Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

Marcelo Alves Gabri

COMO TORNAR A EMPRESA MÓVEL: Desafios e Tendências da Computação Móvel.

Rio de Janeiro

2014

Marcelo Alves Gabri

COMO TORNAR A EMPRESA MÓVEL: Desafios e Tendências da Computação Móvel.

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Claudio Miceli de Farias, M.Sc, UFRJ, Brasil.

Rio de Janeiro

2014

Marcelo Alves Gabri

COMO TORNAR A EMPRESA MÓVEL: Desafios e Tendências da Computação Móvel.

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2014.

Claudio Miceli de Farias, M.Sc, UFRJ, Brasil

RESUMO

GABRI, Marcelo Alves. **COMO TORNAR A EMPRESA MÓVEL: Desafios e Tendências da Computação Móvel**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

Com o avanço tecnológico, constantemente são desenvolvidos novos recursos que nos permitem inúmeras possibilidades, a mobilidade é uma delas. O acesso móvel surge como um grande desafio para as empresas e introduz novos hábitos na forma de trabalho das pessoas.

Com os dispositivos móveis como smartphones e tablets o computador torna-se uma ferramenta sempre presente, e possibilita ao usuário acessar os recursos corporativos de qualquer lugar e a qualquer momento.

A mobilidade é uma forte tendência para o mundo corporativo e já é um movimento natural. Milhões de dispositivos móveis são ativados diariamente no mundo, e cada vez mais os usuários querem usar esses dispositivos na sua rotina de trabalho o que nos remete a um movimento conhecido como BYOD (*bring your own device*) que em português significa “Traga seu próprio dispositivo”.

O objetivo desse trabalho é orientar os gestores e profissionais de tecnologia da informação e comunicação (TIC) quanto às novas tecnologias e suas tendências.

Apresentando alguns padrões de infraestrutura de rede sem fio IEEE 802.11x, 802.16 e 802.20, passando pelas redes celulares 2G, 3G e 4G LTE, descrevendo como toda essa tecnologia se integra ao ambiente de trabalho, impulsionando as atividades profissionais e proporcionando melhorias para a empresa e seus usuários.

ABSTRACT

GABRI, Marcelo Alves. **COMO TORNAR A EMPRESA MÓVEL: Desafios e Tendências da Computação Móvel**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2014.

With technological advancement, new features are constantly being developed that allow us numerous opportunities, mobility is one of them. Mobile access emerges as a major challenge for companies and introduces new habits in the way people work.

With mobile devices like smartphones and tablets the computer becomes an ever-present tool, and allows the user to access corporate resources from anywhere and anytime.

Mobility is a strong tendency for the corporate world and is now a natural movement. Million mobile devices are activated daily worldwide, and more and more users want to use these devices in their routine work which brings us to a movement known as BYOD (*bring your own device*) which in Portuguese means "Bring Your Own Device ".

The aim of this work is to guide managers and professionals of information technology and communication (TIC) as the new technologies and trends.

Featuring some standard infrastructure wireless IEEE 802.11, 802.16 and 802.20 wireless, through the cellular networks 2G, 3G and 4G LTE, describing how all this technology is integrated into the workplace, boosting their professional activities and providing improvements to the company and its users.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

BYOD	Bring Your Own Device
TIC	Tecnologia da Informação e Comunicação
CM	Computação Móvel
FM	Frequency Modulation
AM	Amplitude Modulation
IMTS	Improted Mobile Telephone Service
AMPS	Advanced Mobile Phone System
TACS	Total Acess Communications System
NMT	Nordie Mobile Telephone
NAMTS	Nippon Advanced Mobile Telephone System
GSM	Group Speciale Mobile
CDPD	Celular Digital Packet Data
PCS	Personal Comunications Services
PCs	Computadores Pessoais
MDM	Mobile Device Management

SUMÁRIO

1 **INTRODUÇÃO**

A atual tecnologia de comunicação já permite que as informações sejam acessadas praticamente de qualquer lugar e a qualquer momento. Com a popularização dos dispositivos móveis, como *smartphones* e *tablets*, cada vez mais vemos a computação móvel (CM) e seus dispositivos ganharem força e espaço na rotina das pessoas, e não somente para uso pessoal, mas também como ferramenta de trabalho.

A computação móvel (CM) baseia-se no aumento da nossa capacidade de mover os serviços computacionais conosco, ou seja, o computador torna-se um dispositivo sempre presente que expande a capacidade de um usuário utilizar os serviços que um computador oferece, independentemente de sua localização. CM representa um novo paradigma computacional. Surge como a quarta revolução da computação, antecedida pelos centros de processamento de dados da década de 60, o surgimento dos terminais nos anos 70 e as redes de computadores na década de 80. A palavra-chave que define este novo paradigma é a mobilidade [6].

Combinada com a capacidade de acesso, a computação móvel tem transformado a tecnologia em uma ferramenta que pode ser carregada para qualquer lugar [6].

Agora para os profissionais de tecnologia da informação e comunicação (TIC), não basta disponibilizar os aplicativos, serviços e sistemas para os computadores da rede corporativa. Alguns desses recursos precisam estar disponíveis também para os dispositivos móveis [1].

Especialistas afirmam que a mobilidade é um caminho natural. Os *smartphones*, antes proibidos pela maior parte das empresas, estão sendo usados atualmente por centenas de profissionais em todo o mundo para acessar

informações corporativas e estar em atividade 24 horas. Os dispositivos móveis já fazem parte da rede corporativa e com eles surgem inúmeras possibilidades inovadoras de negócios e de carona surgem também os desafios e problemas [1].

Nos próximos capítulos serão apresentadas as tendências, oportunidades e desafios da CM e como as empresas estão se preparando para esse novo tempo. Também serão apresentadas algumas tecnologias e soluções para atender os desafios da mobilidade e relatar alguns casos de sucesso de empresas que apostaram na mobilidade.

Para concluir, será apresentado um estudo comparativo sobre os padrões de redes sem fio 802.11ac, 802.11ad, 802.11af. Serão abordadas as principais características das redes celulares 3G e 4G, e como toda essa tecnologia se integra ao ambiente de trabalho, proporcionando melhor experiência para o profissional e maior aproveitamento para a empresa.

1.1 HISTÓRIA E EVOLUÇÃO DA COMPUTAÇÃO MÓVEL

Alguns momentos na história são muito importantes na evolução da computação móvel. O telégrafo foi o primeiro sistema de comunicação, que em meados do século XIX, permitia a transferência de palavras faladas a longas distâncias via código Morse. Esse sistema foi baseado na comunicação com fio. Em 1901 sinais de rádio já atravessavam o Oceano Atlântico, este foi o início da comunicação sem fio.

Abaixo serão detalhados alguns pontos importantes da evolução da computação móvel [6].

- **1820:** Através de um experimento Hans Christian Oersted (1777 – 1851) descobre que a corrente elétrica produz um campo magnético. Essa

afirmação foi quantificada por Andre Marie Ampere (1775-1836), criando a Lei de Ampere.

- **1830:** Joseph Henry (1799-1878) descobre que a variação do campo magnético induz uma corrente elétrica, mas não publica o resultado. Em 1831, Michael Faraday (1791-1877) descobre independentemente esse efeito que passaria a ser conhecida como a Lei de Faraday e, mais tarde, a terceira equação de *Maxwell*.

- **1864:** James Clark Maxwell (1831-1879) modifica a Lei de Ampere, ampliando a Lei de Faraday e desenvolvem as quatro equações de Maxwell sobre campos magnéticos.

- **1876:** Alexander Graham Bell (1847-1922) inventou o telefone.

- **1887:** Heinrich Rudolph Hertz (1847-1879) detecta as ondas eletromagnéticas previstas pelas equações de *Maxwell*.

- **1896:** Guglielmo Marconi (1874-1937) inventa o primeiro receptor sem fio prático: o telégrafo sem fio.

- **1907:** Início do serviço de radiodifusão comercial transatlântico (estações terrestres imensas: antenas de 30 x 100m).

- **1914:** Início da Primeira Guerra Mundial. Rápido desenvolvimento das comunicações e sua interceptação.

- **1921:** Radiodifusão comercial entra em operação nos Estados Unidos.

- **1928:** A Polícia de Detroit introduz um sistema de acionamento de carros baseado em radiodifusão (unidirecional) na faixa de 2 MHz.

- **1933:** A FCC autoriza o uso de quatro canais na faixa de 30-40 MHz.

- **1935:** Modulação em Frequência – FM (*Frequency Modulation*) surge como alternativa para a Modulação em Amplitude – AM (*Amplitude Modulation*), reduzindo os problemas de ruídos na transmissão, ou melhor, desempenho com relação à perda de sinal, ou desvanecimento.

- **1939:** Pesquisa e uso da comunicação via rádio expande imensamente durante a Segunda Guerra Mundial.

- **1945:** AT&T Bell Labs inicia experimentos com uso de frequências mais altas com o objetivo de melhorar os serviços móveis.

- **1947:** AT&T lança o IMTS (*Improted Mobile Telephone Service*), um sistema de transmissão onde apenas uma torre de alta potência atendia uma grande área ou cidade. Em seguida, AT&T Bell Labs propõe o conceito de celular.

- **Anos 50:** Os Sistemas requerem uma elevada banda para transmissão, uma faixa de 120KHz para transmitir um circuito de voz de apenas 3 KHz. Esta faixa é reduzida pela metade. Com os transistores os equipamentos reduzem de tamanho e já são transportáveis. Nessa época os primeiros sistemas de *paging* (serviço de mensagem unidirecional) começam a surgir.

- **Anos 60**: Um Novo receptor de FM permite reduzir a banda 30 KHz, abrindo espaço para um maior número de canais de comunicação com o mesmo espectro. Bell Labs já testa técnicas de comunicação celular e surgem os primeiros aparelhos portáteis.

- **Anos 70:** A FCC aloca um espectro de frequência para os sistemas celulares. Nesse período AT&T lança o sistema celular conhecido por AMPS (*Advanced Mobile Phone System*). Inicialmente era um serviço de luxo. Destinado para uso em automóveis e de aplicação limitada tendo em vista a baixa durabilidade das baterias. Atendiam uma capacidade limitada de tráfego em um número reduzido de usuários. A primeira rede celular no mundo foi lançada no Japão em 1979.

- **1983:** O Sistema AMPS evoluiu para os padrões atuais com a primeira rede celular americana lançada em 1983, em Chicago e Baltimore. Outros sistemas similares entram em operação no mundo: TACS (*Total Acess Communications System*) no Reino Unido (1925), NMT (*Nordie Mobile Telephone Service*) na Escandinávia (1981). NAMTS (*Nippon Advanced Mobile Telephone System*) no Japão. O AMPS ainda em uso nos EUA, Brasil e grande parte do mundo, é considerado um sistema de primeira geração. A transmissão em FM, reduzida à 25khz nos anos 70 entra nos anos 90 na faixa de 10khz.

- **1991:** Validação inicial dos padrões TDMA e CDMA nos EUA. Introdução da tecnologia micro celular.

- **1992:** Introdução da tecnologia Pan Europeu GSM (*Group Speciale Mobile*).

- **1994:** Introdução ao Sistema CDPD (*Celular Digital Packet Data*). Início dos serviços PCS (*Personal Comunications Services*), CDMA e TDMA.

- **1995:** Início dos projetos de cobertura terrestre de satélites de baixa orbita, como o projeto *Iridium*.

A figura abaixo ilustra o tempo gasto por cada nova tecnologia para atingir 1milhão de usuários.

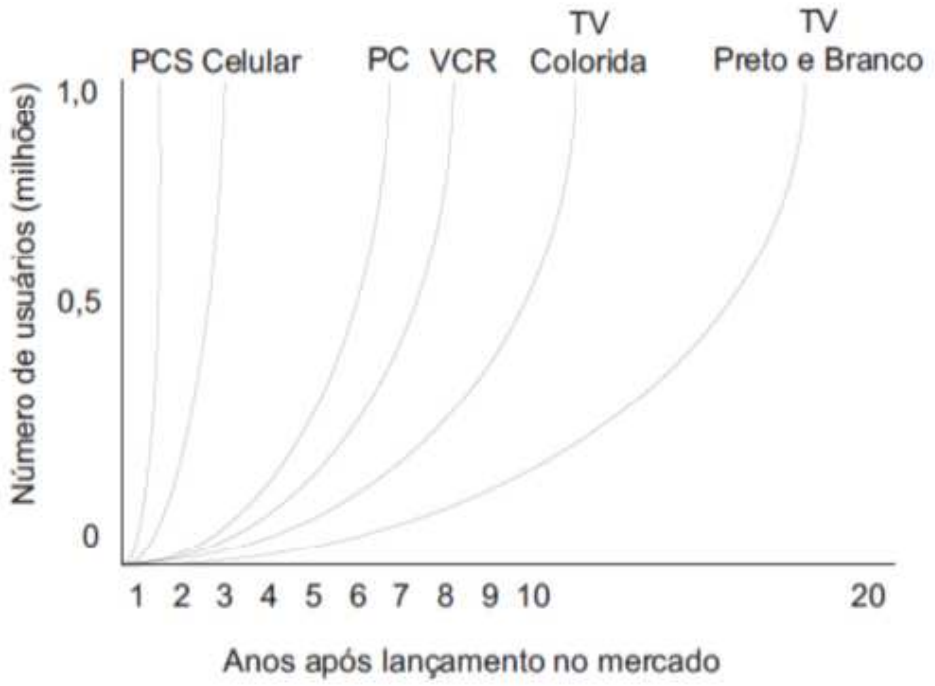

Figura 1 – Número de usuários X Anos após lançamento no mercado [6]

Cabe ressalta que em Julho 2007 Apple iniciou as vendas da primeira versão do iPhone (conhecido com IPhone 2G) e até janeiro de 2008 foram vendidos quatro milhões de aparelhos. Já a segunda versão do *smartphone* da Apple o iPhone 3G, no primeiro fim de semana após seu lançamento vendeu 1 milhão de aparelhos [13].

Traçando um comparativo rápido entre o aparelho de TV, o computador pessoal e os dispositivos móveis, percebemos que enquanto a TV (preto e branco) demorou quase 20 anos para alcançar a marca de 1 milhão de aparelhos vendidos,

o computador pessoal (PC) levou aproximadamente 6 anos e os tradicionais celulares 2 anos para atingir a mesma marca. Isso nos leva a conclusão de que a tecnologia está cada vez mais presente na rotina dos usuários e com muitas vezes com uma velocidade impressionante, como o exemplo do iPhone 3G, que em poucos dias vendeu mais de 1 milhão de aparelhos.

1.2 PRÓXIMOS CAPÍTULOS

No capítulo 2 serão apresentados os conceitos básicos das tecnologias que servem de alicerce para a computação móvel, tais como: As redes celulares de 1º, 2º, 3º e 4º geração. Serão apresentados também as principais características das redes sem fio 802.11 e seus padrões 802.11b/a/g/n/ac/ad/af.

No capítulo 3 serão apresentados detalhes das redes metropolitanas 802.16 e 802.20.

O capítulo 4 será dedicado a segurança das redes sem fio e redes celulares, serão descritos os principais mecanismos de proteção para ambas as tecnologias.

No capítulo 5, veremos como as novas tecnologias se integram ao ambiente corporativo, proporcionando um melhor aproveitamento dos recursos e atendendo melhorando a experiência do usuário final. Nesse capítulo também serão apresentados alguns casos de sucesso de empresas que inovaram e conseguiram proporcionar melhoria em suas atividades com a adoção de novas tecnologias.

Para concluir, no capítulo 6 seguem as conclusões e os trabalhos futuros.

2 **CONCEITOS BÁSICOS**

Computação móvel representa um novo paradigma computacional, com o objetivo de prover aos seus usuários acesso a rede independentemente de onde eles estejam fisicamente.

A convergência de várias tecnologias de redes sem fio no mesmo dispositivo o permite conectar-se a diferentes redes, como por exemplo: Redes celulares [14], Wi-Fi [16], *WIMAX* [15], nas próximas seções serão apresentadas as principais tecnologias de comunicação móvel e onde elas são utilizadas [19].

2.1 PRINCIPAIS TECNOLOGIAS DE REDES CELULARES

Este item descreverá as principais tecnologias em redes móveis, comparando algumas de suas características, apontando suas vantagens e desvantagens.

2.1.1 **Primeira Geração das Redes de Telefonia Celular**

As redes celulares basicamente estão voltadas para integração de voz, dados e multimídia, geralmente para usuários móveis. Para que isso seja possível, é necessário que alguns padrões sejam adotados [20].

A Primeira geração surgiu nos EUA no início dos anos 80, sistema analógico que permiti apenas transmissão de voz. Utiliza comutação por circuito (canal dedicado), com tecnologia FDMA (*Frequency Division Multiple Access*), tendo como padrão o AMPS (*Advanced Mobile Phone System*). Opera na faixa de 800MHz, e já permitia *Handoff e Roaming*, elementos essenciais para as comunicações celulares.

2.1.1.1 Handoff

Técnica utilizada por redes de comunicação móvel para tratar a transição de uma unidade móvel de uma célula para outra, de forma transparente ao usuário,

para permitir a continuidade dos serviços e aplicações em execução. Por isso, deve ser realizado de forma ágil e sem perda de dados [37].

Por exemplo, se um veículo se desloca de uma célula para uma célula adjacente, a rede entrega a ligação em curso para a nova célula, de forma tranparente para o usuário. Quem administra a entrega da ligação ativa, são as controladoras das estações base [37].

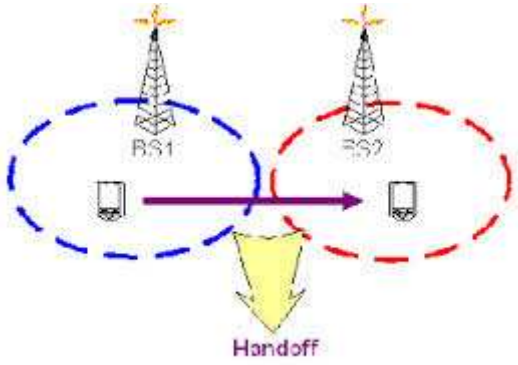

Figura 2 – Handoff, dispositivo se movendo de uma célula para outra. [21]

2.1.1.2 Roaming

Roaming pode ser definido como a capacidade de um usuário de uma rede celular se conectar em áreas fora da localidade geográfica onde está registrado, para realizar ou receber chamadas, enviar e receber dados ou utilizar outros serviços [37].

Como por exemplo, um usuário que está registrado no Rio de Janeiro, se conectar em estações rádio base em Manaus e utilizar os recursos disponíveis normalmente.

2.1.2 **Segunda Geração das Redes de Telefonia Celular – 2G**

A segunda geração, redes 2G, é a evolução do AMPS (*Advanced Mobile Phone System*), primeira geração – Surgiu da necessidade de um sistema com maior capacidade e qualidade, trazendo as seguintes vantagens sobre o sistema anterior: Codificação digital, melhor qualidade de voz, comunicação criptografada e ainda a possibilidade de navegar na internet com velocidades entre 20Kbps e 50kbps. Opera na faixa 900MHz, 1800MHz e 1900Mhz. A rede 2G mais conhecida é o GSM (*Global System for Mobile Communication*), que utiliza tecnologia TDMA (*Time Division Multiple Access*) e CDMA (*Code Division Multiple Access*) [38].

A rede 2G proporciona boa qualidade de voz a um baixo custo, e oferece suporte a um grande número de serviços, entre eles: SMS, MMS, GPRS.

Entre a segunda e a terceira geração temos o 2,5G, que usa GPRS (*General Packet Radio Service)*, evolução do GSM, oferecendo velocidade máxima de 115Kbps e EDGE (*Enhanced Data Rates for Global Evolution*), também chamada de EGPRS (*Enhanced GPRS*), pois pode aumentar em três ou quatro vezes a capacidade do GPRS [38].

2.1.3 **Terceira Geração das Redes de Telefonia Celular – 3G**

A terceira geração, redes 3G, entrou em operação em 1991, com tecnologia baseado no sistema Europeu, e com frequência de operação na faixa de 2.1Ghz. Passamos a ter velocidades entre 384kbits a 2Mbits, com isso a ênfase pelo trafego de dados estava cada vez mais evidente. Além do aumento da velocidade tivemos ainda a total compatibilidade com as redes 2G. Para a época, o 3G oferecia boa velocidade. No entanto, os avanços

tecnológicos demandavam novos desafios ao 3G, o que foi possível com o HSPA (*High Speed Packet Access*) [32].

2.1.3.1 HSPA - Speed Packet Access

O HSPA foi um avanço tecnológico que possibilitou mudanças significativas nas taxas de download e upload na tecnologia 3G. As velocidades com HSPA são de 1.8 MB/s, 3.6MB/s, 7.2MB/s ou até 14.4MB/s, embora essa última esteja disponível em poucos países [29].

Vale ressaltar que os valores mencionados são teóricos, e dificilmente são atingidos na prática, devido a interferências e situações que causam perda de velocidade. Com esse aumento de qualidade com o HSPA, o padrão é comumente chamado de 3.5G ou ainda 3G+ [30].

A grande diferença é a inclusão de dois canais novos no sistema, que atuam em alta velocidade e permitem uma melhor conexão para o usuário. Os canais chamam-se HSDPA e HSUPA, com as letras D e U representando o recebimento *(downlink)* e o envio *(uplink)* dos dados [29].

2.1.4 **Quarta Geração das Redes de Telefonia Celular – 4G**

A Quarta geração, redes 4G, em fase de implantação no Brasil, as redes 4G LTE (*Long Term Evolution*) [34], estão presentes nos estados sedes da copa do mundo. O foco é o tráfego de dados (pacotes). Podendo ser até 10 vezes mais rápida que a rede 3G. Testes com o LTE indicam picos de navegação de até 120 Mbps. Essa tecnologia já está em total operação na Europa, Ásia e EUA [34].

2.2 ARQUITETURA DAS REDES LOCAIS SEM FIO IEEE 802.11

Há alguns anos, somente era possível conectar computadores por meio de redes cabeadas. Este tipo de conexão é bastante simples, mas impõe algumas limitações, como por exemplo: A extensão e o limite de alcance do cabo, que limita a movimentação do computador. Ambientes mais complexos podem exigir adaptações na estrutura do prédio para a passagem dos cabos e a manipulação constante ou incorreta pode danificar cabos e conectores. As redes sem fio (*Wireless*) surgiram para eliminar algumas dessas limitações [14].

O padrão IEEE 802.11 define uma arquitetura para as redes sem fio, baseada na divisão da área coberta em células. Essas células são denominadas de *BSA (Basic Service Area)*. O tamanho da BSA (célula) depende das características do ambiente e da potência dos transmissores/receptores usados nos equipamentos. Abaixo estão os elementos que fazem parte do conceito da arquitetura de rede sem fio [14].

- ***BSS (Basic Service Set)*** – Conjunto Básico de Serviço, representa um grupo de estações comunicando-se por radiodifusão ou infravermelho em uma BSA.

- **Ponto de acesso *(Access Point – AP)*** – São estações especiais responsáveis pela captura das transmissões realizadas pelas estações de sua BSA, destinadas a estações localizadas em outras BSAs, retransmitindo-as, usando um sistema de distribuição.

- **Sistema de distribuição** – Representa uma infraestrutura de comunicação que interliga múltiplas BSAs para permitir a construção de redes cobrindo áreas maiores que uma célula.

- ***ESA (Extended Service Area)*** – Área de Serviço Estendida, representa a interligação de vários BSAs pelo sistema de distribuição através dos APs.

- ***ESS (Extended Service Set)*** – Conjunto de Serviço Estendido, representa um conjunto de estações formado pela união de vários BSSs conectados por um sistema de distribuição.

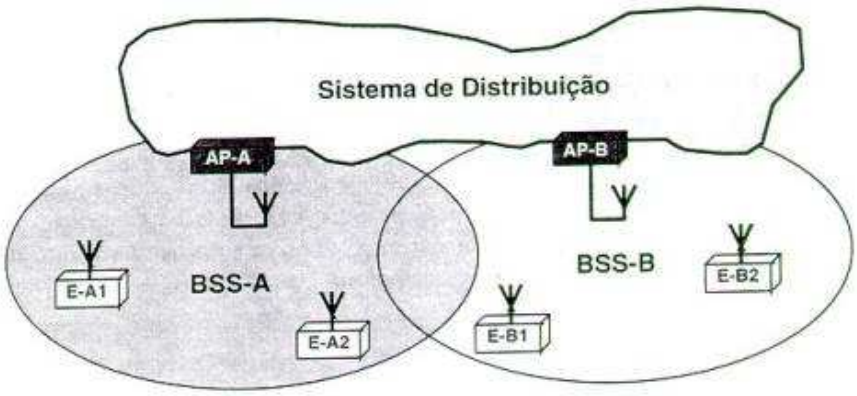

Figura 3 – União de duas BSS Formando uma ESS [14.]

2.2.1 **Rede Sem Fio IEEE 802.11b**

A primeira atualização do 802.11 foi 802.11b. A principal característica desta versão é a possibilidade de estabelecer conexões nas velocidades: 1 Mbps, 2 Mbps, 5,5 Mbps e 11 Mbps. Opera no mesmo intervalo de frequências do 802.11 original (entre 2,4 GHz e 2,4835 GHz)

A área de cobertura de uma transmissão 802.11b, teoricamente, pode chegar a 400 metros em ambientes abertos e 50 metros em lugares fechados. O alcance da transmissão pode sofrer influência de uma série de fatores, tais como objetos que causam interferência ou impedem a propagação da transmissão.

O padrão 802.11b foi o primeiro a ser adotado em larga escala, sendo, portanto, um dos responsáveis pela popularização das redes Wi-Fi.

2.2.2 **Rede Sem Fio IEEE 802.11a**

O padrão 802.11a foi disponibilizado quase na mesma época que a versão 802.11b. Sua principal característica é a possibilidade de operar com taxas de transmissão de 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps e 54 Mbps. Com alcance de cerca de 50 metros. Com frequência de operação 5 GHz, diferente do 802.11 original.

A operação nesta frequência pode ser interessante, por apresentar menos possibilidades de interferência, pois, é uma frequência pouco usada. Por outro, pode trazer problemas, já que não é uma frequência regulamentada em muitos países. Além disso, pode fazer com que haja dificuldades de comunicação com dispositivos que operam no padrão 802.11 original (entre 2,4 GHz e 2,4835 GHz).

Apesar das altas taxas de transmissão, o 802.11a não chegou a ser tão conhecido como o padrão 802.11b.

2.2.3 **Rede Sem Fio IEEE 802.11g**

O padrão 802.11g foi disponibilizado em 2003 e é tido como o "sucessor natural" da versão 802.11b, pois, é totalmente compatível com este.

O principal atrativo do padrão 802.11g é poder transmitir com taxas de até 54 Mbps, assim como acontece com o padrão 802.11a. No entanto, ao contrário desta versão, o 802.11g opera na faixa de 2,4 GHz (canais de 20 MHz) e possui praticamente o mesmo poder de cobertura do seu antecessor, o padrão 802.11b.

2.2.4 **Rede Sem Fio IEEE 802.11n**

O padrão 802.11n pretende ser o sucessor do 802.11g, tem como principal característica o uso de um esquema chamado MIMO (*Multiple-Input Multiple-Output*), capaz de aumentar consideravelmente as taxas de transferência de dados por meio da combinação de múltiplas antenas. Com isso, é possível, por exemplo, usar dois, três ou quatro emissores e receptores para o funcionamento da rede.

Uma das configurações mais comuns é o uso de APs e estações que utilizam três antenas. Com esta característica, o padrão 802.11n, é capaz transmitir na faixa de 300 Mbps e, teoricamente, podendo atingir taxas de até 600 Mbps. No modo de transmissão mais simples, com uma via de transmissão, o 802.11n pode chegar à casa dos 150 Mbps.

O padrão 802.11n pode trabalhar nas faixas de 2,4 GHz e 5 GHz, o que o torna compatível com os padrões anteriores. Alguns estudos apontam que sua área de cobertura pode passar de 400 metros.

2.2.5 **Rede Sem Fio IEEE 802.11ac**

O padrão 802.11ac pretende substituir o padrão 802.11n. A principal vantagem do 802.11ac está em sua velocidade, estimada em até 433 Mbps em modo simples, e podendo superar os 6 Gbps em um modo mais avançado utilizando múltiplas vias de transmissão (No máximo 8 antenas).

Também conhecida como 5G Wifi, o 802.11ac trabalha na frequência de 5 GHz, possui técnicas mais avançadas de modulação, trabalhando com o esquema *MU-MIMO (Multi-User MIMO)*, que permite transmissão e recepção de sinal de vários terminais, como se estes trabalhassem de maneira colaborativa, na mesma frequência [16].

MU-MIMO permite a transmissão simultânea de diferentes quadros de dados para diferentes clientes. O uso de *MU-MIMO* requer que o equipamento seja capaz de utilizar a percepção de diferentes emissores. Ele também precisa de sistemas de filas sofisticados que podem tirar proveito da oportunidade de transmitir para vários clientes, quando as condições forem adequadas.

Os avanços na tecnologia de fabricação de chips permitiram aos designers tirarem proveito de níveis adicionais de poder de processamento quando comparados com implementações anteriores do padrão 802.11. Isto permitiu o uso de técnicas de codificação mais sensíveis, além de códigos de correção de erros mais agressivos que usam menos bits de seleção, para a mesma quantidade de dados, que os padrões anteriores ao 802.11ac [16].

Embora 802.11n use canais de até 40MHz de largura, as versões anteriores do 802.11 usam tipicamente canais de 20MHz. O padrão 802.11ac usa canais de até 80MHz como padrão, com opções de 160MHz ou dois blocos de 80MHz. Para isso, é necessário adaptar alguns recursos de ajuste automático de rádio, para que os canais de maior largura de banda sejam usados somente quando necessário, para assim economizar espectro.

O IEEE 802.11ac oferece vantagens significativas sobre as implementações anteriores, e sua compatibilidade vai permitir que ele seja introduzido no ecossistema *Wi-Fi* existente com o mínimo de interrupções.

Assim como com os outros padrões 802.11, existe uma camada física PLCP e isso define uma unidade de dados PPDU.[16].

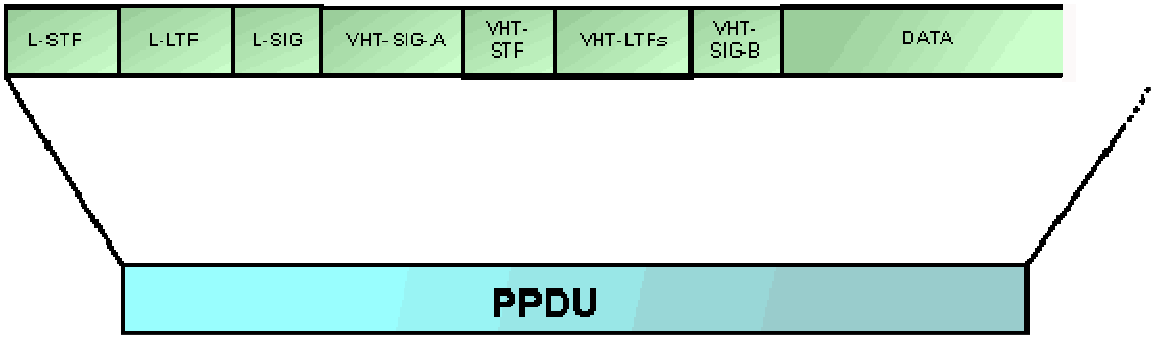

Figura 4 - IEEE 802.11ac PPDU [15]

- ***L-STF*** - Este é um campo curto, de dois símbolos de comprimento, e transmitido para compatibilidade com versões anteriores do 802.11. O campo é duplicado a cada sub-banda com rotação de fase. As subportadoras são giradas, em 90° ou 180°, em algumas sub-bandas para reduzir o pico em relação média de energia.

- ***L-LTF*** - Este é um campo longo, de dois símbolos de comprimento. Incluindo os critérios de transmissão, sendo transmitido nas sub-bandas e nas rotações de fase.

- ***L-SIG*** - Este é um campo de um símbolo de comprimento. Como a L-STF e L-LTF é um campo para compatibilidade com versões anteriores do 802.11.

- ***VHT-SIG-A*** - Este é um campo de dois símbolo de comprimento, um transmitido em BPSK e um segundo em QBPSK, ou seja, BPSK rotação de 90°. Este modo de transmissão permite a detecção au tomática de uma transmissão VHT. Contém informações que permitem ao receptor interpretar corretamente os pacotes de dados posteriores. Informações que incluem largura de banda, número de MIMO, STBC utilizado, intervalo de guarda, BCC ou codificação LDPC, MCS e informações de formação de feixe.

- ***VHT-STF*** *(VHT Short Training Field)* - Este é um campo de um símbolo de comprimento e é usada para melhorar a estimativa de controle de ganho para o funcionamento do MIMO.

- ***VHT-LTF*** *(VHT Long Training Field)* - Podem incluir 1, 2, 4, 6 ou 8 VHT-LTFS. A matriz de mapeamento de 1, 2, ou 4-VHT LTFS é o mesmo que no 802.11n enquanto as seis e oito combinações VHT-LTF foram adicionados para 802.11ac.

- ***VHT-SIG-B*** - Este campo é de detalhes da carga de dados, incluindo o comprimento, modulação de codificação, esquema para o modo multi-usuário. Bits são repetidos para cada sub-banda de 20MHz.

2.2.6 **Rede Sem Fio IEEE 802.11ad**

Enquanto o padrão IEEE 802.11ac é uma extensão do 802.11n, o padrão IEEE 802.11ad representa um paradigma completamente novo, pois, ele visa proporcionar taxas de transferência de dados superiores a 6 Gbps em frequências em torno de 60 GHz, tendo em vista que hoje os 2,4 e 5 GHz para os padrões 802.11 anteriores são muito congestionados.

Para atingir altas velocidades a tecnologia utiliza a banda ISM de 60 GHz que entrega largura de banda e garante níveis de interferência reduzidos.

Usando frequências na faixa de micro ondas, o IEEE 802.11ad tem um alcance de poucos metros. O objetivo dele e ser usado para a transferência de um volume de dados muito grande, entre pontos bem próximos, como por exemplo, a transmissão de um vídeo HD para dispositivos sem fio em uma mesma sala. Quando e necessário cobrir maiores espaços, o 802.11ac pode ser usado.

Comparando o 802.11ac e o 802.11ad, ambos fornecem transmissão de dados muito maiores do que os seus antecessores. No entanto, eles têm usos distintos. O IEEE 802.11ac é uma evolução da capacidade WLAN anterior, com a capacidade de competir diretamente com os sistemas Gigabit com fio, oferecendo muito melhor layout e flexibilidade da conexão. Em contraste com o IEEE 802.11ad, que é uma nova solução de conectividade ad-hoc, de curto alcance, que oferece taxas de transmissão extremamente altas [16].

2.2.7 **Rede Sem Fio IEEE 802.11af**

O padrão IEEE 802.11af, também conhecido como White-fi, que é o termo que está sendo usado para descrever o uso de uma tecnologia Wi-Fi dentro do

espectro não utilizado do sistema de TV (Canais UHF não usados no sistema de TV). O grupo de trabalho IEEE 802.11af foi criado para definir esse padrão [16].

Como o padrão IEEE 802.11af usa um espectro que não é alocado pelo sinal de TV, o sistema como um todo não deve causar interferência para os usuários. Com o constante avanço da tecnologia e o poder de processamento cada vez maior, este padrão se apresenta como mais uma opção de rede sem fio.

Embora o padrão ainda não esteja totalmente definido, já é possível ver muitos dos benefícios que podem ser obtidos:

Características de propagação: Tendo em vista o fato de que o sistema IEEE 802.11af irá operar em conjunto com o sistema de TV, com frequências abaixo de 1 GHz, isso permitiria alcançar grandes distancias, comparado aos sistemas Wi-Fi atuais.

Largura de banda adicional: Uma das vantagens do uso do sistema de TV é que as frequências não utilizadas poderiam ser acessadas. No entanto, para alcançar altas taxas de transferência de dados, seria necessário agregar vários canais de TV para fornecer as larguras de banda dos atuais padrões *Wi-Fi*.

Devido a esses benefícios, acredita-se que o padrão IEEE 802.11af oferece vantagens suficientes para permitir o seu desenvolvimento.

Para que o sistema IEEE 802.11af *White-fi* seja capaz de operar, é necessário garantir que o sistema não cria qualquer interferência indevida com as transmissões de televisão existentes. Para alcançar este objectivo, há uma série de tecnologias e as regras que podem ser utilizados.

Rádio cognitivo: Uma maneira pela qual um sistema IEEE 802.11af *White-fi* seria capaz de operar utilizando tecnologia de rádio cognitivo, detectar transmissões existentes e passar para canais alternativos.

Detecção geográfica: Outro método que é utilizado por muitos sistemas, é a detecção geográfica. Embora os detalhes não estejam totalmente definidos, leva em consideração uma base de dados geográfica e um conhecimento prévio dos canais que estão disponíveis, assim sistema evita usar canais ocupados.

2.3 WIMAX IEEE 802.16

O padrão WiMax IEEE 802.16, define uma interface sem fio para redes metropolitanas (*WMAN*). Foi definido pela WiMax Fórum como uma tecnologia sem fio para possibilitar conexão banda larga, mais barata, para o usuário final, uma alternativa para a conexão a cabo, ou DSL.

O WiMax Fórum é uma organização sem fins lucrativos formada para promover e certificar compatibilidade e interoperabilidade para equipamentos de acesso sem fio a banda larga, que estejam em conformidade com o padrão IEEE 802.16. Algumas de suas funções são: Certificar a conformidade de equipamentos e promover o uso da tecnologia. Dentre seus membros estão grandes empresas como a Intel, Ericsson, Motorola, France Telecom e Microsoft.

O WiMax é baseado na tecnologia do IEEE 802.16, visando oferecer conectividade fixa, nômade, portável e eventualmente móvel sem a necessidade de visada direta com uma estação base a distâncias entre 3 a 10 quilômetros geralmente. Um equipamento com certificado pelo WiMax Fórum deve ter uma

capacidade de 40 Mbps por canal, possibilitando milhares conexões a velocidade de DSL.

As redes WiMax trabalham de uma forma bem semelhante que as redes celulares que conhecemos. As estações clientes (SS – static station) se conectam através de estações base (BS – base station) em uma determinada área, que é chamada de célula. O raio da célula pode chega a quilômetros, e a união das células cobre grandes áreas.

Existem dois tipos de topologia: O padrão IEEE 802.16: PMP (ponto-multi-ponto) e a Mesh. Sendo que a PMP é definida como obrigatória e a Mesh como opcional.

ento de qualNa topologia PMP a estação base tem total controle e gerencia o tráfego dentro da célula, se uma estação quiser se comunicar com outra terá que, obrigatoriamente, passar seus dados para a BS e então a BS encaminhará os dados a estação de destino.

Na topologia Mesh existe a comunicação normal entre a estação base e as SSs, mas não há tanto controle da estação base sobre o tráfego, pois o tráfego também pode ser roteado pelas SSs. Então, não existe obrigatoriedade de ser passar os dados pela BS, as SSs podem trocar informações sem intermediários.

O PMP possui um ponto único de falha, caso a BS falhe todas as SSs da célula ficarão incomunicáveis. Já na Mesh, se a BS falhar, as SSs podem transmitir, se tornando o roteador de tráfego para a célula. Porém, o Mesh é mais complicado de se implementar que o PMP [15].

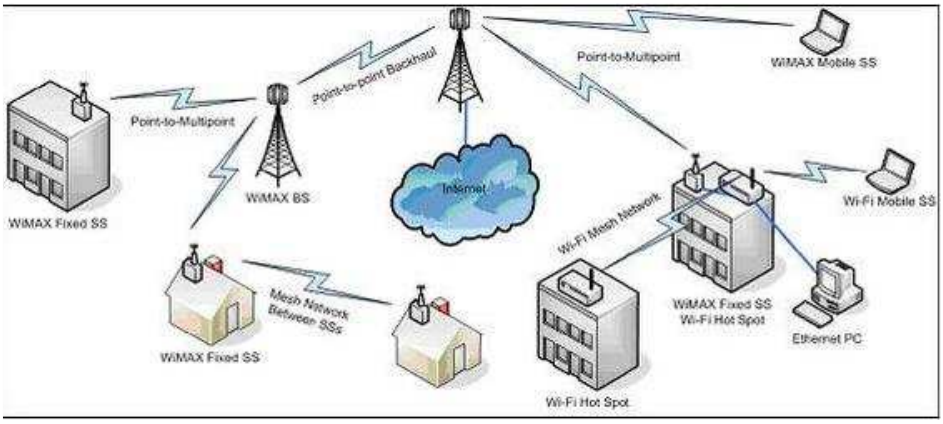

Figura 5 – Topologia de uma rede WIMAX IEEE 802.16 [15]

2.3.1 **WiMax IEEE 802.16m**

O WiMax 802.16m, já aprovado pelo *Institute of Electrical and Electronics Engineers*, pode proporcionar velocidades de download de mais de 300. O IEEE 802.16m, também conhecido como *WirelessMAN-Advanced* ou WiMax-2, foi desenvolvido como o próximo passo na evolução do padrão tecnológico WiMax [15].

O 802.16e já está em desenvolvimento há mais de quatro anos e surge em um momento em que maioria das operadoras já se comprometeu em desenvolver redes 4G LTE (*Long-Term Evolution*), padrão que possui algumas das características básicas da tecnologia WiMax, mas foi consolidada por um grupo de padronização diferente.

A Samsung é um dos grandes fabricantes a apostar no padrão WiMax-2. A empresa fez demonstrações durante a CEATAC, realizada em Tóquio, de uma versão provisória da norma 802.16m, usando velocidades de 330 Mbps. O padrão IEEE 802.16m utiliza várias técnicas, tais como a Mimo (*Multiple-In Multiple-Out*), capaz de gerir múltiplos fluxos de dados. E também pode ser usada com unidades de *femtocell* e redes capazes de se auto organizarem.

A norma 802.16m foi reconhecida como uma tecnologia 4G pela ITU (*International Telecommunication Union*), juntamente com a LTE-Advanced. No entanto, a ITU redefiniu a sua terminologia sobre as tecnologias de 4G, admitindo nesse conjunto algumas das normas criadas com as melhorias em 3G. O padrão WiMax é usado como serviços fixos e móveis de banda larga em muitas partes do mundo. A versão 802.16e WiMax móvel foi aprovada na década passada, bem antes do LTE. Mas é o LTE que está recebendo maior suporte por parte da indústria.

Mesmo a *Clearwire*, maior fornecedora de WiMax no mundo, tem feito testes com modelos de serviço com LTE. Além disso, os fabricantes mundiais de celulares apoiaram a aprovação da versão final do *LTE-Advanced* [15].

2.4 IEEE 802.20 *MOBILE BROADBAND WIRELESS ACCESS (MBWA)*

O Padrão IEEE 802.20, também conhecido como Mobile-Fi, busca assegurar a interoperabilidade dos sistemas BWA (*Broadband Wireless Access*) em um ambiente móvel operando em bandas abaixo de 3,5 G Hz licenciadas. O objetivo do padrão 802.20 é aperfeiçoar o transporte de dados, focando em altas taxas de transmissão, acima de 1 Mbps, e suportando mobilidade veicular de até 250 Kmh com um tempo de latência mínimo e adequado [16].

O Mobile-Fi teve seu desenvolvimento aprovado em 2002, foi especificamente projetado para transportar dados IP de uma forma completamente móvel. Seu principal objetivo é permitir o desenvolvimento de uma rede de acesso banda larga sem fio, para celulares que atendam as principais necessidades do mercado, como por exemplo: Operabilidade entre os diversos fabricantes de celulares.

O Mobile-Fi pode atingir até 4 Mbps. A palavra-chave, relacionada com tal tecnologia, é a mobilidade. Fornecê-la com qualidade envolve inúmeros desafios.

Um deles é a forma de efetuar *handoff*. O Mobile-Fi possui pequena latência, cerca de 20ms, mesmo em velocidades de até 250KMh, velocidade mais que suficiente para diversas aplicações [18].

É interessante ressaltar que o padrão IEEE802.20, assim como o WIMAX IEEE 802.16, é baseado na modulação OFDM (*Orthogonal Frequency Division Modulation*) que apresenta uma série de vantagens sobre a DSSS (*Direct-Sequence Spread Spectrum*) utilizada no Wi-Fi (IEEE 802.11b) [16].

3 **SEGURANÇA**

Uma vez que permitimos a comunicação de dispositivos móveis com a rede corporativa, devemos manter uma infraestrutura que permita a troca de dados e acesso às informações desejadas de forma segura.

Segurança Wi-Fi é uma questão importante para todos os usuários de redes sem fio. E é definido sob IEEE 802.11i onde sistemas WEP, WPA e WPA2 são amplamente mencionados.

Como o sinal sem fio pode ser pego por usuários não autorizados, é imperativo assegurar que mesmo que o sinal seja capturado, ele não poderá ser acessado.

3.1 SEGURANÇA EM REDES WI-FI 802.11x

O Ponto de Acesso - *AP Wi-Fi* anunciar sua presença, enviando periodicamente um sinal chamado *beacon* que contém o *SSID* da rede. Isso permite aos usuários identificar o AP e tentar se conectar a ele.

Uma vez detectado, é possível tentar se conectar ao AP, e então o processo de autenticação *Wi-Fi* começa. Para que um cliente possa se conectar ao AP, é necessário conhecer a chave de acesso, e a troca dessa chave deve ser feita de forma segura e para isso existem alguns padrões de segurança bem conhecidos.

3.1.1 ***WEP - Wired Equivalent Privacy***

O WEP foi a primeira forma de autenticação usada com Wi-Fi. Infelizmente, foi facilmente de quebrado, e outros padrões mais robustos surgiram. O objetivo do WEP era tornar as redes sem fio tão segura como as comunicações com fio.

Infelizmente, não foi possível, pois a chave logo foi quebrada, e agora existem muitas aplicações de código aberto que pode facilmente descobrir a chave WEP em questão de segundos.

Em termos de operação, a chave WEP usa uma mensagem de texto claro enviada pelo cliente, então esta é criptografada usando uma chave previamente compartilhada. O WEP usa diferentes tamanhos de chave, os comprimentos mais comuns são 128 ou 256 bits.

O sistema de segurança do WEP é falho. Principalmente porque não aborda a questão da gestão de chaves e esta é uma consideração primária para qualquer sistema de segurança. Normalmente as chaves estão distribuídas manualmente ou através de outra rota segura. O sistema WEP usa chaves compartilhadas, ou seja, o AP usa a mesma chave para todos os clientes e, portanto, isto significa que se a chave é comprometida, todos os usuários estão vulneráveis.

Obviamente o WEP é melhor do que usar nenhum sistema de segurança, pois, nem todas as pessoas que escutam um AP serão capazes de quebrar a chave.

3.1.2 ***WPA - Wi-Fi Protected Access***

O WPA é um melhoramento do software/firmware do WEP. A primeira versão deste é também conhecido como WPA1 ou WPAv1.

Foi concebido com a finalidade de proporcionar uma melhoria funcional para o sistema WEP, a metodologia de acesso WPA foi criada.

Um dos elementos chave do WPA é o uso do TKIP Temporal Key Integrity Protocol. O TKIP é parte do padrão IEEE 802.11i e opera através da realização de combinação de chaves.

Além disso, o WPA também fornece suporte para o algoritmo AES, isso proporciona uma melhora significativa no nível de segurança.

3.1.3 **WPA2 - *Wi-Fi Protected Access v2***

O WPA2 é a atualização para WPAv1 e proporciona melhora significativa no nível de segurança. O WPA2 pretende substituir o WPAv1. Ele implementa os elementos obrigatórios do IEEE 802.11i. Em particular, ele introduz ao *CCMP*, um novo modo de criptografia baseada em AES com uma forte segurança.

A certificação para WPA2 começou em setembro de 2004 e agora é obrigatória para todos os novos dispositivos que levam a marca Wi-Fi.

No próximo capítulo será descrito como essas novas tecnologias se integram ao ambiente de trabalho e proporcionam melhores condições de trabalho aos usuários.

3.2 SEGURANÇA PARA REDES CELULARES

Em pouco mais de uma década houve um crescimento extraordinário relacionado à telefonia móvel, a tecnologia saltou da primeira para a quarta geração. Cada vez mais os telefones são utilizados como computadores, e, portanto ficando cada vez mais suscetíveis a ataques.

Um dispositivo móvel desprotegido conectado em uma rede insegura pode resultar em uma invasão. Em outras palavras significa que um invasor pode ouvir suas chamadas, ler suas mensagens de texto, acompanhar sua atividade na internet e não obstante apontar sua localização geográfica.

Para que uma rede seja considerada segura, de acordo com a norma ISO IEC 17799 [25], ela deve garantir:

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

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

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

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

Os quatro conceitos acima são válidos para qualquer modelo de informações, dados e comunicações. Nesse contexto serão descritos abaixo os tipos de ataques mais comuns em redes celulares:

3.2.1 **Principais Ataques em Redes Celulares**

Acesso não autorizado (*Unauthorized Access*) - Se um método de autenticação não é propriamente aplicado ou é mal configurado, então um invasor pode ter acesso livre a rede e usar seus serviços mesmo não sendo autorizado para isso [31].

Obstrução do meio (*Channel Jamming*) - É uma técnica usada pelos invasores cujo objetivo é destruir ou degradar o sinal da interface aérea, e dessa forma desabilitar o acesso dos usuários legítimos dessa rede deixando-os expostos a “outras” redes [31].

Negação de serviço (*Denial of Service*) - É causada pelo envio excessivo de dados na rede, mais do que ela pode suportar, deixando os usuários sem os recursos de rede disponíveis [31].

Espionagem (*Eavesdropping*) - Se o tráfego na interface aérea não for fortemente criptografado, um invasor pode espiar ou interceptar dados importantes ou ligações telefônicas confidenciais [31].

Mensagens Falsificadas (*Message Forgery*) - Se o canal de comunicação não for suficientemente seguro, um invasor pode mudar o conteúdo das mensagens em ambas as direções sem ao menos que os reais receptores perceberem isso [31].

Ataque Invasor-no-meio (*Man In The Middle Attack*) - Um atacante pode estar entre um telefone celular e um ponto de acesso da rede para interceptar mensagens [31].

Sequestro de sessão (*Session Hijacking*) - Um usuário malicioso pode sequestrar uma sessão já estabelecida e atuar como um legítimo usuário de uma determinada estação base [31].

Devido à natureza do meio de uma rede móvel, que é o ar, não há como oferecer algum tipo de “Mecanismo 100% Seguro”. Porém existem alguns métodos para tentar minimizar ou até eliminar ataques às redes móveis, abaixo veremos alguns deles.

3.2.2 **Segurança para Primeira Geração de Redes Celulares**

Baseada no sistema AMPS (*Advanced Mobile Phone System*), foi a primeira geração de rede celular adotada em larga escala. Com tecnologia totalmente analógica, para transmissão apenas de voz.

A rede 1G não oferecia sistemas de criptografia e, portanto qualquer pessoa que capturasse os dados no ar poderia decodificar os dados. Nos anos 90 essa prática acabou se tornando cada vez mais comum. Um atacante com equipamentos especializados como um *RF Scanner UHF* que demodula sinais FM podia facilmente escutar ou reproduzir conversas particulares, quebrando o sigilo telefônico [26].

Além disso, era possível também capturar o ESN (*Electronic Serial Number*) e o MIN (*MobileIdentification Number*) que autenticavam o usuário ao sistema. O ESN era um número de 12 dígitos enviados pelo telefone celular para a rede Core da operadora para efeitos de tarifação e identificação de usuários. No entanto esses dados eram transmitidos em formato texto e caso alguém interceptasse o par ESN/MIN esses dados poderiam ser clonados para outro telefone gerando um enorme precedente de problemas e vulnerabilidades [26].

Essas vulnerabilidades tomaram uma proporção tão grande que algumas operadoras adotaram um sistema de *PIN Code* antes de se efetuar uma chamada, essa providencia apenas minimizou o problema. Então, a solução mais plausível seria migrar as redes analógicas para redes digitais. Diante disso, em 2002, a FCC (*Federal Communications Commission*) decidiu que não iria mais conceder portadoras de banda A e B para suportar o serviço AMPS. Nesse cenário as operadoras se viram forçadas a evoluir suas redes para D-AMPS (*Digital AMPS - mais conhecida como TDMA*) ou para tecnologias concorrentes e mais bem-sucedidas como o CDMA2000, GSM, entre outras. Assim se iniciou a segunda geração das redes móveis celulares [27].

3.2.3 **Segurança para Segunda Geração de Redes Celulares**

Foi neste momento que pela primeira vez dados eram transmitidos pelo ar de forma digital. Além disso, novos serviços começaram a surgir, como *SMS* (*Short Message Service*), transmissões de pacotes de dados, identificador de chamadas.

Como todo pacote era transmitido com criptografia digital, ganhou-se facilidade e flexibilidade de utilização de recursos para aperfeiçoar a segurança. Essa nova forma de transmissão, criptografada, dados foi revolucionária em termos de segurança, mas ainda não foi o suficiente para evitar outras formas de ataques.

Pela primeira vez as redes celulares tiveram um nível de segurança moderado. Se comparado com os métodos das redes da geração anterior, houve uma significativa melhora no processo de autenticação e confidencialidade dos usuários. Além do *SIM Card* agora também se utilizam os algoritmos A3/A8 junto ao *AuC*, e devido a isso a clonagem de telefones ficou reduzida a um valor quase inexpressivo. Outro avanço importante foi a adoção de algoritmos de criptografia A5.1, A5.2 e A5.3 garantindo maior segurança das informações no meio [28].

3.2.4 **Segurança para Terceira Geração de Redes Celulares**

Muitas das características das redes 3G foram herdadas da rede 2G, toda a parte de *Switching Core* e *Packet Core* da rede foram mantidos, no entanto, as redes 3G, se diferenciam totalmente, das redes 2G, na parte de acesso (*Radio Access*). Em termos de segurança o processo de é idêntico as redes GSM/GPRS/EDGE e isso facilita bastante para que se tenha uma migração suave ou interoperabilidade entre redes 2G e 3G [32].

No 3G também foi implementado um novo cartão SIM, denominado *uSIM* (*UMTS/UTRAN SIM*) e com ele as novas técnicas de autenticação e cifragem

puderam ser aplicadas. O método de autenticação e troca de chaves, *AKA* (*Authentication and Key Agreement*), utiliza o mecanismo de desafio/resposta (*Challenge/Response*) semelhante ao utilizado no *GSM*, porém com 5 elementos (*quintuplets*) ao invés de 3 (*triplets*). O algoritmo *AKA* fornece autenticação mútua para o usuário e a rede, além disso, o usuário e a rede combinam uma chave de cifragem (*Chiper Key – CK*) e uma chave para integridade (*Integraty key – IK*) [33].

Com o uso do uSIM novas técnicas de autenticação se tornaram possíveis. Além disso, o tamanho das chaves foi aumentado de 64 para 128bits, dificultando bastante ou até inviabilizando ataques por força bruta.

Foi criada também uma camada de segurança, o UEA, e nela os algoritmos de autenticação, cifragem e integridade são aplicados.

Para aumentar a confidencialidade, somente o algoritmo UEA1(AES) é utilizado, por ser o mais forte [33].

3.2.5 **Segurança para Quarta Geração de Redes Celulares**

A quarta geração dos sistemas de comunicação celular teve como princípio de desenvolvimento ser totalmente IP, isto é, todos os elementos, com exceção do terminal, devem se comunicar por interfaces puramente IP. Com isso, várias técnicas de autenticação, integridade e confidencialidade já existentes e utilizadas nas redes IP são empregadas no 4G, como por exemplo, o *IPSec,* o *CMP* (*Certificate Management Protocol*) e o *TLS* (*Transport Layer Security*) [34].

Uma rede 4G utiliza menos elementos físicos, equipamentos que a rede 3G porém cada um com mais funções. É previsto ainda a utilização de células para cobertura de pequenas áreas, tais como residências ou escritórios, denominadas *Femto Cells* (*HeNB – Home eNB*). No LTE a cifragem é aplicada para os dados de

usuário e de controle, e a proteção de integridade é aplicada somente para os dados de controle, através do protocolo PDCP (*Packet Data Convergence Protocol*) [34].

Com o PDCP ocorre o controle da quantidade de pacotes enviados e recebidos (*COUNT*) e o controle da sequência dos pacotes (*SN – sequence number*). Com esse procedimento os ataques do tipo replay attack, onde o invasor tenta reenviar um pacote capturado anteriormente, é bastante dificultado.

A integridade é garantida através do campo *MAC-I* (*Message Authentication Code for Integrity*) para cada pacote, calculado com base nas chaves AS (*Access Stratum*), na mensagem em si, no *RBI* (*Radio Bearer ID*), na direção (*Uplink ou Downlink*) e no valor do COUNT[35].

Os principais avanços das redes 4G são que todas as interfaces, exceto a de rádio, são IP e isto facilita e flexibiliza bastante a instalação e manutenção das redes. Os sistemas de autenticação e troca de chaves foram melhorados, se comparados com os sistemas aplicados às redes 2G e 3G, utilizando chaves *HMAC-SHA-256*. A criptografia utiliza vetores de autenticação incompatíveis com os utilizados em redes 3G e para se manter a compatibilidade dos usuários, o *USIM* deve verificar o bit de separação (*separation bit*). Os algoritmos utilizados são o *AES* e o *SNOW 3G*, que utilizam chaves de 128 bits, e com capacidade de processar chaves de 256 bits, num próximo release.

Nas interfaces *S1-U* e *S1-MME* podem, opcionalmente, ser aplicados mecanismos de segurança baseados em *IPSec* [35].

3.2.6 **Segurança para Redes WiMax**

O padrão IEEE 802.16, especifica uma interface sem fio para redes metropolitanas (*WMAN*). Foi atribuído a este padrão o nome WiMAX (*Worldwide*

Interoperability for Microwave), criado por um grupo de indústrias cujo objetivo é promover a compatibilidade e interoperabilidade entre equipamentos baseados no padrão IEEE 802.16. Este padrão é similar ao padrão Wi-Fi (IEEE 802.11), que já é bastante difundido, porém agrega novos recursos, visando um melhor desempenho de comunicação permitindo velocidades de até 1 Gbps [39].

Os grupos de trabalho destinados a especificação do padrão 802.16 desenvolveram vários mecanismos de segurança para proteção contra roubo de serviço e para proteger as informações do usuário [39].

Para a proteção da informação, o WiMAX utiliza o RSA (*Rivest Shamir Adleman*), o DES-CBC (*Data Encryption Standard- Cipher Block Chaining*) e AES-CCM (*Advanced Encryption Standard in Counter with CBC-MAC*) como algoritmos de criptografia [40].

Para cifragem, o HMAC (*Hashed Message Authentication Code*) e o CMAC (*Cipher-based Message Authentication Code*) são utilizados [40].

O padrão 802.16 ainda especifica que cada usuário da rede deve utilizar o certificado X.509 para identificá-lo. O uso de certificados X.509 torna difícil um atacante falsificar a identidade dos assinantes legítimos, oferecendo ampla proteção contra roubo de serviço. A emenda 802.16e adicionou suporte para o *Extensible Authentication Protocol* (EAP) para redes WiMAX [40].

4 **NOVAS TECNOLOGIAS E O AMBIENTE DE TRABALHO**

Os tradicionais ambientes de trabalho, geralmente não conduzem os usuários, automaticamente, a um bom nível de satisfação e à requerida lealdade esperada pelas empresas. Grandes corporações já perceberam esse comportamento e estão buscando formas de atrair e principalmente reter seus talentos.

As novas tecnologias, descritas anteriormente, são responsáveis por mudanças no ambiente de trabalho e no comportamento dos usuários. Cabe ressaltar, que ao se utilizarem dessas novas tecnologias, os usuários passam a se envolver ainda mais no trabalho.

Os padrões 802.11ac, 802.11ad e 802.11af, são especificações de redes Wi-Fi que trazem velocidades na casa dos Gigabits. Isso indica uma possível substituição natural para as redes cabeadas.

As redes sem fio Wi-Fi, já é realidade em muitas empresas e algumas vezes substitui totalmente a tradicional rede cabeada, garantindo assim flexibilidade na movimentação de pessoal, permitindo a conexão de dispositivos móveis à rede corporativa, possibilitando maior conforto aos usuários, bem próximo ao ambiente encontrado fora da empresa.

Ao chegar em casa, o usuário pode realizar suas funções profissionais, pela internet, devido as elevadas velocidades disponíveis de conexões banda larga, a experiência do usuário é como se estivesse em seu posto de trabalho dentro da empresa.

As redes celulares 3G/4G ou outros tipos de tecnologias de rede, cada vez mais aproxima os usuários ao ambiente corporativo. Hoje basta um SmartPhone e

uma conexão de dados para que o usuário consiga executar a maioria de suas atividades normais de trabalho.

Esses novos meios de comunicação modificam totalmente as noções de tempo e espaço, acrescentam velocidade nas trocas de informações, derrubando fronteiras, introduzindo grandes transformações. Agora, os usuários, não precisam mais estar no mesmo lugar ao mesmo tempo para desenvolver seus trabalhos, permitindo que as empresas operem em qualquer lugar e a qualquer hora.

Grandes empresas já permitem que os usuários usem o dispositivo que mais os agrada para executar suas atividades profissionais, esse comportamento é conhecido como Bring your own device (BYOD) em português “Traga seu próprio dispositivo”, melhorando a produtividade, a satisfação, o recrutamento de novos talentos e a retenção de funcionários [17].

No capítulo a seguir serão apresentados casos de sucesso utilizando novas tecnologias.

4.1 CASOS DE SUCESSO

A próxima seção apresenta casos de sucesso de empresas que apostaram nas novas tecnologias para alavancar seus negócios.

4.1.1 **Unimed Ganha Mobilidade com e-mail na Nuvem**

A Unimed Juiz de Fora oferece assistência médica de alta qualidade. Mais de 125 mil pessoas são atendidas pelo plano de saúde na unidade Juiz de Fora, o que representa cerca de 20% da população local.

Como toda grande corporação, o e-mail é uma ferramenta essencial no dia a dia dos colaboradores. No entanto, a solução utilizada não atendia as necessidades

do negócio. “Nosso correio eletrônico era baseado em Linux, mas era uma ferramenta que não tinha conceito de webmail e sem nenhum tipo de mobilidade”, lembra Sandro Domingos de Abreu, supervisor de TIC da Unimed.

Para resolver os problemas de mensageria, o departamento de TIC da Unimed Juiz de Fora optou por uma solução de mensageria na nuvem. Quase 400 contas foram migradas para a nuvem, facilitando o trabalho dos colaboradores em geral. Além de oferecer mobilidade e padronização nos serviços de webmails, a nova solução permite o agendamento de salas, eventos e ainda conta com uma agenda corporativa.

Os ganhos percebidos pela Unimed Juiz de Fora atingem todos os departamentos da empresa. Desde a área de suporte até o usuário final, os benefícios avaliados são muitos. “Eles ganharam mobilidade, flexibilidade de integração e um grande avanço tecnológico”. Agora, os colaboradores também podem acessar os e-mails por smartphones, de qualquer lugar e em qualquer momento. “Esse foi um dos pontos fortes da migração, porque na outra ferramenta isso não era possível”, comemora Sandro [11].

4.1.2 **Trabalhando na Nuvem**

Tradicionalmente, para trabalhar com um computador, e executar atividades rotineiras, é necessário instalar uma série de aplicativos e suas infinitas atualizações. Por isso, trabalhar “na nuvem“, cada vez mais é uma realidade.

Que tal escrever e editar textos, utilizar planilhas eletrônicas e produzir apresentações de trabalho diretamente na internet? Melhor: sem pagar nada por isso. A rivalidade entre Google e Microsoft novamente favorece o usuário. Os dois gigantes oferecem serviços desse tipo: você pode usar editores de texto, planilhas

eletrônicas, aplicativos para a produção de apresentações e até desenhos e salvar tudo o que criar na nuvem, ou seja, as informações ficam armazenadas nos servidores das empresas que oferecem os serviços. Em seguida, pode compartilhar seus documentos com outras pessoas [41].

Um programador chamado Mark O'Connor deu adeus ao seu fiel *MacBook Pro* e começou a trabalhar exclusivamente em um *iPad* + *Linode* 512 conectado à Nuvem. Num primeiro momento ele não acreditava que pudesse dar certo, mas um ano depois ele já nem se recordava de onde está seu velho *MacBook*.

As 10 horas de vida da bateria do *iPad*, a conexão 3G e a combinação de teclado *iPad* + *Wireless* me liberta muito, hoje eu posso trabalhar em quer que lugar que eu possa sentar, diz Mark [36], que relata ainda que pode mudar de dispositivo a qualquer hora que quiser, já que todos os seus dados estão na nuvem [36].

Mark O'Connor é o exemplo perfeito de que um profissional satisfeito, com seu local de trabalho e usando o dispositivo de sua preferência, produz mais e melhor.

5 **CONCLUSÕES**

A Mobilidade é um caminho natural e para algumas empresas já é realidade. Os dispositivos móveis, que antes eram de uso pessoal, estão cada vez mais presentes nas redes empresariais.

Com o avanço tecnológico, constantemente são desenvolvidos novos recursos que nos permitem inúmeras possibilidades, a mobilidade é uma delas. O acesso móvel surge como um grande desafio para as empresas e introduz novas formas de trabalho, e o mercado cada vez mais competitivo exige que todos estejam sempre disponíveis.

A tecnológica atual já permite que as informações sejam acessadas praticamente de qualquer lugar e a qualquer momento, com a popularização dos dispositivos móveis como smartphones e tablets o computador torna-se uma ferramenta sempre presente, permitindo que as pessoas estejam cada vez mais conectadas, com isso é importantíssimo a preocupação com a segurança dos dados trafegados.

O crescimento extraordinário nas áreas de comunicação celular e redes locais sem fio permitem que informações e recursos possam ser acessados e utilizados em qualquer lugar e em qualquer momento. Por isso, a preocupação com a segurança das informações torna-se cada vez mais importante. Para garantir a segurança vários protocolos foram desenvolvidos. Esses protocolos utilizam técnicas de criptografia para alcançarem seus objetivos, tais como, sigilo, autenticação, integridade dos dados e não-repúdio [22].

O mercado já oferece algumas soluções de infraestrutura para integrarem os dispositivos móveis com a rede corporativa de forma segura, cabe aos gestores e

profissionais de TIC uma profunda análise para compreender qual delas é a mais adequada ao seu negócio.

Os novos padrões de rede Wi-Fi 802.11ac, 802.11ad, 802.11af abrem ainda mais o horizonte das empresas, pois quebram paradigmas, como as velocidades de acesso, que antes eram vistas como intransponíveis, possibilitando inúmeras aplicações.

O estudo realizado identificou como as novas tecnologias contribuem com o crescimento e consequentemente com a produtividade das empresas.

As tecnologias de redes sem fio e redes celulares trazem flexibilidade e em conjunto com os dispositivos móveis proporcionam agilidade nos negócios da empresa e consequentemente suporte para as tomadas de decisão.

Existem desafios para atingir essa maturidade, mas os benefícios são muitos e justificam o investimento.

Para os próximos trabalhos, serão estudadas formas de prover a integração de novas tecnologias ao ambiente corporativo utilizando soluções de código aberto, isso pode possibilitar significativa redução de custo de implantação.

REFERÊNCIAS

[1] Symantec **Pesquisa da Symantec sobre a Situação da Mobilidade 2012.** Disponível em: http://www.symantec.com/pt/br/about/page.jsp?id=mobiletrends. Acesso em: 14 ago. 2013.

[2] Nielsen **Mobile Majority: U.S. Smartphone Ownership Tops 60%**. Disponível em: http://www.nielsen.com/us/en/newswire/2013/mobile-majority--u-s--smartphone-ownership-tops-60-.html. Acesso em: 14 ago. 2013.

[3] Nielsen **Smartphones: Still Room to Grow in Emerging Countries.** Disponível em: http://www.nielsen.com/us/en/newswire/2013/smartphones-still-room-to-grow-in-emerging-countries.html. Acesso em: 14 ago. 2013.

[4] Figueiredo, C.M.S e Nakamura, E.F **Computação Móvel: Novas Oportunidades e Novos Desafios.** T&C Amazônia, 2003.

[5] Alverga, P.R e Ramos, A.S **Evolução, aplicações, barreiras e tendências do M-Business**. XXIV Encontro Nac. de Eng. de Produção, 2004.

[6] Mateus, G.R e Loureiro, A.F **Introdução a Computação Móvel.** 2. ed., Minas Gerais, 1998.

[7] Lyytinen, K. e Youngjin, Yoo Issues **and Challenges in Ubiquitous Computing**. Communications of the ACM. Vol. 45 no. 12, 2012

[8] Cavallini, R **Mobilize**. São Paulo, SP – Ed. dos Autores, 2010.

[9] Rabello, R.R **Android: Um Novo paradigma de desenvolvimento móvel.** Revista WebMobile Magazine, 18. ed, 2009.

[10] Junior, C.F e Fernandes, A.M. **Análise das tendências tecnológicas para Computação Móvel aplicada à área da Saúde** Universidade do Vale do Itajaí,

[11] Microsoft **Unimed Juiz de Fora (MG) ganha mobilidade com implantação de e-mail na nuvem**. Disponível em: *www.microsoft.com/brasil/Casos/versao_doc.aspx?id=1112*. Acesso em: 24 ago. 2013.

[12] Computerworld **Vendas de smartphones vão ultrapassar as de PCs em 2011** Disponível em: http://computerworld.uol.com.br/telecom/2009/08/25/vendas-de-smartphones-vao-ultrapassar-as-de-pcs-em-2011/. Acesso em 26 ago. 2013.

[13] O Globo.com **Com venda recorde de iPhones, Apple bate expectativas** Disponível em: http://oglobo.globo.com/tecnologia/com-venda-recorde-de-iphones-apple-bate-expectativas-no-2-tri-91519. Acesso em 15 jul. 2013.

[14] Soares, L. F. G. Et al. **Redes de Computadores - Das LANs, MANs e WANs às redes ATM** - Ed. Campus, 1995.

[15] **WIMAX Forum** Disponível em: http://www.wimaxforum.org. Acesso em 18 nov. 2013.

[16] **IEEE802.ORG** Disponível em: http://www.ieee802.org. Acesso em 16 nov. 2013.

[17] Harrison, Jeffrey S. **Administração estratégica de recursos e relacionamentos** - Porto Alegre - Bookman, 2005.

[18] **Grupo de Teleinformática e Automação** Disponível em: http://www.gta.ufrj.br. Acesso em 16 nov. 2013.

[19] **Universidade Federal de Pernabuco** Disponível em: http://www.cin.ufpe.br/~if679/textos/ConvergenciaDigital.html Acesso em 03 fev. 2014.

[20] **COPPE – UFRJ, Grupo de Atuação em Redes sem Fio** Disponível em: http://www.garf.coppe.ufrj.br Acesso em 03 fev. 2014.

[21] **ITPortal** Disponível em: http://www.itportal.in/2011/10/handoverhandoff-scenarios-in-gsm-system.html Acesso em 03 fev. 2014.

[22] **GTA - UFRJ** Disponível em: http://www.gta.ufrj.br/ftp/gta/TechReports/SXR02.pdf Acesso em 03 fev. 2014.

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

[24] Rose, G. **A precis of the new attacks on GSM encryption 2003**. Disponível em: https://opensource.qualcomm.com/assets/pdf/GSM_Attacks.pdf Acesso em 02 fev. 2014.

[25] **NBR ISO IEC 17799-2005**. Disponível em: http://portal.cjf.jus.br/sigjus/arquivos-diversos/NBRISO-IEC-17799-2005.PDF/view Acesso em 02 fev. 2014.

[26] Tude, E. **AMPS/TDMA (IS-136). 2003**. Disponível em: http://www.teleco.com.br/tutoriais/tutorialtdma/Default.asp. Acesso em 02 fev. 2014.

[27] TELECO - **Tutoriais**. Disponível em: http://www.teleco.com.br/tutoriais.asp. Acesso em 04 fev. 2014.

[28] Gardezi, Ali I. **Security in Wireless Cellular Networls. 2006**. Disponível em: http://www.cse.wustl.edu/~jain/cse574-06/cellular_security.htm Acesso em 04 fev. 2014.

[29] UMTS Forum. **Hspa: high speed wireless broadband - from hsdpa to hsupa and beyond.** 2009 Disponível em: http://www.umts-forum.org/component/option,com_docman/task,doc_download/gid,1632/Itemid,12/

Acesso em: 01 jan. 2014.

[30] UMTS Forum**. Mobile Broadband Evolution: the roadmap from HSPA to LTE** 2009 Disponível em: http://www.umtsforum.org/component/option,com_docman/task,doc_download/gid,2089/Itemid,12/ Acesso em: 01 jan. 2014.

[31] Perez, D., Picó, J**. A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications**. 2011. Disponível em: http://taddong.org. Acesso em: 20 jan. 2014.

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

[33] Straccialano, André L. **Segurança em redes 3G – UMTS** 2008. Disponível em: www.wirelessbrasil.org/wirelessbr/artigos/seguranca-umts-geral.pdf Acesso em: 05 fev. 2014.

[34] Poole, I. **LTE Security Authentication.** 2011. Disponível em: http://www.radioelectronics.com/info/cellulartelecomms/lte-long-term-evolution/lte-security-authentication.php. Acesso em: 10 fev. 2014.

[35] Poole, I. **5G Mobile Cellular Tecnology**. 2012. Disponível em: http://www.radioelectronics.com/info/cellulartelecomms/5g-mobile-cellular/technology-basics.php Acesso em: 10 fev. 2014.

[36] **Trabalhando na Nuvem.** Disponível em: http://yieldthought.com/ Acesso em: 10 fev. 2014.

[37] **Handoff in Cellular Systems.** Disponível em: https://www.cs.tcd.ie/~htewari/papers/tripathi98.pdf Acesso em: 19 fev. 2014.

[38] **Overview of the GSM system and protocol architecture.** Disponível em: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=210402 Acesso em: 19 fev. 2014.

[39] Teixeira, Edson R. D. **WiMAX 2004**. Disponível em: http://www.teleco.com.br/tutoriais/tutorialwimax/default.asp Acesso em: 19 fev. 2014.

[40] Yang, E. **A Survey of WiMAX and Mobile Broadband Security 2009**. Disponível em: http://www.cse.wustl.edu/~jain/cse571-09/ftp/wimax1/index.html Acesso em: 19 fev. 2014.

[41] **Trabalhando na Nuvem**. Disponível em: http://veja.abril.com.br/quem/google-docs-vs-office-3.shtml Acesso em: 19 fev. 2014.