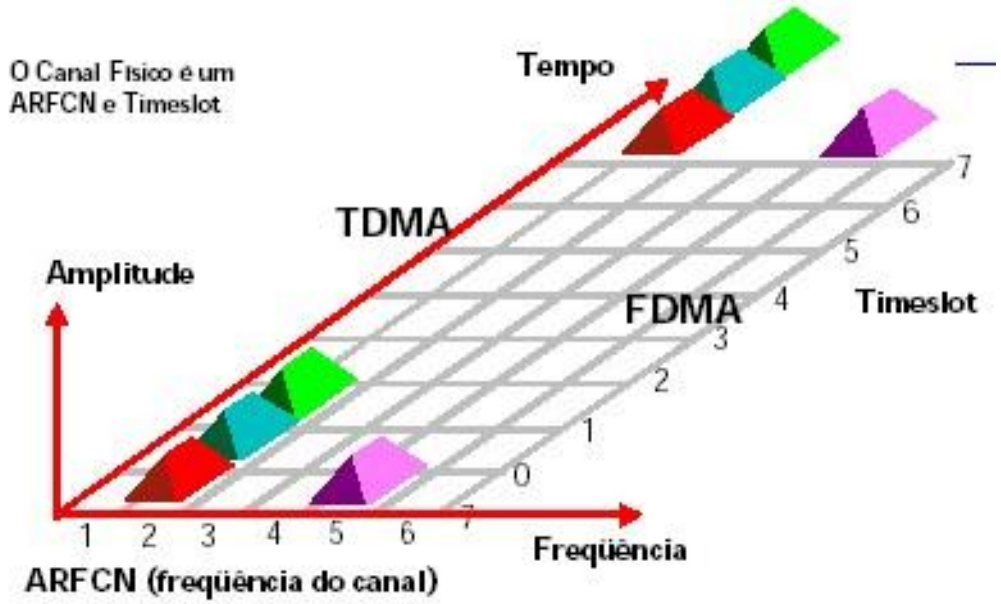

Figura 12 - TDMA e FDMA
Fonte: (GUINTHER, 2012)

A banda é dividida em 200 kHz de largura de banda cada utilizando o FDMA, que por sua vez são subdivididas em 8 *timeslots* com duração total de 4.615 ms utilizando o TDMA, portanto podendo suportar até 8 estações móveis. Estes *timeslots* são identificados de 0 a 7, e cada conjunto de 8 intervalos corresponde a um quadro TDMA.

O sincronismo é um imprescindível para a comunicação. Para isso, as informações são transmitidas sincronizadas com um atraso no início do quadro TDMA. A BTS atrasa em 3 intervalos o envio do seu quadro TDMA, de forma que o enlace direto (*downlink*) e o reverso (*uplink*) tem 3 intervalos de diferença, conforme a Figura 13 abaixo.

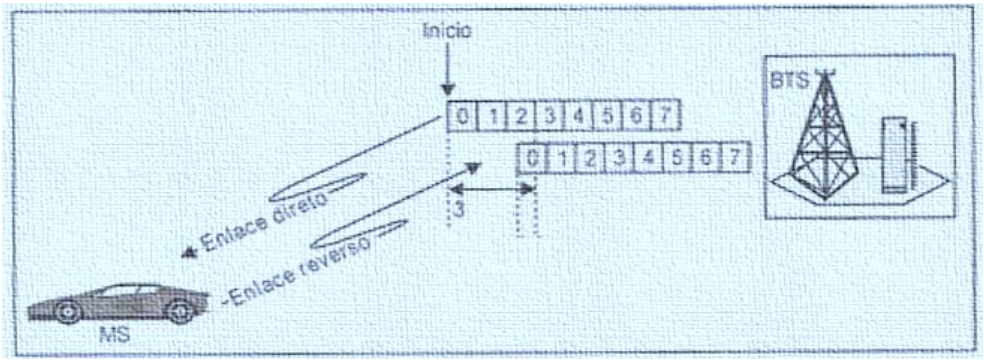

Figura 13 - Comunicação entre MS e BTS
Fonte: (SANTOS, 2008)

***Frequency Hopped Multiple Access* (FHMA)**

"Sistema de acesso múltiplo digital no qual as portadoras dos usuários são postas de forma pseudoaleatória dentro do canal da banda larga, ao invés de permanecer em uma única banda como em sistemas tradicionais" (CASTRO, 2013).

Normalmente, o controle de potência e as tecnologias de transmissão descontínua são adotadas para reduzir a interferência do sistema. Então para evitar interferências e melhorar a qualidade da comunicação do sistema, a tecnologia de salto de frequência é utilizada.

> No FH, a informação é espalhada em uma largura de banda bem maior que a realmente necessária para sua transmissão. Para isso, a mesma é dividida em diversos canais de largura de banda menor. Conhecendo a sequência de saltos que deve ser seguida, o receptor e o transmissor saltam por esses canais. Essa sequência é pseudoaleatória, e é o que torna o FH também seguro formando assim uma nova camada de segurança adicional, já que receptores não desejados não conseguem interceptar o sinal uma vez que eles não conhecem a sequência. A única coisa que eles vêem são ruídos de curta duração (HALL, 2011).

No FHMA a frequência do sinal muda de canal muito rápido, se a frequência da portadora mudar mais de uma vez na duração da transmissão de um símbolo, então é dito *Fast Frequency Hopping System* (CASTRO, 2013). Caso a frequência da portadora demorar e mudar a frequência após vários símbolos serem transmitidos, é tido por *Slow Frequency Hopping*, o GSM, por exemplo, utiliza este último método (CASTRO, 2013).

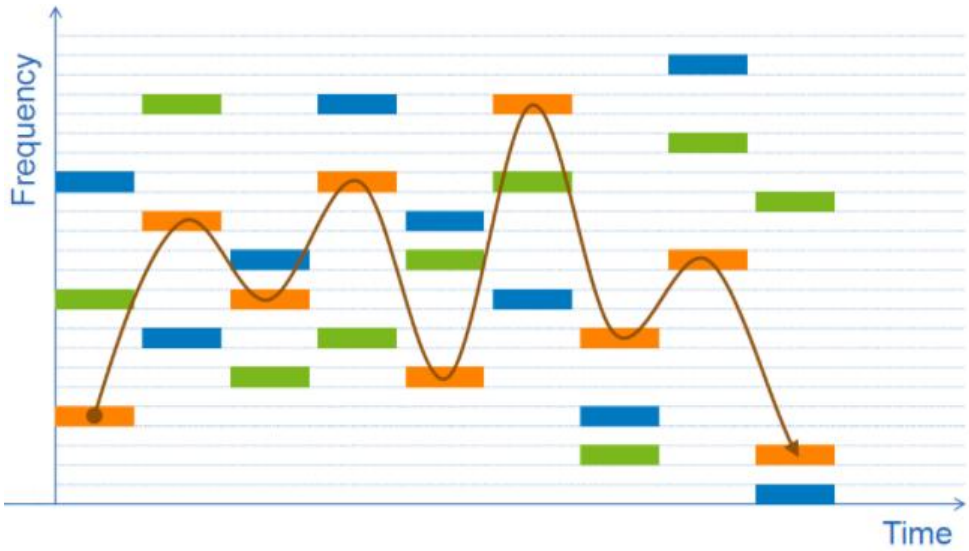

Figura 14 – FHMA
Fonte: (ACADEMY, 2012)

A Figura 14 mostra como o salto na frequência age, permitindo um grau maior de reutilização de frequência, e ainda provê um grau maior de segurança, mesmo que não seja uma medida projetada para a segurança.

Absolute Radio Frequency Channel Numbers (ARFCN)

O ARFCN é um código que identifica um link direto e reverso separados de 45 MHz no GSM 900 e 95 MHz no DCS 1800, sendo cada canal compartilhado entre um número máximo de 8 usuários, através da técnica TDMA. Cada um dos 8 usuários utiliza o mesmo ARFCN e ocupa um mesmo slot temporal por quadro TDMA como mostrado na Figura 15, cada *slot* temporal possui uma duração equivalente de 576,92 µs e sendo que um único quadro TDMA do GSM tem duração de 4.615 ms. A Tabela 7 retrata o uso do ARFCN para calcular as frequências.

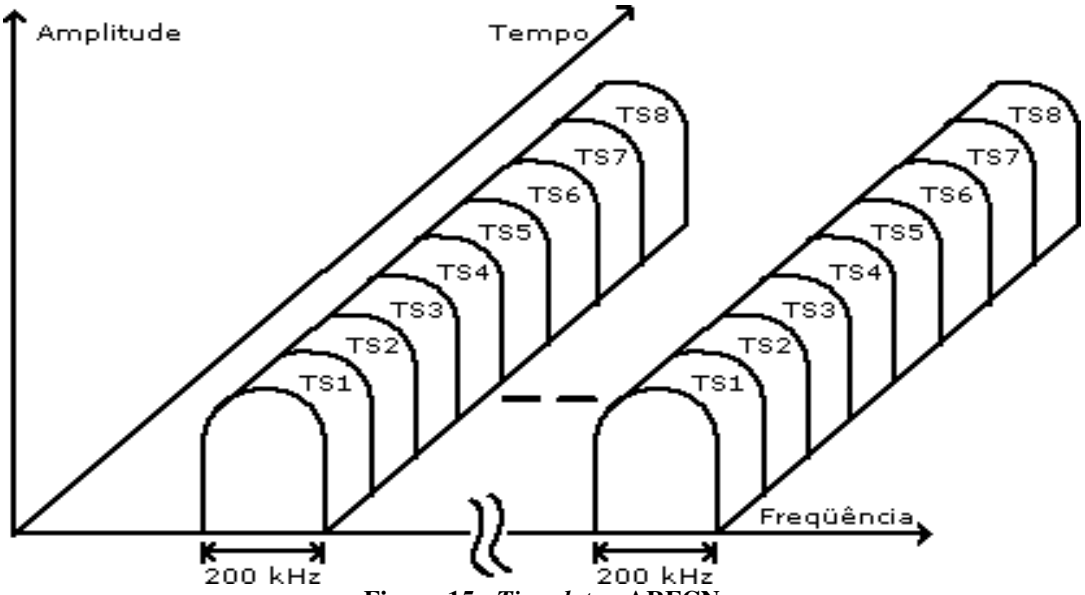

Figura 15 - *Timeslots* e ARFCN
Fonte: (ULBRICH, 2008)

Tabela 7 - Faixa de frequências *downlink* e *uplink*

Descrição	ARFCN	Frequência *Uplink* (f_{up}) MHz	Frequência *Downlink* (f_{dl}) MHz
GSM 450	$259 \leq \text{ARFCN} \leq 293$	$450{,}6 + 0{,}2.(\text{ARFCN} - 259)$	$f_{up}.(\text{ARFCN}) + 10$
GSM 480	$306 \leq \text{ARFCN} \leq 340$	$479 + 0{,}2.(\text{ARFCN} - 306)$	$f_{up}.(\text{ARFCN}) + 10$
GSM 750	$438 \leq \text{ARFCN} \leq 511$	$747{,}02 + 0{,}2.(\text{ARFCN} - 438)$	$f_{up}.(\text{ARFCN}) + 30$
GSM 850	$128 \leq \text{ARFCN} \leq 251$	$824{,}2 + 0{,}2.(\text{ARFCN} - 128)$	$f_{up}.(\text{ARFCN}) + 45$
Primary GSM (P-GSM 900)	$1 \leq \text{ARFCN} \leq 124$	$890 + 0{,}2.\text{ARFCN}$	$f_{up}.(\text{ARFCN}) + 45$
Extended GSM (E-GSM 900)	$0 \leq \text{ARFCN} \leq 124$ $975 \leq \text{ARFCN} \leq 1023$	$890 + 0{,}2.\text{ARFCN}$ $890 + 0{,}2.(\text{ARFCN} - 1024)$	$f_{up}.(\text{ARFCN}) + 45$
GSM Rail (GSM-R 900)	$0 \leq \text{ARFCN} \leq 124$ $955 \leq \text{ARFCN} \leq 1023$	$890 + 0{,}2.\text{ARFCN}$ $890 + 0{,}2.(\text{ARFCN} - 1024)$	$f_{up}.(\text{ARFCN}) + 45$
DCS 1800	$512 \leq \text{ARFCN} \leq 855$	$1710{,}02 + 0{,}2.(\text{ARFCN} - 512)$	$f_{up}.(\text{ARFCN}) + 95$
PCS 1900	$512 \leq \text{ARFCN} \leq 810$	$1850{,}2 + 0{,}2.(\text{ARFCN} - 512)$	$f_{up}.(\text{ARFCN}) + 80$

Fonte: Autor

2.5.3 Canais Lógicos do GSM

Até então somente os canais físicos (PCH[23]) foram abordados, entretanto falta abordar os canais lógicos. Esses canais LCHs[24] são de extrema importância e divide em dois tipos: canais de tráfego (TCH) que transportam voz codificada e canais de controle (CCH) que cuidam da sinalização e sincronismo entre a BTS e a MS. "Enquanto os PCHs são descritos no domínio da frequência e do tempo, os LCHs são mapeados nos canais físicos tendo funções diferentes em cada instante de tempo. Em outras palavras, o canal lógico mostra a função que um canal físico está assumindo em um determinado momento" (CARLÉSIMO, 2013, p. 39).

[23] PHC - *Physical Channel*.
[24] LCH - *Logical Channel*.

Canais de Tráfego

São canais *duplex* bidirecionais usados transmissão de dados e voz entre a MS e a BTS, sendo classificados como:

- **TCH/H** (*Half Rate Traffic Channel*) utilizado em meia taxa (*halfrate*). No primeiro caso a taxa de transmissão é de 13 kb/s e no segundo 6,5 kb/s.

- **TCH/F** (*Full Rate Traffic Channel*), com taxas de transmissão na ordem de 22,8 kbits/s para voz e de 2,4 a 9,6 kbits/s para dados do usuário. Canal especial para dados, taxas de 9,6; 4,8 e 2,4 kb/s.

Canais de Controle

São os canais responsáveis pelas informações, sinalização e sincronismo da MS com a rede para que opere de maneira adequada e sem erros. Existem no total três tipos de categorias de canais de controle:

- **Canais de Difusão - *Broadcast Channels* (BCH)** o objetivo destes canais é transmitir as informações necessárias para que a MS fique sincronizada na rede. Operam somente no sentido do enlace de descida, ou seja, *downlink*. É composto pelos seguintes:

    - **Canal de Correção de Frequência - *Frequency Correction Channel* (FCCH):** responsável pelas informações que possibilitam a correção de frequência da MS. Provê referência de frequência do sistema para o móvel (ME) transmitido um tom senoidal e posteriormente detectado.

    - **Canal de Sincronismo - *Synchronization Channel* (SCH):** responsável por difundir as informações que possibilitam a sincronização da MS, a identificação da BTS com o parâmetro BSIC[25]

[25] BSIC - *Base Station Identity Cod*.

(NCC + BCC) e possibilita que a ME sincronize na estrutura temporal dentro de uma determinada célula.

- **Canal de Controle de Radiodifusão - *Broadcast Control Channel* (BCCH):** é utilizado para transmitir informações em *broadcast* tais como identificação de rede, célula, informações gerais do sistema relativas ao *roaming*, potência máxima permitida na célula, estado *idle* e ao estabelecimento de chamadas.

- **Canais de Controle Comum - *Common Control Channels* (CCCH):** estes canais têm a função de estabelecer e suportar um link dedicado entre o MS e o BTS, além disso provêm ferramentas para o estabelecimento de chamadas, três são do tipo *downlink* e um do tipo *uplink*, o supracitado divide-se em quatros canais:

  - **Canal de Busca - *Paging Channel* (PCH):** transmitido somente no *downlink*, pela BTS. O MS periodicamente "escuta" o PCH e verifica se há tráfego recebido. O MS pode ser abordado pelo seu TMSI ou IMSI. No entanto, as especificações do GSM não permitem a paginação pelo IMEI.

  - **Canal de Acesso Aleatório - *Randon Access Channel* (RACH):** utilizado pela MS para solicitar um canal de controle dedicado, funciona apenas no *uplink*.

  - **Canal de Acesso Concedido - *Access Grant Channel* (AGCH):** informa a MS qual canal dedicado deve ser sintonizado. É uma resposta da BTS ao acesso RACH feito com sucesso pela MS. Transmitido somente no *downlink* e é mapeado pelo mesmo canal físico do TCH.

  - **Canal de Notificação - Notification Channel (NCH):** um canal apenas de *downlink* utilizado para notificar as MS sobre chamadas de voz.

- **Canais de Controle Dedicado - *Dedicated Control Channels* (DCCH):** canal bidirecional ponto-a-ponto utilizados para realizar a transferência de mensagens entre a BTS e a MS quando estes não estão ocupados, medidas de desempenho, mensagens curtas de alta prioridade, etc. Como no caso anterior, podem também ser decomposto em 3 canais:

    - **Canal de Controle Dedicado Independente - *Stand Alone Dedicated Control Channel* (SDCCH):** é utilizado para sinalização durante a inicialização da chamada. Gerenciamento de conexão, mensagens SMS e demais serviços suplementares. Neste canal citado é realizada a autenticação e a atribuição do canal de tráfego (TCH) com o envio do *timeslot* e a frequência correta, assim definindo o canal.

    - **Canal de Controle Associado Lento - *Slow Associated Control Channels* (SACCH):** sempre associado com um SDCCH ou um canal de tráfego, é usado para informar a MS sobre as frequências de células vizinhas, alinhamento de tempo e controle de potência. Pode transmitir mensagens SMS se estiver associado a um canal de tráfego. Por este motivo que as mensagens SMS podem ser recebidas enquanto estiverem ocupadas em uma chamada.

    - **Canal de Controle Associado Rápido - *Fast Associated Control Channels* (FACCH):** mesmo objetivo do SACCH, mas com alta prioridade.

A Figura 16 exemplifica e demonstra a hierarquia dos canais apresentados até agora. Logo em seguida vamos acompanhar o passo-a-passo dos canais lógicos em uma ligação.

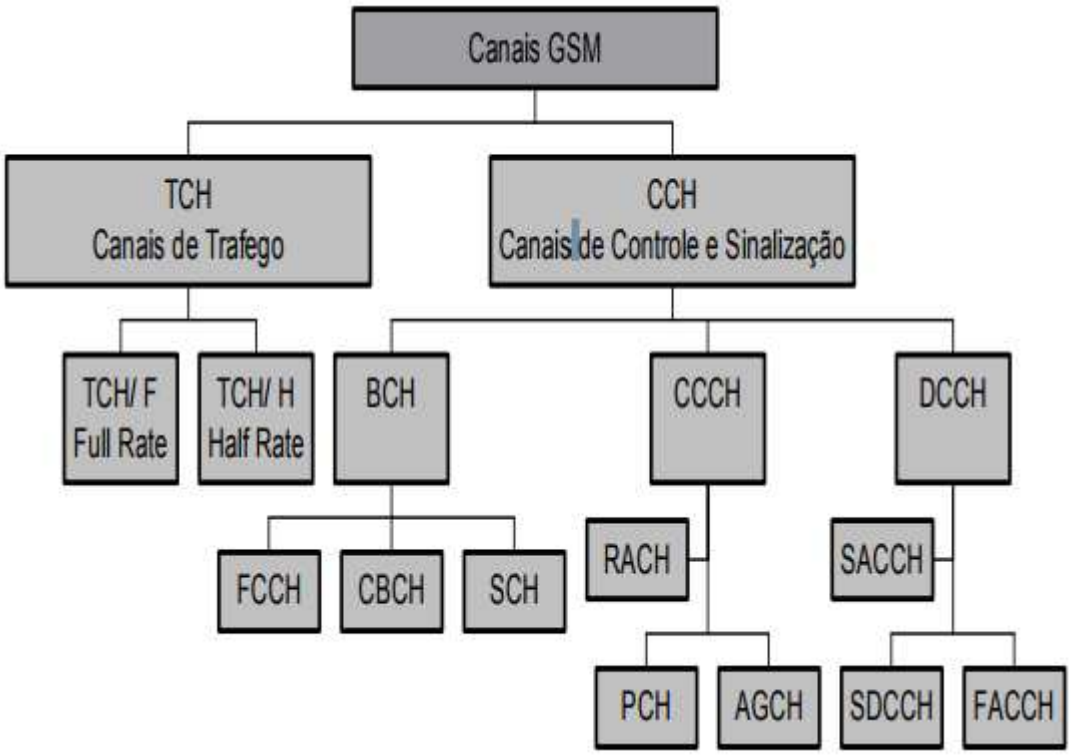

Figura 16 - Canais Lógicos GSM
Fonte: (SILVA; ROCHA; FREIRE, 2014)

Registro da MS na rede GSM

Segundo (UFF TELECOM, 2012, p. 33), o acesso típico do MS á rede referente ao registro e sincronismo, se concentra nos seguintes passos:

1. Inicialmente, o terminal móvel busca uma portadora de radiodifusão (broadcast) na célula onde está localizado. Para isto são medidas todas as portadoras disponíveis na área onde se encontra. A portadora de radiodifusão que contém os canais de controle é identificada por transmitir uma potência superior às demais existentes na célula;

2. A seguir, o terminal móvel recebe o canal lógico FCCH para ajustar sua frequência;

3. O próximo passo é identificar o canal lógico de sincronismo SCH através do qual recebe o código de identificação da ERB;

4. A fase de sincronismo é encerrada com a recepção do canal de controle de radiodifusão (BCCH) e as seguintes informações:

a) O BCCH das células vizinhas com até 16 frequências de portadoras;

b) A identidade global da célula – CGI (*Cell Global Identity*) com o código do país, código da rede móvel, código de área e identidade da célula;

c) A quantidade de canais de controle comum (CCCH);

5. Passando à fase de registro, o terminal móvel transmite um acesso aleatório (RACH) para a ERB/BSC solicitando um canal de controle dedicado (SDCCH). Em resposta, recebe através de um canal de acesso concedido (AGCH) o endereço do SDCCH a ser usado;

6. Através do SDCCH, o terminal móvel envia a atualização das seguintes informações: TMSI (*Temporary Mobile Subscriber Identity*) e LAI (*Location Area Identity*). Estes parâmetros ficam armazenados no terminal móvel;

7. A solicitação de atualização feita pelo terminal móvel alcança o MSC/VLR através da BSC. Se o TMSI enviado pelo usuário coincide com a informação do usuário disponível no VLR este atualiza o novo pedido de registro e ativa o terminal móvel. Caso o VLR não identifique o TMSI, a LAI é decodificada com a finalidade de descobrir em qual MCS/VLR o terminal móvel estava operando anteriormente. O VLR atual se comunica com o anterior para pedir os parâmetros do usuário, inclusive IMSI e assim proceder a sua autenticação;

8. Reconhecido o terminal móvel, O TMSI e a LAI são atualizados no VLR atual e no HLR do usuário.

Chamada Oriunda do MS

Ainda segundo (UFF TELECOM, 2012, p. 34), os passos seguintes correspondem ao procedimento de uma chamada partindo de um MS:

1. O terminal móvel efetua um acesso aleatório através o canal RACH, solicitando um canal de sinalização dedicado SDCCH;

2. A BSC atribui um canal de sinalização através do canal de acesso concedido AGCH;

3. É estabelecido o canal de sinalização (SDCCH) entre o terminal móvel e o MSC/VLR. Este canal suportará toda a sinalização entre a rede e o móvel até que seja estabelecido o canal de tráfego;

4. O MSC solicita à BSC que seja atribuído um canal de tráfego ao terminal móvel;

5. A partir deste momento, o terminal móvel passa a utilizar o canal de tráfego TCH/SACCH;

6. O MSC envia então o pedido para a rede fixa. O usuário móvel passa a ouvir o toque de chamada.

A Figura 17 abaixo demonstra o procedimento descrito da chamada na rede GSM.

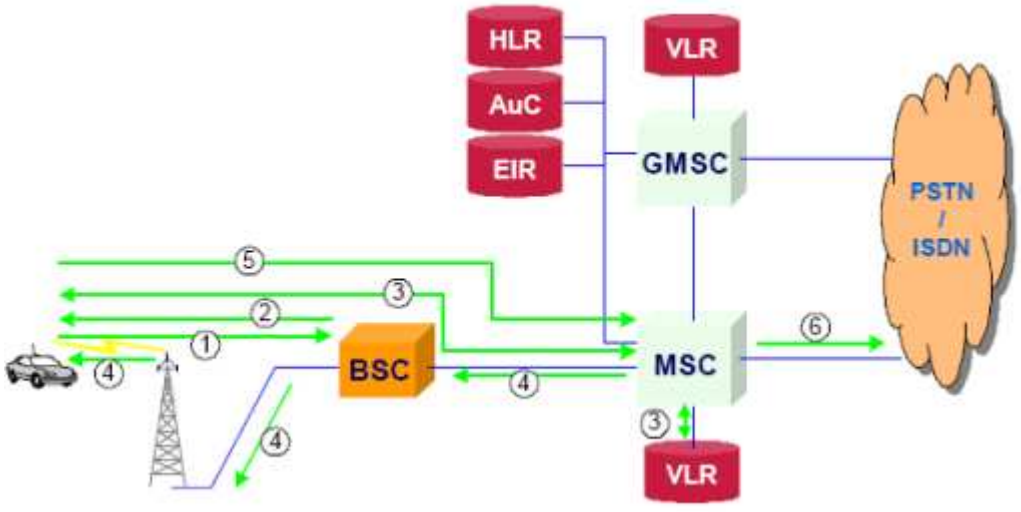

Figura 17 - Chamada originada no MS
Fonte: (UFF TELECOM, 2012, p. 34)

2.6 Segurança

Atualmente as empresas, governos, organizações, etc são inteiramente dependentes de sistemas de informação, visto que as tecnologias de informação e comunicação têm evoluído de forma rápida, fazendo com que tenham maior eficiência, devido a este fato as chances de uma empresa não usar sistemas de informação tornou-se praticamente nula.

Porém, isso pode significar problemas, posto que, se os sistemas de informação sofrer incidências de falhas de segurança, as atividades do negócio serão afetadas e consequentemente haverá prejuízo, não somente financeiro, como também a perda de confiança e reputação.

Neste contexto a importância de se utilizar mecanismos de segurança e de armazenamento das informações é vital para a sobrevivência. Sendo assim, para minimizar os riscos de incidentes deste patamar, é importante que os sistemas utilizados cumpram determinados requisitos de segurança abordados a seguir.

2.6.1 Serviços de Segurança

A recomendação (X.800, 1991) admite a seguinte definição “um serviço prestado por uma camada de um serviço prestado por uma camada de protocolo de comunicação de sistemas abertos, que garante a segurança adequada dos sistemas ou de transferências de dados”, de modo igual temos a recomendação (RFC 2828, 2000) afirmando que “um serviço de serviço de processamento ou processamento ou comunicação prestado por um sistema para dar um tipo específico de proteção aos recursos do sistema recursos do sistema”.

Autenticação

Corresponde a garantia da identidade ou do papel de alguém na comunicação. Essa garantia pode ser feita de diversas maneiras diferentes, mas é geralmente baseada em *Two-Factor Authentication* (2FA), que nada mais é que uma combinação de algo que a pessoa tem (como um cartão inteligente ou um dispositivo que armazena chaves secretas), algo que a pessoa sabe (senha) e algo que a pessoa é (impressão digital) (GOODRICH; TAMASSIA, 2013, p. 5). A Figura 18 ilustra algumas bases para a autenticação de dois ou mais fatores.

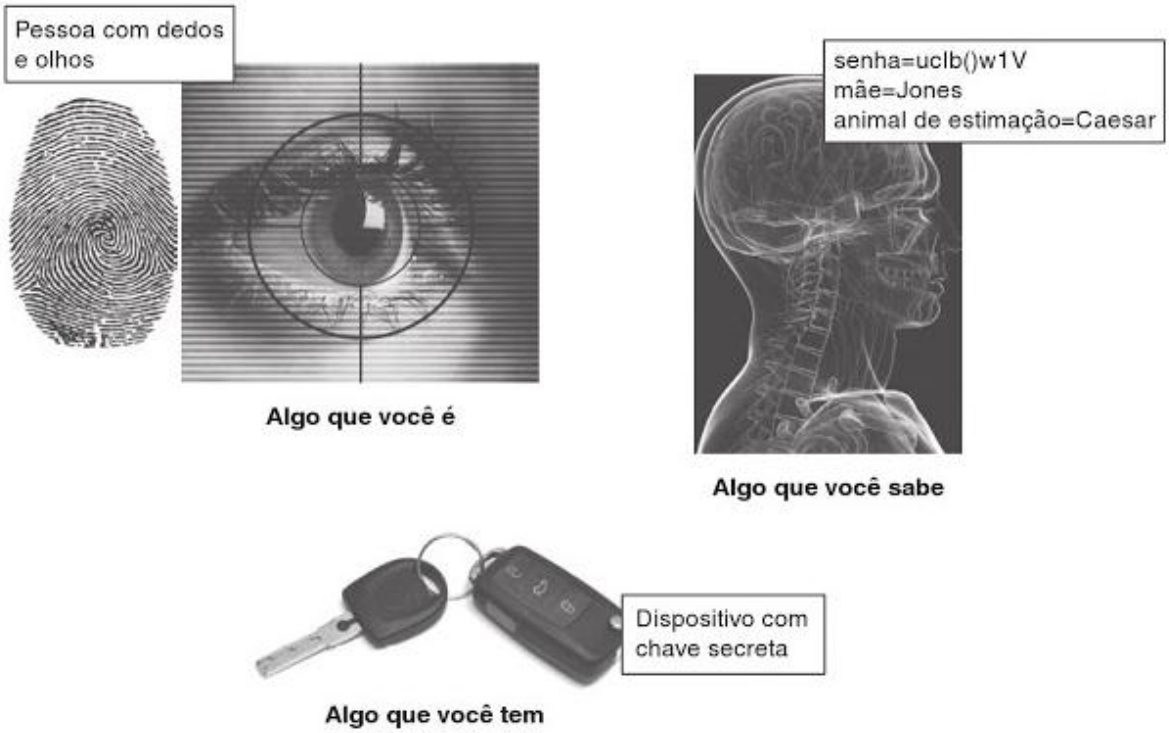

Figura 18 - Bases para autenticação
Fonte: (GOODRICH; TAMASSIA, 2013)

Controle de Acesso

No contexto da segurança da informação, o controle de acesso corresponde as regras e políticas que limitam o acesso a informação confidencial apenas para aquelas pessoas e/ou sistemas com uma "necessidade de saber". Para conseguir isso, cada entidade da organização deve está devidamente identificado por meio da autenticação (STALLINGS, 2008, p. 10). Essa necessidade da autenticação convém que seja por intermédio de uma identidade, como o nome da pessoa ou o número serial do computador, ou pelo papel que alguém desempenha (GOODRICH; TAMASSIA, 2013, p. 6).

Confidencialidade

(GOODRICH; TAMASSIA, 2013, p. 4) em seu livro discorreu:

> No contexto de segurança de computadores, confidencialidade é evitar a relação não autorizada de informação. Isto é, confidencialidade envolve a proteção de dados, propiciando acesso àqueles que são autorizados a vê-los e não permitindo que outros saibam algo a respeito de seu conteúdo. Manter a informação secreta é muitas vezes a essência da segurança de informação, e esse conceito, na verdade, antecede os computadores. Por exemplo, no primeiro uso registrado de criptografia, Júlio César comunicava comandos a seus generais usando uma codificação simples. Na sua

> codificação, César pegava cada letra na sua mensagem e substituía D por A, E por B e assim por diante. Essa codificação pode ser facilmente quebrada, tornando-a uma ferramenta inadequada para obter confidencialidade. Mas, na época, a codificação de César era provavelmente bastante segura, Visto que a maioria dos inimigos de César não conseguia ler em latim. Atualmente, obter confidencialidade é mais desafiador. Computado res estão em todos os lugares e cada um é capaz de executar operações que podem comprometer a confidencialidade. Com todas essas ameaças a confidencialidade da informação, pesquisadores de segurança de computadores e projetistas de sistemas têm desenvolvido muitas ferramentas para proteger informação sensível.

Integridade

A integridade constitui a capacidade do sistema em evitar que as informações sejam alteradas indevidamente, em outras palavras é a garantia de que os dados foram recebidos são congruentes aos dados enviados por uma entidade autorizada. Desta forma, assegura-se que a informação original chegará a seu destino sem nenhum comprometimento.

Irretratabilidade

Oferece proteção contra a negação do serviço, garante que a entidade não negue ter criado ou participado da comunicação, podemos dividir a irretratabilidade em duas partes:

- **Irretratabilidade na origem:** Prova que a mensagem foi enviada pela entidade.
- **Irretratabilidade no destino:** Prova que a mensagem foi recebida pela entidade.

Disponibilidade

Tanto a (RFC 2828, 2000) como a (X.800, 1991) definem disponibilidade como sendo propriedade de um sistema ou de um recurso do sistema ser acessível e utilizável sob demanda por uma entidade autenticada e autorizada do sistema, de acordo com especificações de desempenho, ou seja, o sistema deverá estar disponível sempre que os usuários solicitarem e não deve demasiadamente custoso para a entidade fornecer a disponibilidade, a seguir o exemplo de (GOODRICH; TAMASSIA, 2013, p. 8) sobre essa perspectiva de segurança versus custo.

> Informação encarcerada em um cofre de ferro fundido em uma montanha tibetana e protegida durante o dia inteiro por um esquadrão de ninjas devotados pode ser considerada segura, mas não é segura de forma prática de uma perspectiva de segurança de informação se ela demanda semanas ou meses para ser alcançada. Portanto, a qualidade de uma informação é diretamente associada à sua disponibilidade.

2.6.2 Criptografia

Políticas de segurança de computadores são **inúteis** se não tivermos maneiras de implementa-las. Os serviços de seguranças definidos anteriormente podem ter um papel importante no impedimento de ataques e incentivo à práticas de segurança. Entretanto, soluções tecnológicas é que são o ponto principal para fazer cumprir as políticas de segurança e atingir as metas de segurança. Com o auxilio da criptografia tornamos esta tarefa possível.

A segurança na era da informática nunca foi tão amplamente discutida: casos de violação de contas bancárias, acesso a informações sigilosas, invasão, destruição ou *deface*[26] de sistemas estão cada vez mais comuns. As informações são transmitidas com mais eficiência e velocidade, porém, quase sempre de forma insegura.

A privacidade é muito importante para pessoas e para as empresas. Muitos problemas podem acontecer se uma pessoa não autorizada tiver acesso a dados pessoais como por exemplo: documentos de identificação, endereço, número do cartão de crédito, senhas bancárias ou de crédito automático.

No caso de empresas, os danos podem ser de maior magnitude, atingindo a organização e os próprios funcionários. Dados estratégicos da empresa, previsão de venda, detalhes técnicos de produtos, resultados de pesquisas e arquivos pessoais são informações valiosas que caso alguma empresa concorrente tiver acesso de forma indevida, pode acarretar em sérios problemas e a perda da concorrência no mercado ou ainda sanções na justiça por causa de vazamento de dados de clientes ou funcionários.

Uma definição clara de criptografia a seguir desenvolvida por (ORDONEZ *et al.*, 2005, p. 16) “O ato de transformar um texto legível (texto claro, texto original, texto simples) em algo ilegível (cifra, texto cifrado, texto código) é chamado de “encriptar” (codificar, criptografar, cifrar). A transformação inversa é chamada de “decriptar” (decodificar, descriptografar, decifrar)”. (CARLÉSIMO, 2013, p. 25 apud ERIKSSON, 2005) endossa que o grau de segurança da criptografia está diretamente relacionado aos fatores descritos abaixo:

- Tempo necessário para quebrar seu algoritmo;
- Custo envolvido no processo de quebra do algoritmo;

---

[26] *Deface* - Na segurança da informação, é usado para categorizar os ataques realizados por *defacers* e *script kiddies* para modificar a página de um site na Internet.

- Relação entre a quantidade de informação protegida versus a quantidade de dados necessários para quebrar o segredo.

Termos Utilizados na Criptografia

(STALLINGS, 2008, p. 36) em seu livro propôs os seguintes conceitos:

- **Texto claro (*Cleartext* ou *Plaintext*):** Essa é a mensagem ou dados originais, inteligíveis, alimentados no algoritmo como entrada;

- **Algoritmo de criptografia:** É a sequência de procedimentos que envolvem algoritmos matemáticos capazes de cifrar e decifrar dados sigilosos. O algoritmo de criptografia pode ser executado por um computador, por um hardware dedicado, por um humano e pode acontecer em nível de software ou hardware. Em todas as situações, desde que tenha sido implementado corretamente, o que diferencia é a velocidade de execução e a probabilidade de erros;

- **Chave secreta:** A chave secreta também é a entrada para o algoritmo de criptografia. A chave é um valor independente do texto claro e do algoritmo. O algoritmo produzirá uma saída diferente, dependendo da chave específica sendo usada no momento. As substituições e transformações exatas realizadas pelo algoritmo dependem da chave;

- **Texto cifrado:** Essa é a mensagem embaralhada, produzida como saída. Ela depende do texto claro e da chave secreta. Para determinada mensagem duas chaves diferentes produzirão dois textos cifrados diferentes. O texto cifrado é um fluxo de dados aparentemente aleatórios e, nesse formato, é ininteligível;

- **Algoritmo de descriptografia:** Esse é basicamente o algoritmo de criptografia executado de modo reverso, isto é, de posse do da chave secreto e do texto cifrado obtemos o texto claro.

Segurança dos Sistemas de Criptografia

"Os distintos sistemas de criptografia possuem diferentes graus de segurança, mas todos os métodos desenvolvidos e em uso atualmente são quebráveis, desde que sejam fornecidos tempo e recursos computacionais suficientes" (FILHO, 2004, p. 48).

O custo requerido para quebrar um sistema criptográfico é relacionado com o tamanho da chave que o algoritmo utiliza. Se os recursos exigidos forem maior que o valor da informação que será obtida, então, para todos os fins práticos, o sistema é seguro, porém é importante observar que o poder de processamento dos computadores está sempre crescendo e tornando-se mais barato (FILHO, 2004) .

Tabela 8 - Tempo médio requerido para decifragem em ataque de força bruta

Tamanho da chave (*bits*)	**Número de chaves alternativas**	**Tempo requerido (A 1 Decifragem / μs)**	**Tempo requerido (A 10^6 Decifragens / μs)**
32	$2^{32} = 4{,}3 \times 10^9$	35,8 minutos	2,15 milissegundos
54	$2^{54} = 7{,}2 \times 10^{16}$	1142 anos	10,01 horas
128	$2^{128} = 3{,}4 \times 10^{38}$	$5{,}4 \times 10^{24}$ anos	$5{,}4 \times 10^{18}$ anos
168	$2^{168} = 3{,}7 \times 10^{50}$	$5{,}9 \times 10^{36}$ anos	$5{,}9 \times 10^{30}$ anos

Fonte: (FILHO, 2004)

Percebendo a Tabela 8 chegamos a conclusão que um ataque de força bruta á um algoritmo criptográfico que utiliza chave de até 54 *bits* é plenamente possível, utilizando um equipamento capaz de decifrar 10^6 mensagens por microssegundo. Por exemplo, no sistema GSM a chave utilizada é de 64 *bits*, porém a efetividade da chave normalmente é de 40 *bits* (BRANQUINHO, 2016).

2.6.3 Criptografia Simétrica

Na criptografia de chave simétrica os processos de cifragem e decifragem são feitos com uma única chave, ou seja, tanto o remetente quanto o destinatário usam a mesma chave.

Em algoritmos simétricos, ocorre o chamado "problema de distribuição de chaves". A chave tem de ser enviada para todos os usuários autorizados antes que as mensagens possam ser trocadas. Isso resulta num atraso de tempo e possibilita que a chave chegue a um possível atacante. Abaixo a Figura 19 que ilustra o processo.

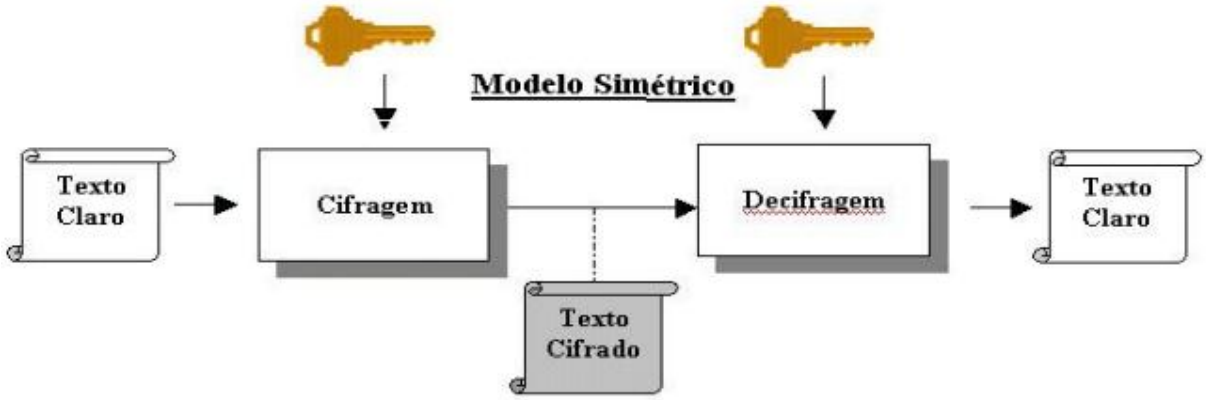

Figura 19 - Criptografia de chave simétrica
Fonte: (ORDONEZ *et al.*, 2005)

Criptografia de algoritmo de blocos

A criptografia em blocos ou cifra de blocos opera sobre blocos de dados. O texto antes de ser cifrado é dividido em blocos que variam normalmente de 8 a 16 *bytes* que serão cifrados ou decifrados. Se o texto não completa o número de *bytes* de um bloco, este é preenchido com dados conhecidos (geralmente valor zero “0”) até completar o número de *bytes* do bloco, cujo tamanho já é predefinido.

Portanto, os algoritmos de blocos no modo mais básico (*Electronic CodeBook* - ECB) processam os dados como um conjunto de *bits*, são os mais rápidos e seguros para a comunicação digital, vide a Figura 20 abaixo.

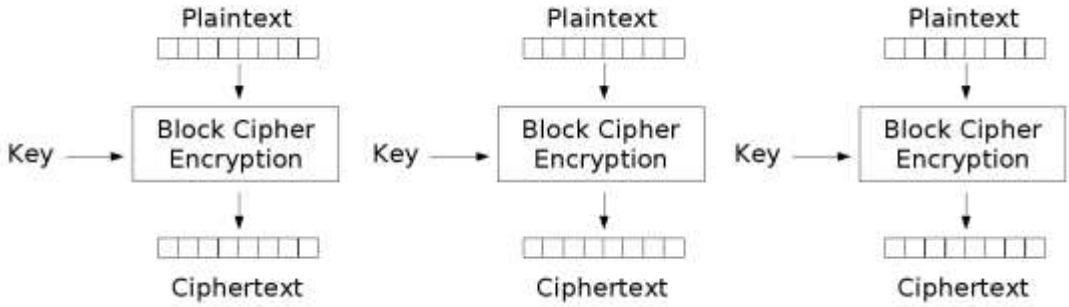

Figura 20 - Criptografia ECB
Fonte: (WIKIPÉDIA, 2008)

Tem ainda como vantagem que os blocos podem ser codificados fora de ordem, o que permite a paralelização, além de ser resistente a erros, uma vez que um bloco não depende do anterior. Entretanto, possuem como desvantagem que se a mensagem possui padrões repetitivos nos blocos, o texto cifrado também o apresentará, o que facilita o serviço do criptoanalista, a Figura 21 demonstra o problema deste algoritmo na criptografia de uma imagem.

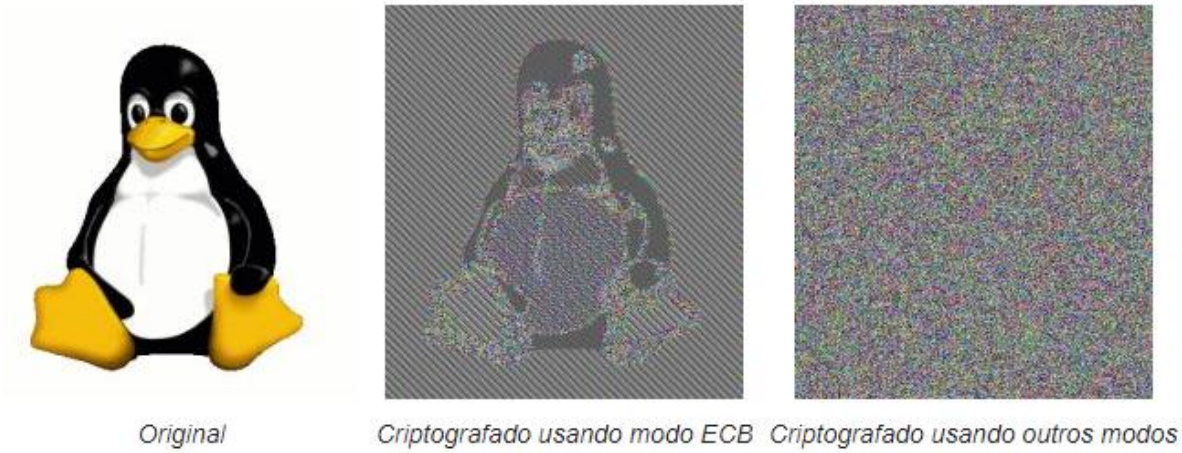

Figura 21 - Criptografia ECB e outros modos
Fonte: (WIKIPÉDIA, 2008)

Um problema na cifra de bloco é que se o mesmo bloco de texto simples aparecer mais de uma vez, a cifra gerada será a mesma facilitando o ataque ao texto cifrado. Para resolver este problema são utilizados os modos de realimentação. O modo mais comum de realimentação é a cifragem de blocos por encadeamento (*Cipher Block Chaining* - CBC). Neste modo é realizada uma operação de XOR do bloco atual de texto simples com o bloco

anterior de texto cifrado. Para o primeiro bloco não há bloco anterior de texto cifrado assim, faz-se uma XOR com um vetor de inicialização (IV), conforme a Figura 22.

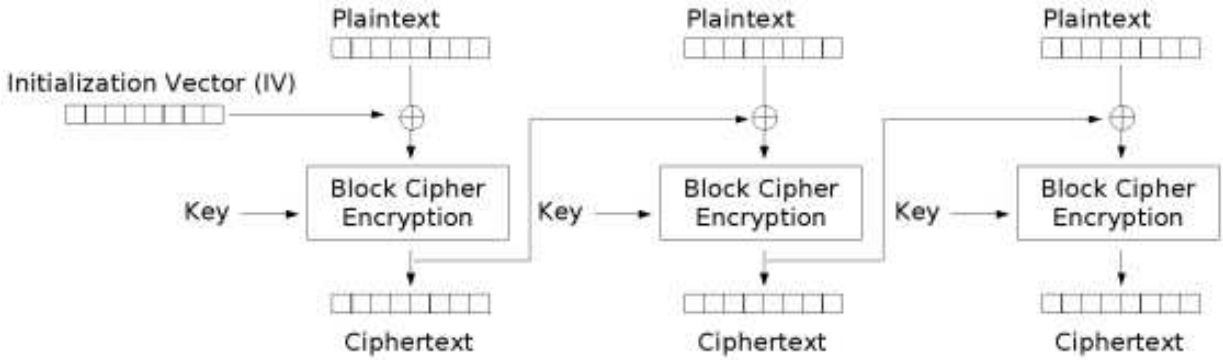

Figura 22 - Criptografia CBC
Fonte: (WIKIPÉDIA, 2008)

Este modo não adiciona nenhuma segurança extra. Apenas evita o problema citado da cifra de bloco.

Criptografia de algoritmo de fluxo

Trata-se de uma cifra de chave simétrica que combina os *bits* do texto claro com um fluxo de *bits*, um a um, sem precisar completar blocos como acontecia na cifra de blocos, e esta operação com unidades pequenas torna o algoritmo extremamente rápido, contudo, a cifra de fluxo pode ser projetada para trabalhar sobre unidades menores do que o *bit* ou unidades maiores que o *byte*.

Neste algoritmo uma chave será inserida no gerador de bits pseudoaleatório (algoritmo que gera uma sequência de números, os quais são aproximadamente independentes um dos outros), assim gerando o fluxo de *bits* conhecido como *keystream* e posteriormente são utilizados operações XOR com o texto claro e a *keystream*, veja a Figura 23.

Note que esta cifra é bem semelhante com o **OTP** (*one-time pad*) a diferença é que um *one-time pad* utiliza números realmente aleatórios e chaves do mesmo tamanho da mensagem, o que o torna **incondicionalmente seguro**, enquanto uma cifra de fluxo utiliza números pseudoaleatórios e chaves bem menores que a mensagem.

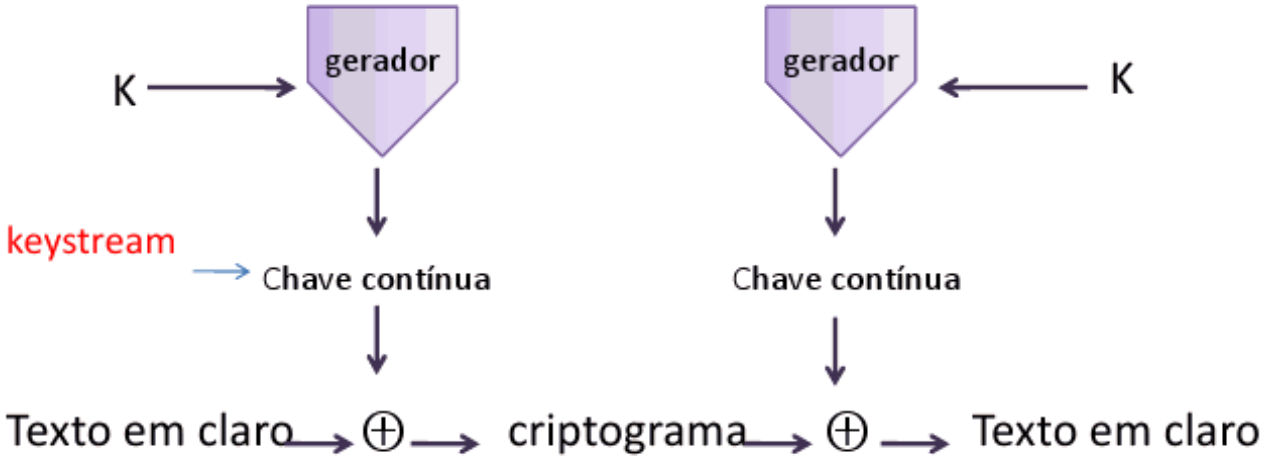

Figura 23 - Cifra de fluxo
Fonte: (PINHEIRO, 2010)

2.6.4 Criptografia Assimétrica

A criptografia assimétrica soluciona o problema da distribuição de chaves através do uso de **chaves públicas**. A primeira vez em que realmente foi possível uma comunicação criptográfica em um meio inseguro, sem precisar trafegar o segredo, foi em 1976 por Whitfield Diffie e Martin Hellman como intuito de resolver o problema da distribuição de chaves.

Neste novo sistema, cada entidade tem um par de chaves chamadas: chave pública e chave privada. A chave pública é divulgada enquanto que a chave privada só é conhecida pela sua própria entidade e esta chave privada nunca irá trafegar no meio. Para mandar uma mensagem privada, o transmissor encripta a mensagem usando a chave pública do destinatário pretendido, que deverá usar a sua respectiva chave privada para conseguir decriptar a mensagem original, a Figura 24 representa o esquema gráfico da criptografia assimétrica.

Atualmente, um dos mecanismos de autenticação mais usados é a assinatura digital, a qual utiliza dos conceitos de criptografia assimétrica. A assinatura digital é uma mensagem que só uma entidade poderia produzir, mas que todos possam verificar que a entidade realmente é quem diz ser.

Além disso, satisfaz a condição de **irretratabilidade**, porquanto a assinatura assegura o nome do autor, que funciona como uma assinatura de documentos, ou seja, que determinada entidade concordou com o que estava escrito. Isso também evita que a pessoa que assinou a mensagem depois possa se livrar de responsabilidades, alegando que a mensagem foi forjada.

Um exemplo de criptossistema de chave pública (criptografia assimétrica) é o RSA (Rivest-Shamir-Adelman) atualmente da empresa RSA Data Security, Inc.

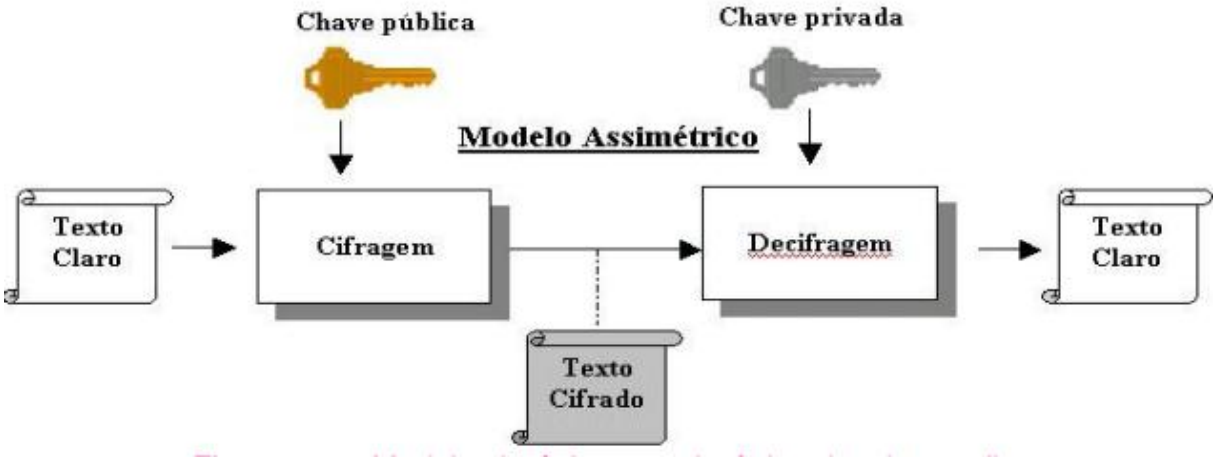

Figura 24 - Criptografia de chave assimétrica
Fonte: (ORDONEZ *et al.*, 2005)

2.6.5 Hashs

Uma função de *hash* é uma via de mão única que gera uma saída de tamanho fixo e sempre igual para o mesmo dado, e uma vez aplicado um *hash* em uma entrada é computacionalmente impossível determinar a entrada a partir de sua saída (BRANQUINHO, 2016, p. 37), e, além disso, qualquer alteração mínima no dado altera completamente o *hash*. Os exemplos de algoritmos de *hash* comumente utilizados são o MD5 e SHA-1. Uma forma de atacar os *hashes*, são as *rainbow tables* (tabelas pré-configurada para engenharia reversa de funções *hash*, usualmente para quebrar as senhas).

2.6.6 Funções de Segurança na Rede GSM

A (ETSI, 2017) estabelece funções básicas de segurança no GSM, os quais serão destacados a seguir.

Identificação do Assinante Móvel

A identificação do assinante é suprida pelo cartão SIM, cada cartão tem um registro no banco de dados da operadora que o forneceu, possui também um **cartão de identidade de**

circuito integrado (ICCID) que corresponde um número de 18 dígitos usando para identificar o *hardware*.

Todavia o que garante a identificação do usuário na rede da operadora é o **IMSI**, já discutido em seções anteriores, o dito-cujo identifica o país, rede e o assinante, porquanto dada a sua importância, a mesmo deve ser mantido em segredo. Existe também a chave de 128 *bits* $\mathbf{K_i}$ (chave esta que nunca irá ser transmitida), utilizada para autenticação e geração da chave de sessão $\mathbf{K_c}$ (64 *bits*) e por fim o cartão SIM também pode armazenar dados do usuário como: contatos, SMS etc.

Privacidade e Obscuridade de Informações do Assinante Móvel

A privacidade do assinante está intimamente ligada ao **IMSI** (o qual já foi visto que esta identidade é única) e da localização do usuário na rede o **LAI**. Para cumprir os requisitos de privacidade é gerado uma identidade temporária chamada **TMSI**, o qual efetivamente garante o sigilo, pois ainda que exista um ataque na rede e capture o TMSI, essa identidade é temporária.

Porém em alguns casos ocorre que o IMSI é enviado, estes são: quando o TMSI não pode ser transmitido por ter sido invalidado, ou quando a MS encontra-se desligada e acaba de ser ligada e necessariamente tem que enviar o IMSI para associação com o TMSI correspondente.

Autenticação do Assinante Móvel na Rede

A autenticação dos assinantes se dá pelo "protocolo desafio-resposta", protocolo esse alimentado pela chave K_i (armazenada somente no SIM e no Auc) e o algoritmo criptográfico proprietário conhecido como A3 (que utiliza a **segurança por obscuridade)**. O detalhamento de todo o processo de autenticação será visto em uma subseção própria.

Confidencialidade dos Dados Trafegados

A confidencialidade dos canais GSM é garantida por meio da encriptação, mais especificamente o algoritmo criptográfico de fluxo e também proprietário A5 (tem por premissa a **segurança por obscuridade**), algoritmo esse que se encontra no ME, diferente do A3 e A8 que estão no cartão SIM.

Basicamente o A5 irá utilizar a chave de sessão K_c de 64 *bits* gerada até então pelo A8, para criptografar todos os dados entre a MS e o BTS, maiores detalhes sobre o processo de encriptação serão visto na próxima subseção.

A família criptográfica A5, utiliza diversos tipos de grau de segurança, são eles:

- A5/0, significa nenhuma encriptação, isto é, os dados são transmitidos em texto claro;
- A5/1, constitui a encriptação padrão;
- A5/2, estabelece uma versão propositalmente mais fraca que o A5/1;
- A5/3, implementa uma encriptação mais forte.

2.6.7 Autenticação e Encriptação na Rede GSM

Um dos pontos principais segurança do GSM, é o seu modo de compartilhar as chaves. A chave de autenticação de usuário (K_i) é armazenada somente no SIM e no AuC, e nunca será transmitida pela rede.

O processo de autenticação e encriptação no sistema GSM utilizam os seguintes algoritmos que são relacionados entre si:

- A3: usado para autenticação de usuários;
- A5: usado para criptografia;
- A8: usado para geração de chave de sessão (K_c).

Os algoritmos A3 e A8 estão gravados no SIM e no AuC, enquanto que o algoritmo A5 está gravado no ME e na BTS. O processo de autenticação pode ser iniciado toda vez que há uma atualização da localização do móvel, supondo uma MS que acaba de ser ligada numa rede em que a MS é visitante, logo o protocolo de desafio-resposta vai ser iniciado e vamos ter os seguintes passos:

1. A MS transmite o IMSI, o MSC/VLR determina que é necessário realizar a autenticação do usuário, ele envia o IMSI ao HLR, de posse das informações o AuC (integrado ao HLR) da *home network* fica encarregado do processo a partir de agora;

2. O AuC seleciona um número aleatório de 128 *bits* chamado RAND. O AuC aplica o RAND juntamente com a chave K_i 128 *bits* e o algoritmo A3 obtendo como resultado

um valor chamado SRES (*Signed Responde*) de 32 *bits*. Da mesma forma, a chave de sessão K_c de 64 *bits* é gerada utilizando-se o algoritmo A8 com a chave K_i e o RAND;

3. O HLR armazena para cada MS os três parâmetros (RAND, SRES, K_c), e quando solicitado os repassa para o MSC/VLR;

4. O MSC/ VLR informa ao MS que execute o processo de autenticação. Para isso envia ao MS pela interface Um o parâmetro RAND;

5. O móvel executa o algoritmo A3, usando a sua chave Ki armazenada no SIM, o valor RAND recebido, obtendo como resultado um valor SRES. Este último valor é retornado ao MSC/VLR. O móvel aplica também o RAND e a chave K_i no algoritmo A8 para obter a chave de sessão de 64 *bits* K_c. Teoricamente igual à chave K_c obtida pelo AuC no passo 2;

6. A rede visitada compara o SRES que recebeu como uma resposta da estação móvel com o SRES recebido anteriormente do AuC e armazenado no VLR. Se os dois valores de SRES forem idênticos, a comunicação será autorizada; caso contrário, será rejeitada;

7. Quando o protocolo de autenticação é completado com sucesso, a BTS e o MS estão prontos para começar o processo de criptografia de voz/dados transmitidos entre elas utilizando a chave K_c (nota-se que a chave de K_c não é transmitida entre a BTS e a MS, sendo gerada independentemente em cada uma);

8. O algoritmo A5 recebe a chave de sessão como entrada e gera uma sequência de 114 *bits* (*keystream*) que passa por uma porta ou-exclusivo com os dois blocos de dados de 57 *bits* transmitidos em um único *timeslot* (FILHO, 2004). “Nota-se que, enquanto a chave K_c permanecer constante em uma sessão GSM, a sequência de 114 *bits* mudará em tempos, devido a mudança do número do *timeslot* TDMA” (FILHO, 2004, p. 65).

As Figuras Figura 25 e Figura 26 abaixo ilustram o processo de autenticação e criptografia do GSM.

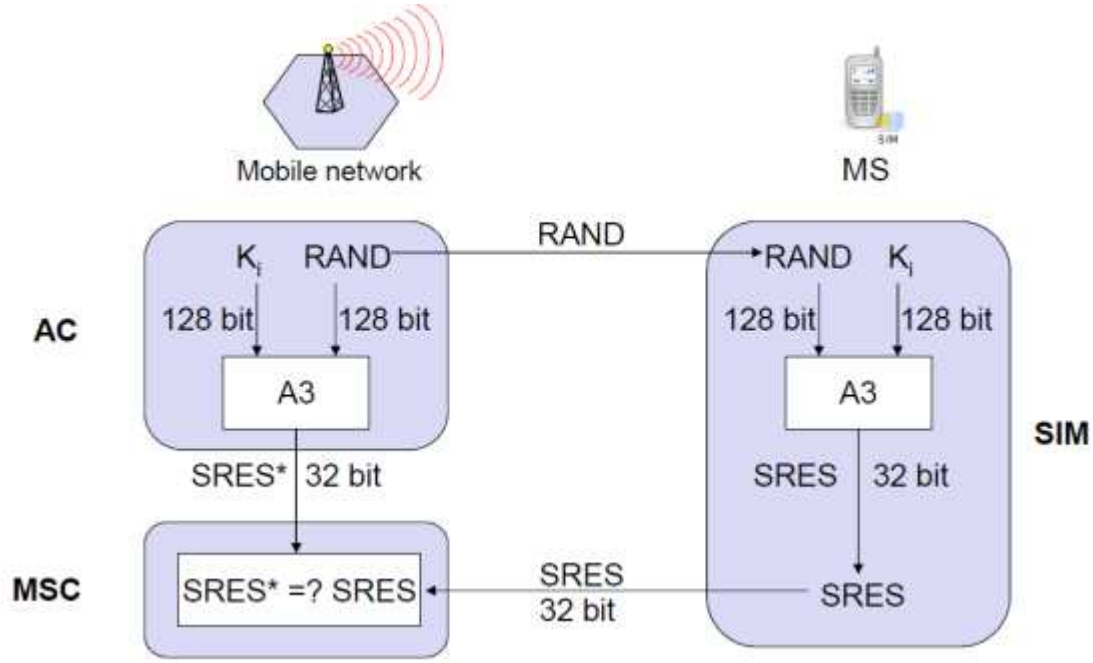

Figura 25 - Autenticação do GSM
Fonte: (GLENDRANGE; HOVE; HVIDEBERG, 2010, p. 55)

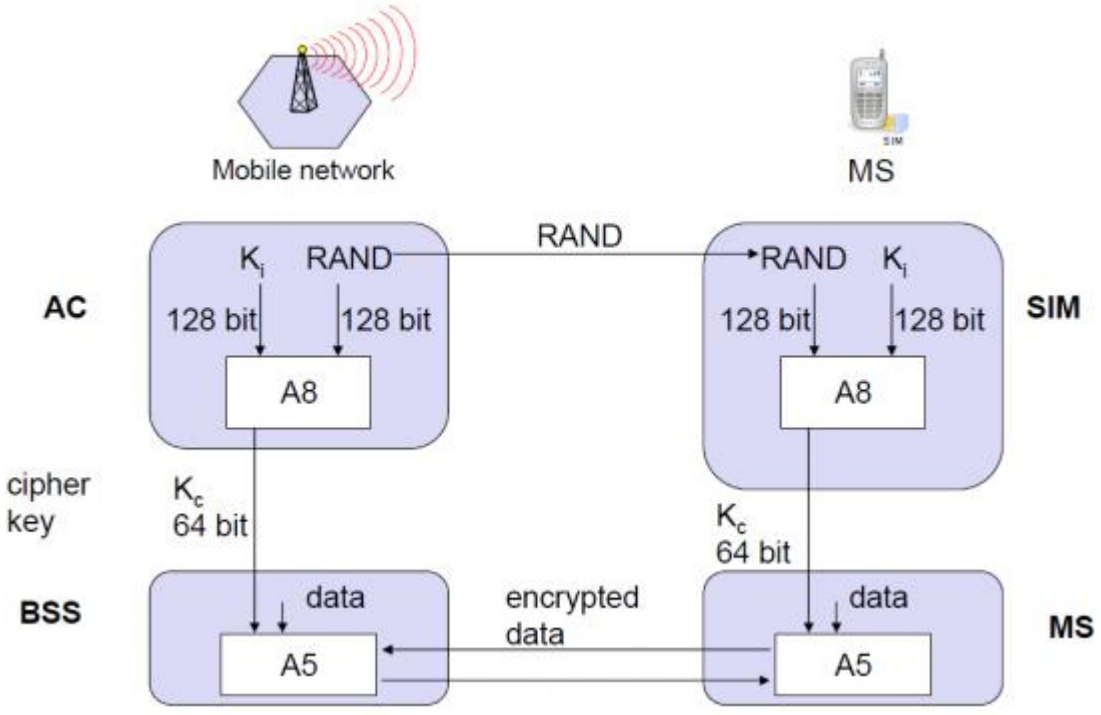

Figura 26 - Encriptação na rede GSM
Fonte: (GLENDRANGE; HOVE; HVIDEBERG, 2010, p. 56)

3 ANÁLISE DA SEGURANÇA DO SISTEMA GSM

3.1 *Software* e *Hardware* para Análise do GSM

Os *softwares* de análise da rede GSM são na sua maioria de código aberto e desenvolvidas especialmente para sistemas **GNU/Linux**, pois somente algumas ferramentas tem compatibilidade com sistemas **Microsoft Windows**, porém não fornecem suporte ou não têm todas as funcionalidades da versão de sistemas Linux.

As distribuições recomendadas para a análise de sistemas celulares são amplamente conhecidas e tem um número expressivo de usuários, como por exemplo: Debian, Ubuntu (baseado no Debian) e Kali Linux (distribuição GNU/Linux baseada no Debian, e é voltado principalmente para auditoria e segurança de computadores em geral).

Os periféricos para a análise de sistemas de telefonia móvel atualmente se tornaram muito mais acessíveis e livres. Entre eles se destacam o SDR (*Software Defined Radio*) por seu custo relativamente baixo e a vasta documentação e exemplos de programação para o mesmo.

3.1.1 Rádio Definido por *Software*

O rádio definido por *software* basicamente é um conjunto de tecnologias de *hardware* e *software*, onde algumas ou todas as funções operacionais do rádio são implementadas através de *software* ou *firmware*, executado em tecnologias de processamento programáveis, por exemplo, um FPGA[27] (SILVA *et al.*, 2015).

O SDR apresenta algumas vantagens em relação ao rádio convencional, por exemplo como a maioria das funcionalidades em SDR é implementada em *software*, o equipamento pode receber novas funcionalidades ou correções de *bug*, no convencional caso encontramos um *bug* em um módulo de demodulação do sinal de um celular, a única solução é mudar o componente ou em alguns casos é mais flexível e basta atualizar o *firmware* (SILVA *et al.*, 2015).

[27] FPGA - *Field-Programmable Gate Array* (ou ainda matriz de portas programáveis) é um dispositivo lógico programável que suporta a implementação de circuitos digitais.

Outra vantagem seria o reuso de *hardware*, pois cada país tem suas próprias regras no que diz respeito às comunicações (modulação diferente, faixas de frequências, potência de transmissão etc), assim as empresas são obrigadas a fabricar diferentes versões de um mesmo *hardware*, ao invés de criar um único *hardware* programável, onde as características de cada região poderiam ser implementadas via *software* (SILVA *et al.*, 2015). Um exemplo seria os diversos padrões de TV digital são adotados em cada região do mundo, produzindo o mesmo tipo de rádio e programando de acordo com cada país, a amortização dos preços é bem maior.

O SDR também apresenta algumas desvantagens como: problemas de interoperabilidade, a proliferação de diferentes implementações pode causar muitos problemas, é o caso de um ponto de acesso que tem que lidar com os pacotes com formatos desconhecidos, ou enfrentar uma rede com uma mistura de estações que implementam o 802.11 tradicional e outras implementações customizadas (SILVA *et al.*, 2015). Atualmente, uma parte ainda significativa da funcionalidade dos transceptores é implementada em *hardware*, de modo que é impossível modificá-la sem o acesso físico ao *hardware*. No SDR as funcionalidades são movidas para o *software*, e estas podem ser exploradas. Por exemplo, um *hacker* poderia inutilizar uma placa Wi-Fi ou um roteador transformando-os em geradores de ruídos para causar interferência (SILVA *et al.*, 2015).

USRP

O *Universal Software Radio Peripheral* (USRP) é um *framework* para o desenvolvimento de rádios digitais, proporcionando uma infraestrutura completa para o processamento de sinais (ETTUS RESEARCH, 2017).

USRP *Hardware Driver* (UHD) é o driver de código aberto para toda a família do USRP, para o desenvolvimento de aplicativos podem ser utilizadas ferramentas como: RFNoC, GNU Radio, LabVIEW e Matlab/Simulink, juntamente com os sistemas operacionais: Linux, Windows e Mac OS.

Uma placa USRP muito popular e de alto desempenho é a **Ettus Research USRP Networked Series N210**. O USRP N210 oferece alta largura de banda e processamento. Este se destina a aplicações de comunicação exigentes. Conforme (ETTUS RESEARCH, 2017), as especificações do produto são:

- A Xilinx Spartan-3A DSP 3400 FPGA;
- Interface *Gigabit Ethernet*;
- Dual 100 MS/s, 14 *bits*, conversor analógico-digital;
- Dual 400 MS/s, 16-*bit*, conversor digital-para-analógico;
- Bloqueio flexível e sincronização;
- Entradas externas para sinais de 10 MHz e 1 PPS (SMA);
- Oscilador GPS opcional;
- Ettus Research MIMO *Cable* que pode ser usado para sincronizar dois dispositivos USRP;
- Suporte para comandos cronometrados e alinhamento LO com a placa filha SBX.

Figura 27 - USRP N210
Fonte: (ETTUS RESEARCH, 2017)

RTL-SDR

O RTL-SDR é um SDR muito barato (aproximadamente US$ 20), com base no *chipset* **RTL2832U**, este chip é muito empregado por placas de TV digital, mas *hobbistas* descobriram que o mesmo pode ser utilizado como uma ótima plataforma SDR. Essa capacidade de *scanner* teria custado centenas ou mesmo milhares de dólares há alguns anos atrás. O mesmo também é frequentemente referido como RTL2832U, DVB-T SDR, RTL *dongle* ou *Software Defined Radio*.

O modelo **Terratec TStick Plus With Realtek RTL2832U/Elonics E4000** tem as seguintes características:

- Faixa de frequência: aproximadamente 52 MHz - 2200 MHz, com um "apagão" entre 1100-1250 MHz;
- Largura de banda máxima: 3 MHz (máximo estável);
- TX/RX: RX (somente opera em modo *downlink*, isto é, na recepção).

A Figura 28 abaixo mostra uma visão geral sobre o RTL-SDR.

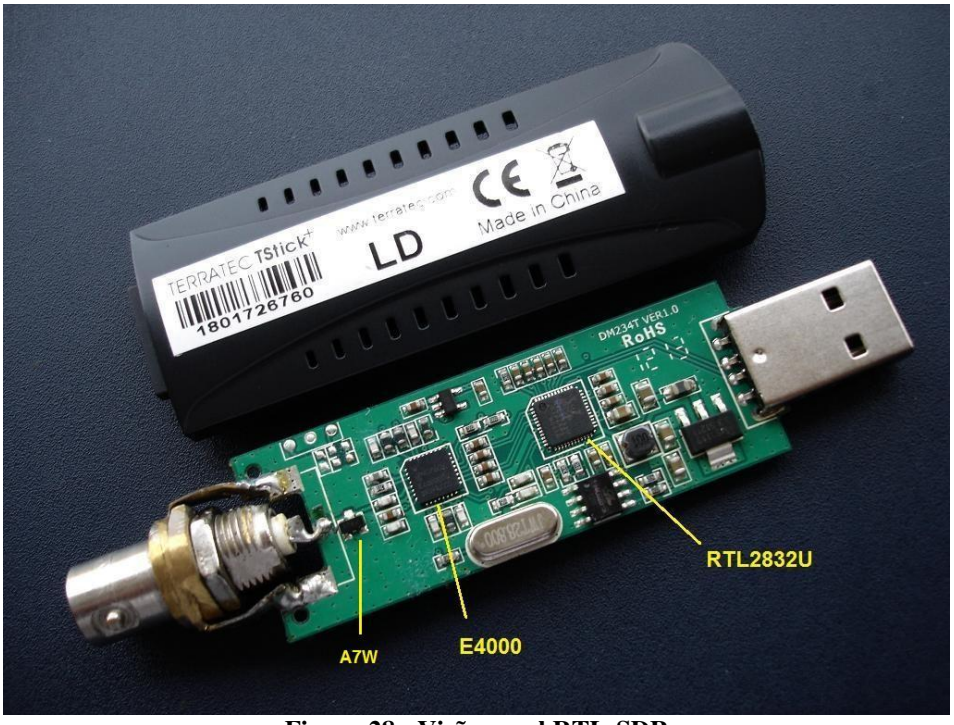

Figura 28 - Visão geral RTL-SDR
Fonte: (RTL- SDR, 2014)

3.1.2 *Softwares* para Análise

GNU Radio

O GNU Radio é um *software* gratuito e de código aberto, que fornece um kit de ferramentas para processamento de sinal. Ele pode ser usado com *hardware* de RF externo de baixo custo, para criar rádios definidos por *software*, ou sem *hardware* em um ambiente similar a simulação. É amplamente utilizado em ambientes de pesquisa, indústria, academia e governos, para pesquisas de comunicações sem fio e sistemas de rádio.

O GNU Radio executa todo o processamento do sinal. Você pode usá-lo para escrever aplicações para receber e transmitir dados com *hardware* de rádio ou para criar aplicações baseadas em simulação. O GNU Radio possui filtros, osciladores, elementos de sincronização, equalizadores, demoduladores, decodificadores e muitos outros tipos de blocos que normalmente são encontrados em sistemas de processamento de sinais.

Geralmente as aplicações de rádio GNU podem ser escritas em linguagem de programação como **Python**, enquanto o processamento de sinal crítico de desempenho é implementado utilizando C++.

Kalibrate

Para transmitir e receber em sistemas celulares, o sincronismo e a frequência têm que serem rigorosamente precisas, e para isso é importante calibrar.

Kalibrate, ou **kal**, pode procurar por estações de base GSM em uma determinada faixa de frequência e podem usar essas estações base para calcular o deslocamento de frequência do oscilador local.

GR-GSM

O GR-GSM (sucessor do **AirProbe)** é um projeto de *software open-source* para a análise da interface Um. Contém um conjunto de ferramentas para monitorar, receptar e decodificar o tráfego GSM. Funciona com qualquer rádio definido por *software*, por exemplo os *dongles* de TV baseados em RTL2832 amplamente disponíveis, e que são popularmente usados como receptores de rádio de *software* de baixo custo.

O GR-GSM permite que todos estudem os protocolos usados na interface de rádio móvel do GSM, ressaltando que esta ferramenta tem um desenvolvimento lento, e algumas funções como a captura do sinal GSM em *uplink* e a decodificação do canal com salto em frequência (*frequency-hopping*) ainda estão em fase de desenvolvimento até a data presente deste trabalho.

OpenBTS

O OpenBTS é uma implementação de código aberto do BTS GSM, desenvolvido pela Range Networks (IEDEMA, 2015). Foi a primeira implementação da interface Um disponível gratuitamente. O objetivo do projeto é simplificar e reduzir o custo da implantação de uma rede GSM. Com o mundo em desenvolvimento e áreas difíceis de alcançar pelas operadoras, surgia assim o interesse em criar redes de telefonia baratas e acessíveis a todos. Além do *software* livre, também necessitamos de um dispositivo USRP relativamente barato, como o Ettus N200, que custa cerca de 1500$, e um laptop para executar o *software*, para começar a operar uma rede móvel.

O OpenBTS permite telefones celulares compatíveis com GSM sejam usados como *end-points* SIP (*Session Initiation Protocol*) em redes VoIP[28]. Assim o OpenBTS substitui a infraestrutura convencional da rede. Em vez de depender de controladores de estação base externos para gerenciamento de recursos de rádio, as unidades do OpenBTS executam esta função internamente. Em vez de reencaminhar o tráfego de chamadas através do MSC de um operador, o OpenBTS redireciona chamadas via SIP para VoIP ou PABX.

Podemos utilizar o Asterisk para garantir a conectividade das chamadas via VoiP, o SIP *Message Queue* (SMQueue) para o gerenciamento de SMS e o SIP *Authorization Server* (SIPAuthServe) para implementar a autenticação dos assinantes, a Figura 29 ilustra estes módulos.

[28] VoIP - *Voice over Internet Protocol*

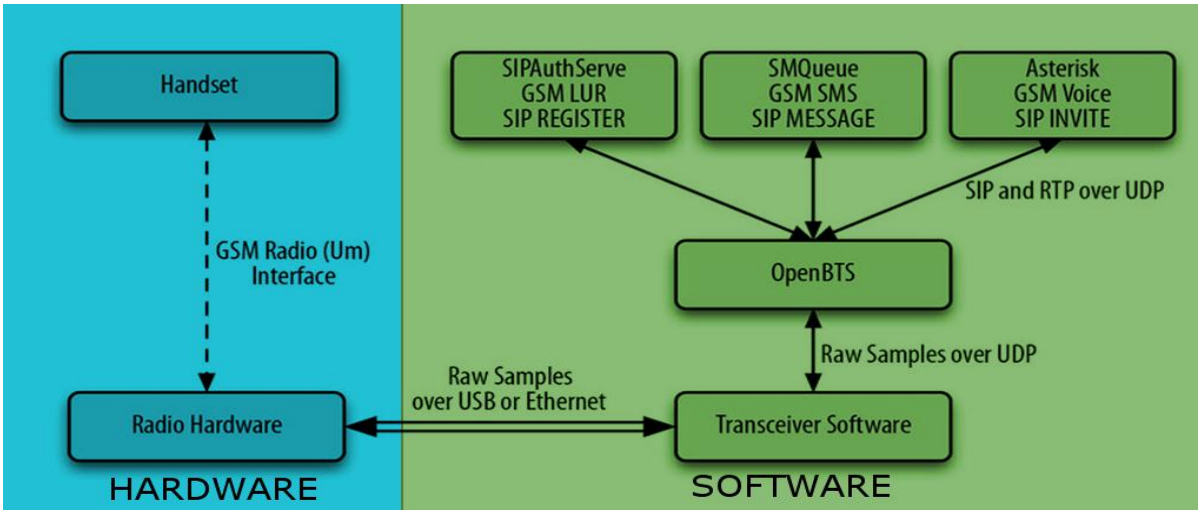

Figura 29 - Esquema rede móvel com OpenBTS
Fonte: (IEDEMA, 2015)

Asterisk

O Asterisk é um PABX (*Private Automatic Branch Exchange*) completo implementado em *software*. Ele é executado em Linux, BSD, Windows (emulado) e MAC OS e fornece todos os recursos que você esperaria de um PABX e muito mais. O Asterisk utiliza a tecnologia voz sobre IP (VoIP) em quatro protocolos e pode interoperar com quase todos os equipamentos de telefonia, usando *hardware* relativamente barato.

O Asterisk inclui muitos recursos disponíveis nos sistemas PABX comerciais e proprietários: correio de voz, conferência, resposta de voz interativa (menus do telefone) e distribuição automática de chamadas e os usuários também podem criar novas funcionalidades.

Osmocom

Osmocom (*Open source mobile communications*) é na verdade um "abrigo" para vários projetos relacionados com comunicações móveis. Isso inclui *software* e ferramentas que implementam uma variedade de padrões de comunicação móvel, incluindo GSM.

OsmocomBB é um *firmware* livre de *baseband* GSM, e implementa a pilha de protocolo GSM do lado do telefone móvel, incluindo camada 1 (TDMA / FDMA), camada 2 (LAPDm) e camada 3 (RR / MM / CC). Funciona como fosse uma placa de rede *ethernet*, em que é possível conectar o telefone ao computador e visualizar o tráfego da rede móvel, assim verificamos como funciona a rede GSM internamente, com base apenas em *software* livre.

Existem vários outros projetos como: **OsmoBTS / OsmoBSC / OsmoNITB / OsmoSGSN /** etc. O OsmoBTS é uma implementação de *software* livre da BTS (funciona na Camada 2 e 3), já o OpenBSC e os projetos relacionados são uma implementação de elementos de rede GSM/GPRS, incluindo o BSC, mas também incluindo o SGSN, e algo que chamamos de NITB (*Network In The Box*), que basicamente engloba todos os elementos da arquitetura da rede em um único módulo minimalista. Abaixo a ilustração dos módulos Osmocom.

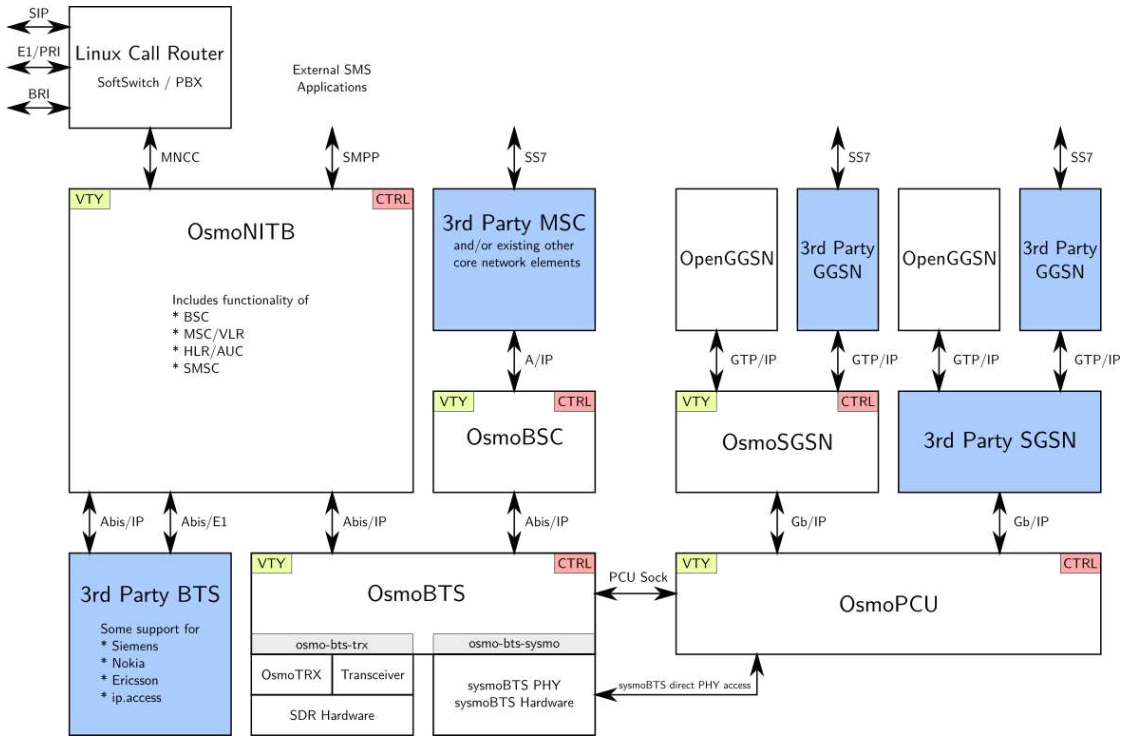

Figura 30 - Diagrama projetos Osmocom
Fonte: (OSMOCOM, 2015)

Wireshark

O Wireshark é um analisador de pacotes de código aberto e gratuito. Ele é usado para solução de problemas de rede, análise, desenvolvimento de *software*, protocolos de comunicação e educação.

O Wireshark permite que o usuário coloque os controladores de interface de rede em modo promíscuo (se suportado pelo controlador de interface de rede), para que eles possam ver todo o tráfego visível, incluindo o tráfego *unicast* não enviado para o endereço MAC do controlador de rede.

Esta ferramenta implementou o **GSMTAP**, que é um formato de pseudo-cabeçalho, utilizado para encapsular os quadros da interface Um em pacotes UDP/IP. Ele tem um propósito semelhante ao do *radiotap* do 802.11 (Wi-Fi). O GSMTAP é implementado como um dissecador do Wireshark e está ligado de forma estática à porta UDP (4729).

3.2 Vulnerabilidades

Serão descritas nesta seção algumas vulnerabilidades de segurança já bem conhecidas pela comunidade de segurança, do sistema GSM. Agora se faz necessário um adendo, este trabalho busca enriquecer ao máximo possível as possiblidades de ataque à rede, porém para a real execução destes, há a necessidade de pedir autorização ao órgão regulador de telecomunicações (ANATEL) e reproduzir os ataques em um ambiente controlado, caso contrário poderá estar infringindo a "lei do grampo digital" (BRASIL, 1996). As vulnerabilidades não discutidas podem-se tornar objetos de pesquisa para trabalhos futuros.

Uma distinção importante entre esses ataques é se eles são ativos ou passivos. Ataques ativos descritos aqui sempre exige a transmissão pelo atacante. Isso significa que os ataques ativos são muito mais visíveis. Também na maioria dos países, essas transmissões em si já são ilegais (BROEK, 2010).

3.2.1 Escuta Passiva (*Eavesdropping*)

É um ataque que tenta capturar, descriptografar e decodificar o tráfego GSM passivamente. Para isso, o tráfego da interface aérea (do BTS a MS) do GSM deve ser interceptado utilizando um **SDR** em conjunto com a ferramenta **GR-GSM**.

Vale ressaltar que a maioria dos SDR mais baratos só suportam o modo *downlink*, e mesmo que se utilizem rádios de *hardware* superior como o USRP, ainda sim não poderíamos capturar o tráfego *uplink* com a ferramenta GR-GSM, posto que esta função ainda está em desenvolvimento. Outro problema que pode ocorrer é a ativação do salto em frequência em BTSs, dificultando a análise, pois o interceptador deverá escolher entre duas abordagens: capturar todos os "*burst*" em diferentes frequências e reuni-los ou então seguir corretamente o salto em frequência, contudo a função de captura com salto de frequência também não está disponível no GR-GSM.

O GSM inovou justamente com a inclusão da criptografia na interface Um, e isto implica que somente é possível analisar o tráfego legível até antes do comando de cifragem de dados da rede. Em relação aos dados encriptados, o GR-GSM é capaz de decodificar o tráfego se o modo de cifragem utilizado for A5/0 (sem encriptação) ou então se o atacante fornecer a chave de sessão K_c (não importando o tipo de cifra A5/1,A5/2 ou A5/3).

Tendo o aparelho móvel em mãos a extração do K_c se torna muito trivial e pode ser feito de várias maneiras, por exemplo: nos celulares **BlackBerry** existe um modo de *Engineering* o qual detalha várias informações importantes , dentre elas é a chave de sessão K_c. Diversos fabricantes de celulares instalam uma espécie de interface de modem no celular o qual é possível enviar comandos AT (PALEARI; FATTORI, 2015), bastando utilizar um *software* de comunicação serial e enviar os comandos específicos para obter a chave de sessão (XENAKIS; NTANTOGIAN, 2015). Também temos a possibilidade de utilizar um leitor de SIM no computador e verificar a chave K_c, sendo este último método bem mais prático.

Caso não tenhamos o aparelho para fazer a extração manual da chave de sessão, resta a possibilidade de aproveitar que o algoritmo A5 não é mais seguro criptograficamente, primeiramente porque a sua principal faceta, a segurança por obscuridade, não surtiu o resultado esperado e está disponível na internet uma possível implementação do algoritmo A5 (BRICENO; GOLDBERG; WAGNER, 1999), e além disso houveram diversos ataques, que serão relatados a seguir.

Os autores Elad Barkan, Eli Biham e Nathan Keller publicaram vários ataques contra a criptografia GSM (BARKAN; BIHAM; KELLE, 2003). O primeiro é um ataque ativo, os telefones GSM podem ser convencidos a usar o tipo de cifra mais fraca (A5/2), podendo ser quebrada facilmente. Um segundo ataque no A5/1 é referente é do tipo compensação de memória-tempo de texto cifrado, que exige uma grande quantidade de *rainbow tables* geradas, porém as tabelas nunca foram divulgadas publicamente.

Em 2007, as Universidades de Bochum e Kiel iniciaram um projeto de pesquisa para criar um acelerador criptográfico com base em **FPGA** massivamente paralelo denominado **COPACOBANA** (GUNEYSU *et al.*, 2007). E esta foi a primeira solução comercialmente disponível, usando técnicas rápidas de troca de memória-tempo que poderiam ser usadas para atacar os algoritmos A5/1 e A5/2, utilizados na criptografia GSM, que na verdade são os mesmos princípios que (BARKAN; BIHAM; KELLE, 2003).

Em 2008, o grupo *The Hackers Choice* (**THC**) lançou um projeto para desenvolver um ataque prático sobre A5/1 (HULTON; MULLER, 2008). O ataque requer a construção de uma grande tabela de aproximadamente 3 TB. O grupo esperava poder gravar qualquer chamada GSM ou SMS criptografado com A5/1, e em cerca de 3-5 minutos derivar a chave de criptografia e, portanto, ouvir a chamada e lê um SMS em claro. Mas as tabelas não foram divulgadas

The A5/1 Security Project foi lançado por Karsten Nohl e Chris Paget, como uma reimplementação do trabalho de 2008 da THC. O projeto teve como objetivo distribuir a geração de *rainbow tables* de forma que qualquer pessoa possa se voluntariar e começar a gerar tabelas, o objetivo era calcular e compartilhar 2 TB de tabelas. O script gerador das tabelas era específico para dispositivos Nvidia que suportam **CUDA**[29], e foi disponibilizado no site do projeto, e as tabelas finalizadas foram compartilhadas via Torrent e Google Drive (PAGET; NOHL, 2010).

Em 2010 na conferência da Black Hat, Karsten Nohl utilizou a ferramenta utilitária **Kraken** (desenvolvida por Frank A. Stevenson (COMPUTEWORLD, 2010)) e as *rainbow tables* de 2 TB, para descriptografar o tráfego GSM capturado. O mesmo, conseguiu encontrar a chave secreta da sessão com cerca de 90% de probabilidade em minutos, utilizando um PC com duas GPUs (NOHL, 2010). Ele explicou que a ferramenta baseia-se no "ataque de texto conhecido", isto é, quando o atacante tem acesso a um conjunto de textos em claro e os correspondentes textos cifrados.

Recomenda-se como meio de mitigação a utilização da **cifra A5/3** pelas operadoras (pois ainda não existem relatos de ataques bem sucedidos contra esta cifra) ou ainda a utilização de VPN, túnel SSH e aplicativos de criptografia ponta-a-ponta.

3.2.2 Estação Rádio Base Falsa (*Fake Base Station*)

Se um MS estiver conectado a uma estação rádio base falsa (BTS), o invasor pode interceptar todas as comunicações feitas pelo MS e fingir ser a pessoa contatada. O atacante também pode iniciar qualquer tipo de comunicação (SMS ou ligações telefônicas) para o MS, apresentando como se fosse de qualquer origem.

---

[29] CUDA – É uma API destinada a computação paralela em GPUs Nvidia.

Este tipo de ataque só é possível porque as estações bases no sistema GSM não se autenticam, somente as MS. E tudo o que é necessário para o atacante é utilizar um bloqueador de sinal para obstruir o sinal da operadora, e paralelo a isso iniciar a transmissão da BTS falsa utilizando o *software* **OpenBTS** em uma frequência igual a do provedor da vítima BTS e com o MCC+MNC da operadora. 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 (PAULA; BRESSAN; ABE, 2013).

O celular executa um *cell re-selection*, um *location update request* e *attach request*, com isso a falsa rede obtém seus parâmetros para a autenticação. Obviamente os emuladores da falsa rede trabalharão sem cifragem (A5/0) e propositalmente autenticam esse usuário, que consequentemente, se conecta na BTS falsa (PAULA; BRESSAN; ABE, 2013).

Como a vítima não está mais conectado ao seu provedor, nenhuma chamada pelo MS irá completar e serão todas encaminhadas a caixa postal, e nem aparecerão nas faturas do plano qualquer registro. Salvo que a rede falsa pode ser interconectada aos demais sistemas de telefonia móvel, fixa e dados, utilizando *softwares* de PABX baseados em VoIP como o **Asterisk**, deste modo a vitima não será privada dos serviços móveis .

Com o auxilio de ferramentas como o Wireshark pode ser usado para espionar as chamadas de voz, basta selecionar: "*Statistics*>VoIP *Calls*". Igualmente, o Asterisk tem a função **MixMonitor**, em que se realizar a escuta e gravação de todo o tráfego de voz entre a MS e a estação falsa criada.

Como meio de mitigação ao ataque de estações falsas, existem aplicativos móveis como o **Android IMSI-Catcher Detector** ou **SnoopSnitch** (ambos para sistema operacional android) que monitoram várias informações sobre a BTS conectada e a avalia como sendo legítima ou falsa (TEIXEIRA, 2016). Contudo o modo mais eficaz de proteger contra este tipo de ataque é a utilização de padrões de redes móveis mais atuais como o 3G ou 4G, já que ambos implementam autenticação da rede e a integridades dos dados.

3.2.3 Ataques de Autenticação

No contexto GSM, os ataques de autenticidade normalmente implicam em um atacante tentando se passar por um assinante. Para representar um assinante, um atacante teria que

passar pela autenticação, contudo para passar desta fase o invasor precisa ser capaz de calcular a resposta correta do **protocolo desafio-resposta** explicado anteriormente, para isso o atacante precisa da chave secreta K_i, mas esta chave só é armazenada na memória do Cartão SIM e no centro de autenticação das operadoras (AuC).

A chave secreta nunca é transmitida e não deve haver nenhuma maneira da chave secreta ser obtida a partir do IMSI (caso este tenha sido interceptado). Supondo que as operadoras protejam o AuC adequadamente, então a recuperação do K_i por este meio deve ser impossível. Um invasor pode tentar clonar o SIM de um assinante e então se identificar como se fosse a vítima, permitindo-lhe fazer chamadas que serão cobradas à vítima.

Clonar o SIM significa basicamente encontrar sua chave secreta K_i. A chave secreta é usada como entrada para o A3 e algoritmo A8. Na implementação A3/A8 original (chamada de **COMP128v1**) foi feito engenharia reversa e a implementação está disponível online (BRICENO; GOLDBERG; WAGNER, 1999), logo após, uma fraqueza do algoritmo foi descoberta, provando novamente os efeitos devastadores da segurança por obscuridade (BROEK, 2010, p. 95). De acordo com (BRICENO; GOLDBERG; WAGNER, 1999) o **RAND** e a resposta **SRES**, originados do protocolo desafio-resposta pode-se realmente obter informações sobre a chave secreta. E com cerca de 150.000 desafios escolhidos, a chave secreta pode ser revelada.

A maneira mais fácil de realizar esse ataque é com acesso físico ao cartão SIM. Um invasor com um leitor de SIM e um *software* apropriado poderia revelar a chave secreta em pouco tempo. Porém várias versões mais recentes foram introduzidas como a **COMP128v2** e **COMP128v3**, impossibilitando até o momento este tipo de ataque.

3.2.4 Ataques de Quebra de Privacidade e Localização

O IMSI é o identificador principal no sistema GSM, os objetivos de segurança da rede móvel indicam claramente que o IMSI não deve ser enviado pela rede, exceto durante o procedimento de registro inicial (quando a MS é ligada) ou após uma identificação TMSI com falha.

Para proteger o IMSI, ele é imediatamente associado a um TMSI, e este é transmitido pela rede, sendo o identificador temporário para esta MS específica. Como o IMSI identifica de forma exclusiva um MS, e os MSs são vinculados a pessoas, logo o vazamento do IMSI

pode quebrar o anonimato do assinante. Se um invasor puder vincular o IMSI a uma localização, então ele pode quebrar a privacidade da localização. Como o vazamento do IMSI pode comprometer a privacidade da localização e da identidade, é imprescindível que a relação **IMSI↔TMSI** permaneça em segredo.

IMSI *Catcher*

Conhecido também como coletor de IMSI, como o próprio nome diz, é um dispositivo que serve para descobrir os IMSIs dos MSs. Como vimos o IMSI é transmitido abertamente pelos MSs e o BTS durante o registro inicial. Então, neste ponto, o IMSI pode ser interceptado. Interceptar esses IMSIs pode ser feito de duas maneiras, passivo e ativo.

Na interceptação passiva, um invasor pode simplesmente escutar o canal **AGCH** de um BTS. Após uma MS enviar uma mensagem que inclui o seu IMSI, no **RACH**, o BTS responderá concedendo ao MS em um canal de sinalização e esta resposta vem no AGCH contendo o IMSI. Então, ouvir esse canal resultará em alguns IMSIs capturados, embora o atacante provavelmente não saiba de quem são esses IMSIs.

Uma maneira muito mais fácil seria um ataque ativa, utilizando uma estação rádio base falsa. Se um atacante começar a transmitir utilizando a estação falsa, com os códigos MCC e MNC da operadora da vítima, em uma localidade próxima ao MS, então o MS tentará se registrar na estação falsa.

Provavelmente, o MS começará a enviar seu TMSI (obtido anteriormente na rede verdadeira) e a estação rádio base falsa irá rejeitar, resultando no MS transmitindo seu IMSI. Naturalmente, o atacante tem que garantir que a transmissão da sua estação falsa seja mais potente do que a da operadora.

3.2.5 Ataque de Negação de Serviço (DoS)

Dieter Spaar demonstrou um ataque de Negação de Serviço (DoS) contra um BTS (SPAAR, 2009). Para este ataque ele utilizou o único telefone conhecido (**TSM30**) que possui um chip de *baseband* reprogramável (**TI Calypso**). Todos os outros chips de *baseband* são proprietários e difíceis de reprogramar. O código-fonte juntamente com o compilador para o TI Calypso vazou, tornando a reprogramação do TSM30 bem mais fácil. Atualmente o **OsmocomBB** é utilizado como *firmware* de *baseband* em celulares compatíveis.

Este ataque é direcionado ao procedimento de registro. Como lembrete, o procedimento de inscrição é iniciado pelo MS enviando um RACH. O BTS irá então reservar um canal dedicado para a sinalização para o MS e responder com um comando de "*immediate assignment*" no AGCH, e então o MS pode começar a se comunicar com o BTS.

Neste ataque, o TSM30 é instruído para transmitir continuamente no RACH. Sem nunca analisar as respostas no AGCH. Os efeitos desse ataque são duplos, primeiro as transmissões contínuas no RACH podem perturbar as transmissões de MSs genuínos. E em segundo lugar todas as solicitações RACH solicitarão a reserva de um canal dedicado para a sinalização. Esses canais de sinalização são liberados após algum tempo, se ficarem inativos, no entanto, a reserva demora o tempo suficiente para esgotar o fornecimento de canais.

Este ataque torna um BTS inútil para todos os MSs que tentem se conectar a ele. O ataque não influencia as conexões abertas, se um MS já estiver em uma conversa via BTS, essa conversa não será afetada. Mas quando a conversa terminar será muito difícil solicitar um canal para a comunicação.

O pesquisador não relatou soluções para este ataque, mas provavelmente envolveria uma atualização dos protocolos para impedir a alocação imediata do canal, similarmente ao que acontece com a mitigação do ataque **SYN *Flood***[30].

[30] SYN Flood - É uma forma de ataque de negação de serviço, na qual o atacante envia uma sequência de requisições SYN para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI.

4 CONCLUSÃO

Mesmo que o sistema GSM tenha sido criado com foco em prover uma segurança bem maior que o padrão anterior (AMPS) e se tornado um sucesso e resistente a ataques na época em que foi concebido, com o tempo surgiram várias explorações de lacunas da rede, na realidade essas vulnerabilidades sempre existiram, mas o *hardware* de rádio e o alto processamento, estes ainda não existiam ou eram poucos acessíveis na época do advento do GSM, outro problema é que muitas especificações do GSM são proprietárias dificultando a análise deste sistema pela comunidade de segurança, enfatizando novamente que a segurança por obscuridade é desastrosa.

Como já foi visto, a rede sofreu inúmeros ataques bem sucedidos e amplamente divulgados na internet. Consequentemente a insegurança deste padrão é um consenso entre os pesquisadores de segurança. Contemporaneamente a vigilância, privacidade e a segurança são assuntos de relevância mundial, posto que agências de espionagem e grupos *hackers* são uma realidade incontestável nos dias de hoje. As lacunas desta rede móvel contribuem e muito para a insegurança dos assinantes, porquanto este referido trabalho diante de todos os fatos relatados, recomenda como medida de segurança a desativação do GSM, já que os padrões mais atuais e seguros como 3G ou 4G, mantém a compatibilidade com o supracitado, assim configurando uma brecha: o invasor nega o serviço do sistema mais seguro e ataca o sistema vulnerável.

Em recomendações a trabalhos futuros, tem-se outras linhas de pesquisa, como por exemplo operar uma estação rádio base GSM falsa, utilizando o OpenBTS ou YateBTS em conjunto com o Asterisk (para não privar o assinante dos serviços de telefonia). Outra recomendação, é a implementação do Kraken para descobrir a chave de sessão em cifras A5/1 e a sua versão mais fraca A5/2 utilizando as *rainbow tables*, disponíveis gratuitamente na internet. Por fim, a utilização do **OsmocomBB**, uma implementação de *software open source baseband*, com o intuito de verificar o tráfego (tanto *uplink* como *downlink*) da rede móvel, e assim compreender todos os aspectos do funcionamento interno do GSM.

BIBLIOGRAFIA

ACADEMY, R. THE DIFFERENCE BETWEEN FDMA AND TDMA. **taitradioacademy**, 2012. Disponivel em: <https://www.taitradioacademy.com/topic/the-difference-between-fdma-and-tdma-1>. Acesso em: 30 nov. 2017.

ANACOM. [S.l.]. 2000.

ANATEL. Anatel Relatório Anual 2006. **anatel**, 2006. Disponivel em: <http://www.anatel.gov.br/hotsites/relatorio_anual_2006/cap_03.htm>. Acesso em: 20 out. 2017.

ANATEL. **Clonagem de Telefone Celular**. [S.l.]. 2007.

BARKAN, E.; BIHAM, E.; KELLE, N. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted. **cs.technion.ac.il**, 2003. Disponivel em: <http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf>. Acesso em: 1 dez. 2017.

BRANQUINHO, P. D. O. **Redes GSM e GPRS**. São paulo: [s.n.], 2016.

BRASIL. LEI Nº 9.296, DE 24 DE JULHO DE 1996. **Lei do Grampo Digital**, Brasília , jul 1996.

BRICENO, M.; GOLDBERG, I.; WAGNER, D. Uma Implementação do Algoritmo GSM A3A8. **scard**, 1999. Disponivel em: <http://www.scard.org/gsm/a3a8.txt>. Acesso em: 1 dez. 2017.

BRICENO, M.; GOLDBERG, I.; WAGNER, D. Uma implementação pedagógica de A5/1. **scard**, 1999. Disponivel em: <http://www.scard.org/gsm/a51.html>. Acesso em: 1 dez. 2017.

BROEK, F. V. D. Catching and Understanding. **GSM-Signals**, 2010. Disponivel em: <http://www.cs.ru.nl/~F.vandenBroek/scriptie.pdf>. Acesso em: 30 nov. 2017.

CARLÉSIMO, D. P. ANÁLISE DE VULNERABILIDADES DOS SISTEMAS GSM/GPRS POR MEIO DE RECURSOS COMPLEMENTARES DE HARDWARE E SOFTWARE , Santo André - SP, 19 Dezembro 2013.

CASAROTTO, N. F. **Análise de investimentos:** matemática financeira, engenharia econômica, tomada de decisão, estratégia empresarial. 9ª. ed. São Paulo: Atlas, 2000.

CASTRO, M. C. F. D. Técnicas de Acesso Múltiplo para Comunicações Wireless. **Comunicações Celulares**, Porto Algre, 2013.

CHIARA, I. D. **Normas de documentação aplicadas à área de Saúde**. Rio de Janeiro: E-papers, 2008.

COMPUTEWORLD. New 'Kraken' GSM-cracking software is released. **computerworld**, 2010. Disponivel em: <https://www.computerworld.com/article/2519495/mobile-wireless/new--kraken--gsm-cracking-software-is-released.html>. Acesso em: 1 dez. 2017.

ETSI. ETSI - European Telecommunications Standards Institute. **ETSI**, 2017. Disponivel em: <http://www.etsi.org/>. Acesso em: 20 out. 2017.

ETTUS RESEARCH. USRP. **ettus**, 2017. Disponivel em: <https://www.ettus.com/>. Acesso em: 1 dez. 2017.

FILHO, E. R. P. AUTENTIÇÃO E OUTROS ASPECTOS DE SEGURANÇA EM SISTEMAS CELULARES. **pgee.ime.eb**, 2004. Disponivel em: <http://www.pgee.ime.eb.br/pdf/elmano_pinheiro.pdf>. Acesso em: 1 dez. 2017.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw Hill, 2008.

GLENDRANGE, M.; HOVE, K.; HVIDEBERG, E. **Decoding GSM**. Norwegian University of Science and Technology. [S.l.]. 2010.

GOODRICH, M. T.; TAMASSIA, R. **Introdução à Segurança de Computadores**. São Paulo: BOOKMAN EDITORA LTDA, 2013.

GUINTHER, R. Estrutura do canal de rádio. **gta.ufrj**, 2012. Disponivel em: <https://www.gta.ufrj.br/seminarios/semin2002_1/roberta/gsm/radio.htm>. Acesso em: 30 nov. 2017.

GUNEYSU, T. et al. Cryptanalysis with COPACOBANA. **sciengines**, 2007. Disponivel em: <http://www.sciengines.com/copacobana/paper/TC_COPACOBANA.pdf>. Acesso em: 1 dez. 2017.

HALL, T. O que é Frequency Hopping - FHSS? **TELECOM HALL**, 2011. Disponivel em: <http://www.telecomhall.com/br/o-que-e-frequency-hopping-fhss.aspx>. Acesso em: 1 out. 2017.

HULTON, D.; MULLER, S. The A5 Cracking Project. **events**, 2008. Disponivel em: <https://events.ccc.de/camp/2007/Fahrplan/events/2015.en.html>. Acesso em: 1 dez. 2017.

IEDEMA, M. **Getting Started with OpenBTS**. [S.l.]: O'Reilly, 2015.

ISO/IEC. **7816-x: Identification cards - Integrated circuit cards**. IEC. [S.l.]. 2013.

MIRO, F. Celulares GSM: O mundo inteiro utiliza. **tecnoblog.net**, 2006. Disponivel em: <https://tecnoblog.net/136/celulares-gsm-o-mundo-inteiro-utiliza/>. Acesso em: 20 out. 2017.

NOHL, K. C.S. Dept. **cs.virginia.edu**, 2009. Disponivel em: <http://www.cs.virginia.edu/~kn5f/>. Acesso em: 08 out. 2017.

NOHL, K. Attacking phone privacy. **srlabs.de**, 2010. Disponivel em: <https://srlabs.de/wp-content/uploads/2010/07/Attacking.Phone_.Privacy_Karsten.Nohl_1-1.pdf>. Acesso em: 30 nov. 2017.

ORDONEZ et al. **Criptografia em Software e Hardware**. 1. ed. [S.l.]: Novatec, 2005.

OSMOCOM. Osmocom - Cellular Infrastructure. **osmocom**, 2015. Disponivel em: <https://osmocom.org/projects/openbsc/wiki>. Acesso em: 1 dez. 2017.

PAGET, C.; NOHL, K. Decrypting GSM phone calls. **srlabs**, 2010. Disponivel em: <https://srlabs.de/bites/decrypting-gsm/>. Acesso em: 1 dez. 2017.

PAIVA, C. H. A. A Burocracia no Brasil: as bases da administração pública nacional em perspectiva histórica. **SCIELO**, 2009. Disponivel em: <http://www.scielo.br/pdf/his/v28n2/27.pdf>. Acesso em: 20 out. 2017.

PALEARI, R.; FATTORI, A. Modem interface exposed via USB. **GITHUB**, 2015. Disponivel em: <https://github.com/ud2/advisories/tree/master/android/samsung/nocve-2016-0004>. Acesso em: 30 nov. 2017.

PAULA, A. S. D.; BRESSAN, M. A.; ABE, T. **SEGURANÇA EM REDES MÓVEIS**. Pontifícia Universidade Católica do Paraná. Curitiba, p. 22. 2013.

PINHEIRO, J. M. S. Cifras em Bloco e Cifras de Fluxo. **projetoderedes**, 2010. Disponivel em: <http://www.projetoderedes.com.br/artigos/artigo_cifras_em_bloco_cifras_de_fluxo.php>. Acesso em: 30 nov. 2017.

POINT, T. GSM - O Subsistema de Comutação de Rede (NSS). **tutorialspoint**, 2016. Disponivel em: <https://www.tutorialspoint.com/gsm/gsm_network_switching_subsystem.htm>. Acesso em: 30 out. 2017.

RFC 2828. IETF. **ietf.org**, 2000. Disponivel em: <https://www.ietf.org/rfc/rfc2828.txt>. Acesso em: 30 nov. 2017.

RODRIGUES; COSTA, M. E. D. Radiopropagação – Comunicações Móveis e Rádio Acesso. **wirelessbrasil**, 2000. Disponivel em: <http://www.wirelessbrasil.org/wirelessbr/colaboradores/marcio_rodrigues/>. Acesso em: 30 out. 2017.

RTL- SDR. ROUNDUP OF SOFTWARE DEFINED RADIOS. **rtl-sdr**, 2014. Disponivel em: <https://www.rtl-sdr.com/roundup-software-defined-radios/>. Acesso em: 30 nov. 2017.

SANT'ANNA, L. Os hackers avançam – e o Brasil abre a guarda. **exame.abril.com.br**, 2017. Disponivel em: <https://exame.abril.com.br/tecnologia/os-hackers-avancam-e-o-brasil-abre-a-guarda/#>. Acesso em: 14 out. 2017.

SANTOS, R. D. L. REDES GSM, GPRS, EDGE E UMTS. **gta.ufrj**, 2008. Disponivel em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/ricardo/index.html>. Acesso em: 30 out. 2017.

SCHILLER et al. Mobile Communications. **web.fe.up.pt**, 2016. Disponivel em: <https://web.fe.up.pt/~amoura/comunicacoes/GSM_UMTS.pdf>. Acesso em: 1 nov. 2017.

SILVA, C. E. T. D.; ROCHA, C. H. D.; FREIRE, V. S. Sistemas de Comunicações Pessoais GSM, Rio de Janeiro, 2014.

SILVA, E. F. R. REDE GSM. **teleco**, 2013. Disponivel em: <http://www.teleco.com.br/tutoriais/tutorialredegsm/>. Acesso em: 30 out. 2017.

SILVA, W. S. et al. Introdução a Rádios Definidos por Software com aplicações em GNU Radio. **sbrc**, 2015. Disponivel em: <http://sbrc2015.ufes.br/wp-content/uploads/Ch5.pdf>. Acesso em: 1 dez. 2017.

SPAAR, D. Playing with the GSM RF Interface. **events**, 2009. Disponivel em: <https://events.ccc.de/congress/2009/Fahrplan/attachments/1507_Playing_with_the_GSM_RF_Interface.pdf>. Acesso em: 1 dez. 2017.

STALLINGS, W. **Criptografia e Segurança de Redes**. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

STEPANOV, M. GSM Security Overview. **cs.huji**, 2013. Disponivel em: <http://www.cs.huji.ac.il/>. Acesso em: 30 out. 2017.

TEIXEIRA, L. Detectando antenas de celular espiãs. **antivigilancia**, 2016. Disponivel em: <https://antivigilancia.org/pt/2016/03/detectando-antenas-de-celular-espias/>. Acesso em: 1 dez. 2017.

TELECO. COBERTURA TELEFONIA CELULAR. **teleco**, 2017. Disponivel em: <http://www.teleco.com.br/cobertura.asp>. Acesso em: 20 out. 2017.

TELECO. Telefonia Celular- Cenário Mundial. **teleco**, 2017. Disponivel em: <http://www.teleco.com.br/tutoriais/tutorialinova1/pagina_3.asp>. Acesso em: 20 out. 2017.

TIM. PIN e PUK. **tim**, 2014. Disponivel em: <http://www.tim.com.br/sp/para-voce/atendimento/perguntas-frequentes/tim-chip/pin-e-puk>. Acesso em: 30 out. 2017.

UFF TELECOM. ARQUITETURA DA REDE GSM. **http:** //www.telecom.uff.br, 2012. Disponivel em: <http://www.telecom.uff.br/pagina/posgraduacao/Lato-Sensu/uploads/6/9/4/8/6948141/comunicaes_mveis_-_parte_2_-_gsm_rev_2012.pdf>. Acesso em: 08 out. 2017.

ULBRICH, H. J. G. Telefonia Celular. **TELECO**, 2008. Disponivel em: <http://www.teleco.com.br/tutoriais/tutorialbandcel/default.asp>. Acesso em: 1 nov. 2017.

WIKIPÉDIA. Modo de operação (criptografia). **wikipédia**, 2008. Disponivel em: <https://pt.wikipedia.org/wiki/Modo_de_opera%C3%A7%C3%A3o_(criptografia)>. Acesso em: 30 nov. 2017.

WILLASSEN, S. Y. Forensics and the GSM mobile telephone system. **utica.edu**, 2003. Disponivel em: <http://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf>. Acesso em: 30 out. 2017.

WYKES, S. M. **Criptografia Essencial:** A Jornada do Criptógrafo. [S.l.]: Elsevier, 2016.

X.800. X.800 : Security architecture for Open Systems Interconnection for CCITT applications. **International Telecommunication Union**, 1991. Disponivel em: <https://www.itu.int/rec/T-REC-X.800-199103-I/en>. Acesso em: 30 nov. 2017.

XENAKIS, C.; NTANTOGIAN, C. Attacking the Baseband Modem of Mobile Phones to Breach the Users Privacy and Network. **ccdcoe.org**, 2015. Disponivel em: <https://ccdcoe.org/cycon/2015/proceedings/16_xenakis_ntantogian.pdf>. Acesso em: 1 dez. 2017.