FUNDAÇÃO DE ENSINO “EURÍPIDES SOARES DA ROCHA”
CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA – UNIVEM
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

LEANDRO LAVAGNINI BARROZO

SEGURANÇA NAS REDES SEM FIO:

WIRELESS E WIMAX

MARÍLIA
2009

LEANDRO LAVAGNINI BARROZO

SEGURANÇA NAS REDES SEM FIO:

WIRELESS E WIMAX

Trabalho de Conclusão de Curso apresentado ao Curso de Ciência da Computação da Fundação de Ensino "Eurípides Soares da Rocha", mantenedora do Centro Universitário Eurípides de Marília – UNIVEM, como requisito para obtenção do grau de Bacharel em Ciência da Computação.

Orientador:
Prof. Ms. Ricardo Petruzza do Prado

MARÍLIA
2009

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

TRABALHO DE CONCLUSÃO DE CURSO – AVALIAÇÃO FINAL

Leandro Lavagnini Barrozo

SEGURANÇA NAS REDES SEM FIO: WIRELESS E WIMAX

Banca examinadora da monografia apresentada ao Curso de Bacharelado em Ciência da Computação do UNIVEM/F.E.E.S.R., para obtenção do Título de Bacharel em Ciência da Computação.

Nota: 7,0 (sete)

Orientador: Ricardo Petruzza do Prado

1°. Examinador: Ildeberto de Gênova Bugatti

2°. Examinador: Emerson Alberto Marconato

Marília, 04 de dezembro de 2009.

Dedico este trabalho aos meus pais, que sempre me deram ajuda para a conclusão do curso, a minha namorada, que sempre me apoiou e incentivou meus estudos, e todos aqueles que direta ou indiretamente me ajudaram neste percurso.

AGRADECIMENTOS

Agradeço a todos os colegas da turma de Ciência da Computação, que me ajudaram durante todo o curso, e me apoiaram em momentos difíceis.

Agradeço em particular:

À minha namorada por sempre ter ficado ao meu lado me incentivando nos estudos e me ajudando a seguir em frente.

Aos meus pais que deram grande força para a conclusão do curso e realização de mais esta etapa de minha vida.

Meus amigos Danilo dos Santos Alves Santana e Thiago Yoshiaki Miyabara Nascimento, que deram grande auxílio e foram muito importantes para a conclusão desta jornada.

Ao Prof. Ms. Ricardo Petruzza do Prado pelo grande auxilio na orientação, e ajuda para conclusão do trabalho.

BARROZO, Leandro Lavagnini. **Segurança nas redes sem fio: Wireless e Wimax.** 2009. 56 f. Trabalho de Curso (Bacharelado em Ciência da Computação) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2009.

RESUMO

Com o surgimento das redes wireless muitas empresas e seguimentos podem ser beneficiados com esta tecnologia pela facilidade de instalação, menor custo, mobilidade e disponibilidade em uma grande área de cobertura. Porém temos que ficar cientes dos riscos que estas redes apresentam, referente à segurança dos dados que trafegam por ela. O foco deste trabalho é pesquisar as tecnologias de redes atuais, como o Wireless para redes locais, e Wimax para redes metropolitanas, estudando quais as ferramentas disponíveis para prover a segurança nestas redes sem fio e propor soluções seguras em cenário publico, doméstico ou corporativo, utilizando ferramentas disponibilizadas pela tecnologia.

Palavras-chave: Wireless. Wimax. Segurança. Redes.

BARROZO, Leandro Lavagnini. **Segurança nas redes sem fio: Wireless e Wimax**. 2009. 56 f. Trabalho de Curso (Bacharelado em Ciência da Computação) – Centro Universitário Eurípides de Marília, Fundação de Ensino "Eurípides Soares da Rocha", Marília, 2009.

ABSTRACT

With the rising of wireless networking and segments, many companies could benefit from this technology due the easy installation, lower cost, mobility and availability in a wide range. But we have to be aware of the risks that these networks have, on the security of the data to be trafficked for it. The focus of this research is to analyze the current network technologies such as wireless local area networks, and WiMAX for metropolitan area networks, studying which tools available to provide security in these wireless networks and propose a solution for use with security, even in a public place, domestic or corporate, using available technology tools.

Keywords: Wireless. Wimax. Security. Network.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AES - Advanced Encryption Standard

AK - Authorization Key

AP – Access Point

CCMP – Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol

CRC - Cyclic Redundance Checks

DES – Data Encryption Standard

DSSS - Direct- Sequence Spread Spectrum

EAP - Extensible Autentication Protocol

FHSS - Frequency-Hopping Spread Spectrum

GHz – GigaHertz

IEEE - Institute of Electric and Electronic Engineers

IP – Internet Protocol

IV – Inicialization Vector

MAC - Media Access Control

Mbps – Megabits per second

OFDM - Orthogonal Frequency Division Modulation

PKM - Privacy key management

PSK - Pre-shared key

QoS – Quality of Service

RADIUS - Remote Authentication Dial In User Service

RC4 - Ron's Code 4

RSN - Robust Security Network

SSID - Service Set Identifier

TEK - Trafic Encription Key

TKIP - Temporal Key Integrity Protocol

WEP - Wired Equivalent Privacy

WLAN – Wireless Local Area Network

WMAN - Wireless Metropolitan Area Network

WPA - Wi-Fi Protected Access

WPAN - Wireless Personal Area Networks

VLAN - Virtual Local Area Network

VoIP – Voice Over IP

VPN – Virtual Private Network

XOR – Exclusive Or

SUMÁRIO

INTRODUÇÃO

As redes sem fio foram desenvolvidas para implementar um tipo de rede com solução de acesso remoto e mobilidade, possibilitando o uso da rede onde é difícil a implantação da tradicional infra-estrutura, oferecendo o uso de equipamentos portáteis com acesso em qualquer lugar dentro da área de cobertura, e permitindo uma série de novas possibilidades de troca de informações com facilidade de instalação e um custo relativamente baixo.

A tecnologia *Wimax* surgiu como uma forma de aumentar as possibilidades das redes sem fio, proporcionando grande largura de banda para troca de dados, vídeo e voz, com qualidade de serviço e maior segurança.

Porém temos que ficar cientes dos riscos que a tecnologia sem fio nos proporciona, em que o meio transmissor é o próprio ar, podendo ser interceptado por qualquer um que esteja ao alcance do sinal transmissor.

Até que ponto estas redes são seguras para a utilização no cenário público e corporativo, em que muitos dos dados que são transmitidos são sigilosos.

No trabalho realizado será apresentado as tecnologias de rede sem fio Wireless, para redes locais e Wimax, para redes metropolitanas, estudando suas características, vulnerabilidades, tipos de ataques sofridos e mecanismos de segurança que garantem o uso seguro destas redes em qualquer tipo de cenário. No final será apresentado uma proposta de implementação de uma rede sem fio segura.

CAPITULO 1 – REDES SEM FIO

A disseminação e desenvolvimento das tecnologias das redes sem fio propiciou não apenas a utilização em ambientes profissionais, mas em diversos tipos de cenários, inclusive domésticos ou redes públicas.

A grande popularidade deste tipo de rede se deve ao fato de não ser necessária a utilização de cabos, trazendo facilidade de instalação, mobilidade e com um custo relativamente baixo. Em vários cenários é vantajosa a utilização deste tipo de rede, como por exemplo, em locais em que é difícil a passagem de cabos, em espaços muito grandes, como por exemplo, em campus universitário, hospitais, em lugares onde há a necessidade de mobilidade, dentre várias outras utilizações. Estas redes estão evoluindo e novas tecnologias sendo desenvolvidas, possibilitando diversas aplicações nos mais diversos cenários.

1.1 Hierarquia da rede

Através do *Institute of Electric and Electronic Engineers* (Instituto de Engenheiros Eletricistas e Eletrônicos), ou IEEE, uma organização profissional sem fins lucrativos, fundada nos Estados Unidos, foi estabelecida a hierarquia das redes sem fio, classificando-as conforme seu tipo. A figura 1 ilustra esta hierarquia em suas camadas.

Podem ser definidos três principais padrões de redes sem fio, conforme ilustração da figura 1.

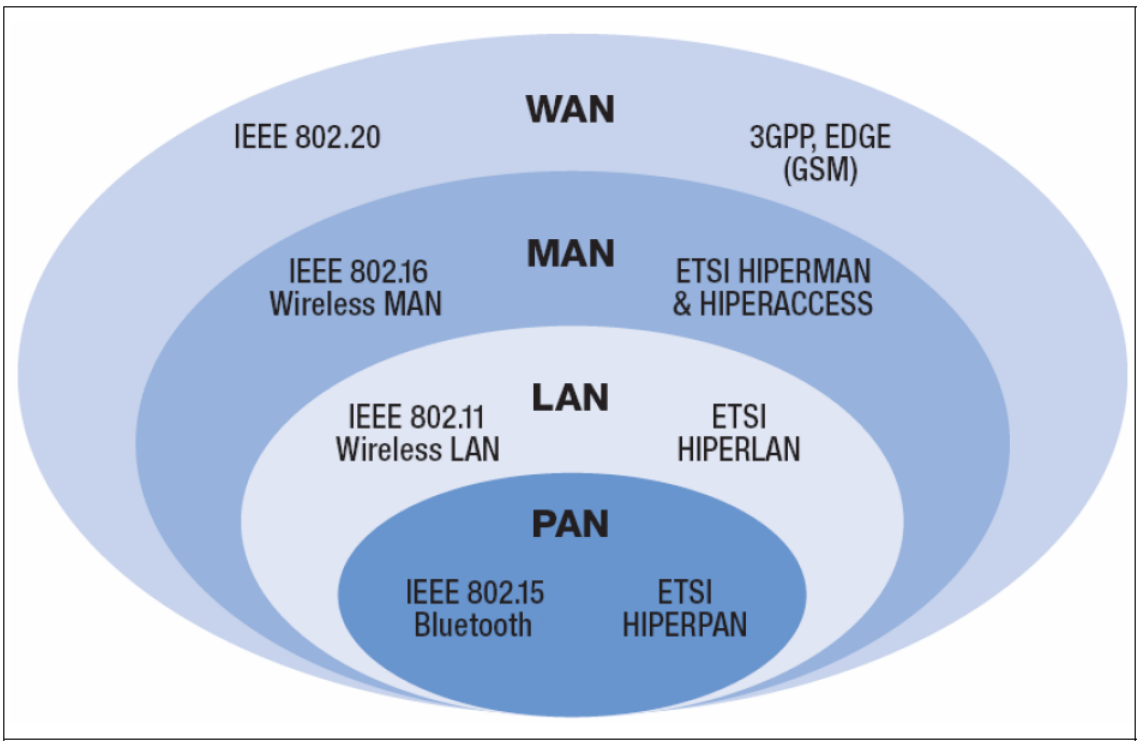
WPAN (*Wireless Personal Area Networks*) ou rede sem fios pessoal definido pelo padrão Bluetooth incorporado no padrão 802.15.

WLAN (*Wireless Local Area Networks*) ou rede sem fio local definido pelo padrão 802.11.

WMAN (*Wireless Metropolitan Area Network*) ou rede sem fio metropolitana definido pelo Padrão 802.16 (BARCELAR, s.d).

WAN (*Wide Area Network*) ou rede de longa distância, que abrange grande área geográfica, como países ou continentes. Definido pelo padrão 802.20.

Figura 1: Hierarquia das redes sem fio



Fonte: BARCELAR, s.d

1.2 Vantagens das redes sem fio

Flexibilidade: dentro da área de cobertura, uma determinada estação pode comunicar-se sem nenhuma restrição. Permite que a rede chegue em lugares onde os fios não poderiam chegar. Assim como facilidade de expansão e manutenção reduzida.

Facilidade: a instalação pode ser rápida, evitando passagem de cabos em dutos, canaletas, forros, etc. Tem o uso mais eficiente do espaço físico.

Diversas topologias: podem ser configuradas em uma variedade de topologias para atender a aplicações especificas.

Mobilidade: A rede pode ser utilizada em diversos locais dentro da área de cobertura com a utilização de dispositivos portáteis, não ficando preso a um determinado local.

1.3 Desvantagens das redes sem fio

Qualidade de serviço: mesmo com o avanço nesta tecnologia que vem sendo desenvolvida, a qualidade de serviço provida pelas redes sem fio, ainda é inferior quando comparadas com as redes cabeadas, tendo como principais razões a pequena banda passante devido a limitações dos equipamentos que fornecem sinal wireless, e falhas devido a interferências no meio.

Segurança: Os canais sem fio são mais suscetíveis a interceptores indesejados, pelo próprio fato de o meio transmissor de dados neste tipo de rede ser o próprio ar, podendo ser interceptado por qualquer um que esteja ao alcance do transmissor.

CAPITULO 2 – VISÃO GERAL DA TECNOLOGIA WIRELESS

Foi estabelecido ao *wireless* o padrão IEEE 802.11 que começou a ser desenvolvido em 1997, que se encontra na camada WLAN na hierarquia da rede, utilizado para fins de rede local, que pode incluir variações de técnicas de modulação. As mais populares técnicas são aquelas definidas pelos padrões 802.11a, 802.11b, 802.11g e 802.11n. São redes muito utilizadas atualmente, principalmente para conexão com dispositivos móveis (*Notebooks*, *Palms*, *Smartphones*, etc.), mas que estão sendo utilizadas também para *desktops*. Uma vantagem desta rede, é que trabalha em cima de faixas de freqüências não licenciadas, 2.4GHz e 5GHz, podendo ser utilizadas sem a necessidade de licenciamento das estações. A tabela 1 mostra algumas modulações do padrão IEEE 802.11.

Tabela 1: Padrões IEEE 802.11

Padrão IEEE	Freqüência	Alcance	Taxa
802.11a	5GHz	< 50m	6-54Mbps
802.11b	2.4GHz	<100m	2-11Mbps
802.11g	2.4GHz	<100m	20-54Mbps
802.11n	2.4GHz	<100m	300Mbps

2.1 Padrão IEEE 802.11b

A versão 802.11b do padrão original foi aprovado em meados de 1999 a 2001. O 802.11b trabalha em faixa de freqüências de 2.4 GHz com uma taxa de dados máxima de 11 Mbps (Megabits por segundo).

2.2 Padrão IEEE 802.11a

A versão 802.11a do padrão original foi aprovado em 1999. Trabalha em faixas de freqüência de 5 GHz, com taxa de dados máxima de 54 Mbps e trabalha com modulação OFDM (*Orthogonal Frequency Division Modulation*) que permite conexão sem visada direta (podendo possuir obstáculos entre o ponto de acesso e o cliente). 802.11a não é compatível com o 802.11b por não trabalharem com as mesmas faixas de freqüência, e velocidades

diferentes. O padrão 802.11a não é muito utilizado atualmente por não possuírem muitos equipamentos fabricados com suporte a ele.

2.3 Padrão IEEE 802.11g

Surgiu em meados de 2002 sendo a tecnologia que possui uma combinação ideal para utilização, trabalhando em faixas de freqüência de 2.4 GHz como o padrão 802.11b e com taxa de dados máxima de 54 Mbps, como o padrão 802.11a, e também possui modulação OFDM (*Orthogonal Frequency Division Modulation*) que permite conexão sem visada direta (podendo possuir obstáculos entre o ponto de acesso e o cliente. É a modulação mais utilizada atualmente, pois a maioria dos equipamentos fabricados tem suporte a este padrão.

2.4 Padrão IEEE 802.11n

O padrão mais atual, trabalha em faixas de freqüência de 2.4 GHz e 5 GHz e possibilita taxa de dados máxima de 300 Mbps. Atualmente já estão começando a serem fabricados equipamentos com suporte a este padrão.

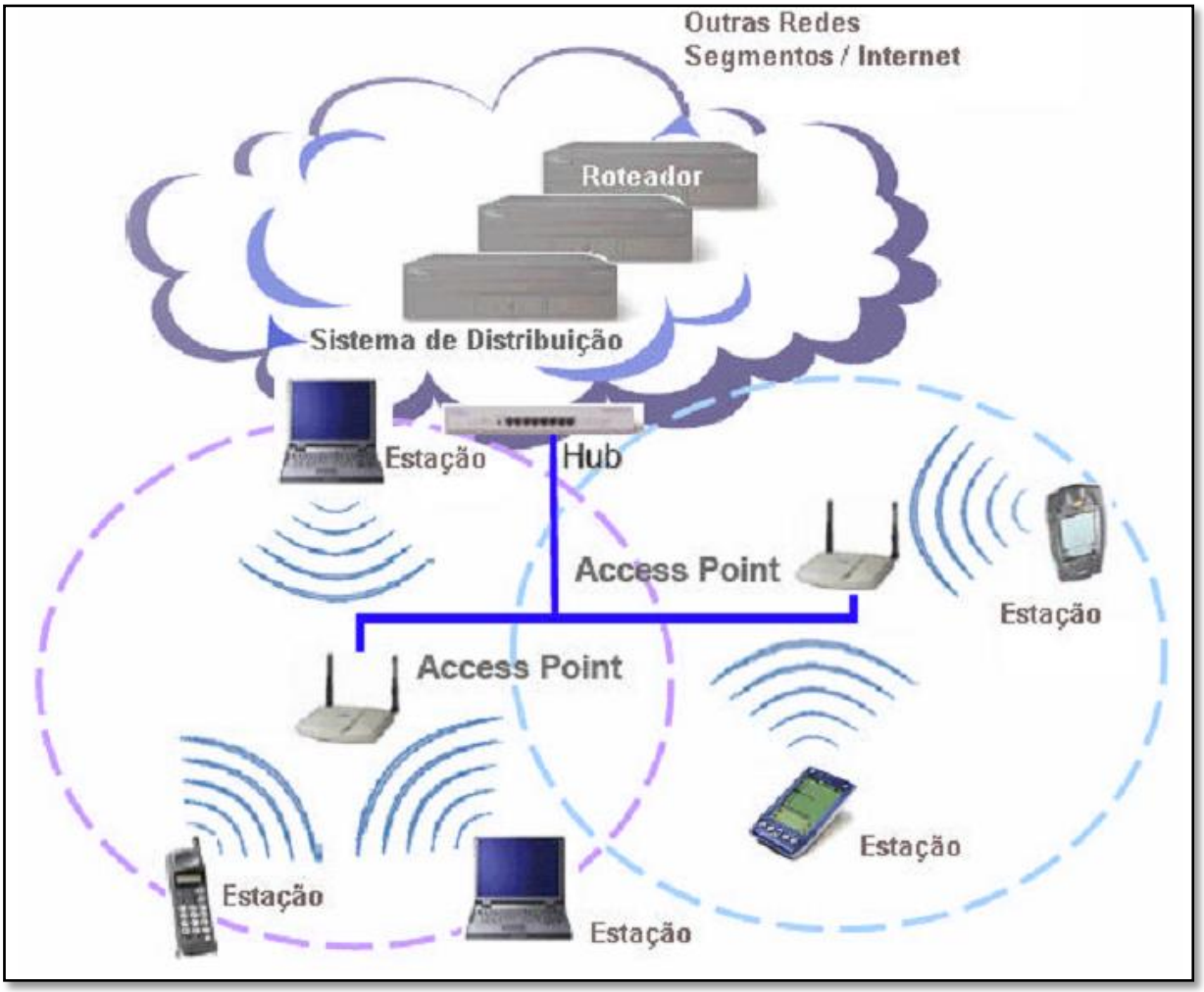
2.5 Implementação das redes Wireless

A implementação das redes *Wireless* é muito fácil de ser realizada, dependendo da rede poderá ser feita em algumas horas, visto que não há a necessidade de passagens de cabos.

Como virtualmente não há limites de pontos de acesso, esta rede pode ser expandida facilmente, instalando novos APs (*Access Points*), ou mesmo apenas adicionando novas estações clientes sem necessidade de alteração na parte física da rede. Por exemplo, se for necessário a adição de um novo computador na rede, não é necessário passagens de cabos, basta apenas conectar o computador a rede sem fio.

A figura 2 ilustra um exemplo de utilização da rede Wireless, mostrando os equipamentos que são utilizados neste tipo de rede.

Figura 2: Exemplo de utilização de uma rede Wireless



Fonte: AMARAL, s.d.

CAPITULO 3 – VISÃO GERAL DO WIMAX

O termo *Wimax* (*World Interoperability for Microwave Access*) deve-se ao *Wimax* Forum, que tem por objetivo garantir a interoperabilidade entre os equipamentos baseados no padrão IEEE 802.16.

O *Wimax* encontra-se na camada WMAN da hierarquia de rede sem fio, normalmente utilizadas para fins de redes metropolitanas, devido a seu grande alcance de sinal.

O *Wimax* ampliou as possibilidades das tecnologias de rede sem fio, proporcionando várias funcionalidades que o *Wireless* não possui.

Com as funcionalidades que esta tecnologia suporta, uma grande quantidade de serviços de banda larga é possível, como voz por IP (Voip) e vídeo sob demanda, além de grande área de cobertura com a possibilidade de mobilidade sem perda de conexão.

3.1 Benefícios oferecidos pela tecnologia Wimax

Largura de banda: Grande largura de banda, compreendida entre 75 e 134 Mbps (Megabits por segundo), podendo transmitir acesso simultâneo a centenas de clientes ou empresas.

Independência de protocolos: Com ele é possível a transmissão utilizando de diversos tipos de protocolos diferentes, como IP (*Internet Protocol),* ATM (*Asynchronous Transfer Mode*), Ethernet, dentre outros.

Serviços: É capaz de transmitir voz sobre IP (Voip), vídeos, dados, dentre outros.

Possui Qualidade de Serviço (QoS – *Quality of Service*), o que garante qualidade para transmissão de vídeos e voz, que são tipos de dados que não toleram *delay*, *jitter* e erros.

Delay é o atraso em que o pacote tem ao chegar ao seu destino. Este atraso pode ser causado pelo pacote ter pego uma rota maior, por ter encontrado congestionamento de dados pelo caminho, dentre outros fatores. A variação destes atrasos é conhecida como *Jitter*.

A entrega fora de ordem pode ocorrer por causa de pacotes que chegam ao seu destino em ordens diferentes, por terem tomado rotas distintas e com diferentes atrasos.

O *Wimax* utiliza modulação OFDM (*Orthogonal Frequence Division Modulation*), o que permite comunicação sem linha de visada direta (podendo possuir obstáculos entre o ponto de acesso e o cliente). Diferente do FHSS (*Frequency-Hopping Spread Spectrum* –

Espalhamento de Espectro por Salto de Freqüência) e do DSSS (*Direct- Sequence Spread Spectrum* – Espalhamento de Espectro por Seqüência Direta), o OFDM transmite centenas de portadoras, simultaneamente, em diferentes freqüências com espaçamento ortogonal, a fim de evitar interferências. Dessa forma, basta a recuperação de apenas uma portadora para recuperar a mensagem transmitida. Utilizando a modulação OFDM, foi possível resolver a problemática da interferência por sinais de rádios em obstáculos, através da grande quantidade de portadoras minimizando as atenuações em algumas faixas de freqüência. A performance sem linha de visada, ou seja, sem visão livre e direta entre o cliente e o ponto de acesso, é assegurada mais fortemente quando se está próximo da estação base, entre 5 e 8 quilômetros, porém com linha de visada pode-se atingir um alcance compreendido entre 50 e 70 quilômetros (BARCELAR, s.d).

A figura 2 ilustra um exemplo de utilização do *Wimax* numa rede metropolitana, onde existem pontos de acesso *Wimax* espalhados de forma estratégica garantindo uma cobertura sobre a cidade. Através desta rede é possível ter comunicação em vários pontos, possibilitando uma única rede que poderá ser utilizada por hospitais, centros policiais, bombeiros, setores públicos, e até mesmo de dentro de uma viatura utilizando dispositivos portáteis para tal comunicação, facilitando a troca de dados entre eles e gravando informações em um banco de dados centralizado.

Figura 3: Exemplo de utilização do *Wimax* numa rede metropolitana.

Fonte: http://images.google.com.br/images?hl=pt-BR&source=hp&q=wimax&btnG=Pesquisar+imagens&gbv=2&aq=f&oq=#gbv=2&hl=pt-BR&q=wimax&sa=N&start=72&ndsp=18, Acessado em 18/05/2009.

3.2 O padrão 802.16 do Wimax

Os primeiros desenvolvimentos do *Wimax* foram utilizados com o padrão IEEE 802.16 que trabalhava em freqüências entre 10 GHz a 66 GHz. Depois foi implementado o padrão IEEE 802.16a trabalhando em freqüências entre 2 GHz a 11 GHz, focando em conexão sem linha de visada. Atualmente está sendo utilizado o padrão IEEE 802.16e que é uma implementação do 802.16a, essa nova modulação, possibilita garantir conexões em movimento de até 60 Km/h dentro da área de cobertura sem perder a conexão.

Variações do padrão IEEE 802.16 foram implementadas conforme a tecnologia foi evoluindo. Na tabela 2 é apresentada a evolução do padrão IEEE 802.16 do *Wimax*.

Tabela 2: A família IEEE 802.16.

A Família IEEE 802.16	
802.16	Padrão para ***BWA*** operando em freqüências entre 10 e 66 GHz. Necessita de linha de visada.
802.16a	Atualiza o padrão 802.16 para operar em freqüências de 2 a 11 GHz; Alcance de 50 km; NÃO necessita de linha de visada.
802.16b	Aplicações permitindo uso de freqüências de 5 a 6 GHz não licenciadas.
802.16c	Interoperabilidade das freqüências até 66 GHz com linha de visada.
802.16d	Aprimoramento do 802.16, 802.16a e 802.16c, tornando-os obsoletos.
802.16e	Introduz suporte a mobilidade até 60 km.
802.16f	Evolução do 802.16 introduzindo o conceito de redes em malha (*mesh networks*).
802.16g	Outra evolução para suporte a mobilidade.

Fonte: DIAS, 2005.

3.3 Qualidade de Serviço (QoS)

Com o aumento da utilização de aplicações multimídias como áudio, vídeo, voz sobre IP, jogos nas redes, fez-se necessário um melhor tratamento destes dados, que não toleram *delay*, *jitter*, erros ou entrega fora de ordem.

O QoS é uma camada responsável pelo tratamento destes tipos de problemas que ocorrem nas transmissões de dados, trabalhando de forma que estes sejam minimizados e viabilizados o trafego de informações que não toleram estes problemas.

No padrão 802.16 do *Wimax* está previsto esta camada do QoS, o que torna possível transmissões de vídeos, voz, dentre outros dados de forma eficaz.

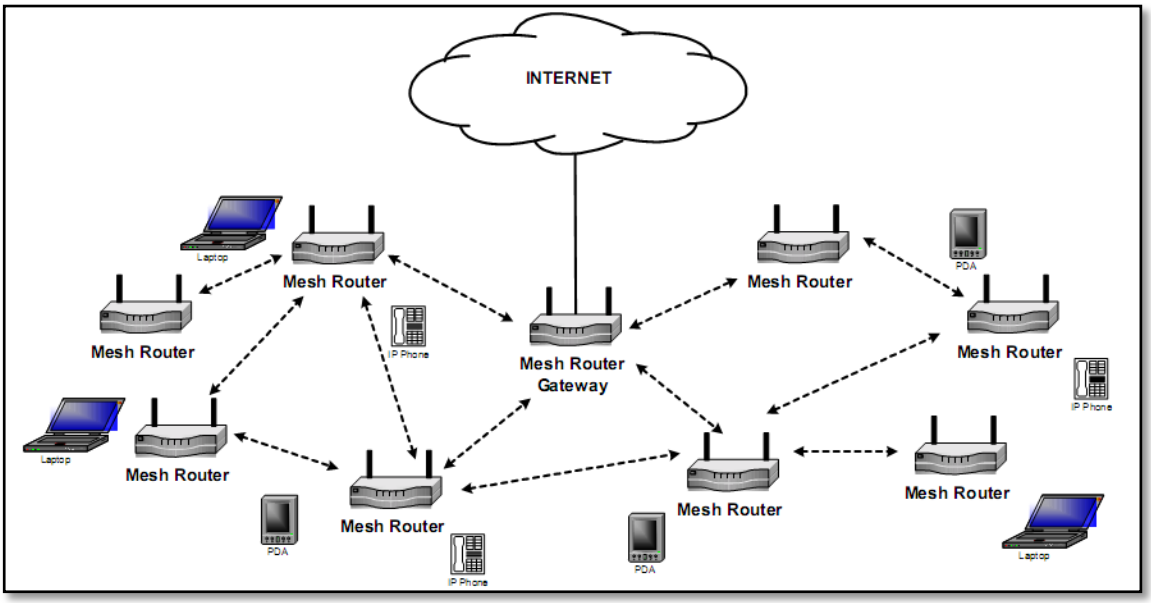
3.4 Redes Mesh

Existe um tipo de implementação do padrão *Wimax*, que é a utilização de Redes *Mesh* (Malha). Este tipo de rede possui topologia dinâmica, variável e de crescimento orgânico, com roteamento dinâmico (ABELÉM, s.d).

Esta rede é implementada com vários nós, um se comunicando com outros próximos, que se interligam e provém um acesso do tipo malha, formando uma grande cobertura.

A figura 3, ilustra um exemplo de Rede *Mesh*.

Figura 4: Figura 3 – Rede *Mesh*.



Fonte: ABELÉM, s.d.

Cada roteador é um nó da rede, que se comunica com outros roteadores e ao mesmo tempo geram sinal para acesso do usuário, que utilizará através de algum dispositivo móvel (*notebook*, celular, *smartphones*, etc.). Cada roteador calcula a melhor rota para seu destino. E se há falha em algum, a rede não fica comprometida, pois o próprio roteador já escolhe um caminho diferente até o destino.

Normalmente a comunicação entre os nós é realizada através de uma faixa de freqüência e a comunicação com as estações clientes, utiliza faixa de freqüência diferente.

CAPITULO 4 - SEGURANÇA

Atualmente, a segurança é fundamental em qualquer tipo de rede, mas principalmente em redes coorporativas ou públicas, em que dados sigilosos e dados de estratégias de negócios são trafegados. Sem segurança pode-se ter grandes prejuízos e perda de informações importantes e/ou fundamentais para o trabalho realizado.

A cada dia são desenvolvidas diversas aplicações para quebrar as seguranças dos sistemas, invadir e realizar ataques pelas vulnerabilidades da rede. A solução para conter estes ataques é inibir as vulnerabilidades destes sistemas e utilizar ferramentas que façam com que os dados não se tornem visíveis a todos, mas sim, apenas a quem interessa.

> A rede sem fio é um sonho que se tornou realidade para o espião: dados gratuitos sem qualquer trabalho. Por essa razão, não é preciso dizer que a segurança é ainda mais importante para sistemas sem fio que para sistemas fisicamente conectados (TANENBAUM, ANDREW S., 2003).

As redes sem fio possuem vulnerabilidades diferentes das redes cabeadas, justamente pelo fato do meio transmissor ser o próprio ar, podendo ser interceptado muito mais facilmente por qualquer um que esteja dentro da área de cobertura. Essa vulnerabilidade das redes sem fio ainda é uma questão pela qual há uma resistência para utilização deste tipo de rede em empresas ou seguimentos públicos, que necessitam de segurança. Por esse motivo são desenvolvidas ferramentas para tornar estas redes confiáveis para utilização em diversos tipos de aplicações.

> É surpreendentemente fácil projetar um sistema com total segurança em termos lógicos usando VPNs e *firewalls*, muito embora na prática ele vaze como uma peneira. Essa situação pode ocorrer se algumas das máquinas forem sem fio e usarem comunicação de rádio, que passa pelo *firewall* em ambos sentidos (TANENBAUM, ANDREW S., 2003).

4.1 Ataques nas redes sem fio

Com o crescimento das redes, e a grande utilização destas para transferência dos mais diversos tipos de dados, inclusive dados sigilosos, os ataques aumentaram e novas ferramentas para quebrar a segurança são desenvolvidas a cada dia.

Para falarmos dos ataques que existem nas redes primeiramente vamos entender um pouco por que motivo estes são realizados e de que forma podem acontecer.

Existem motivos dos mais diversos para os intrusos tentarem interceptar ou alterar dados de uma determinada rede. A tabela 3 mostra exemplos de intrusos e seus objetivos.

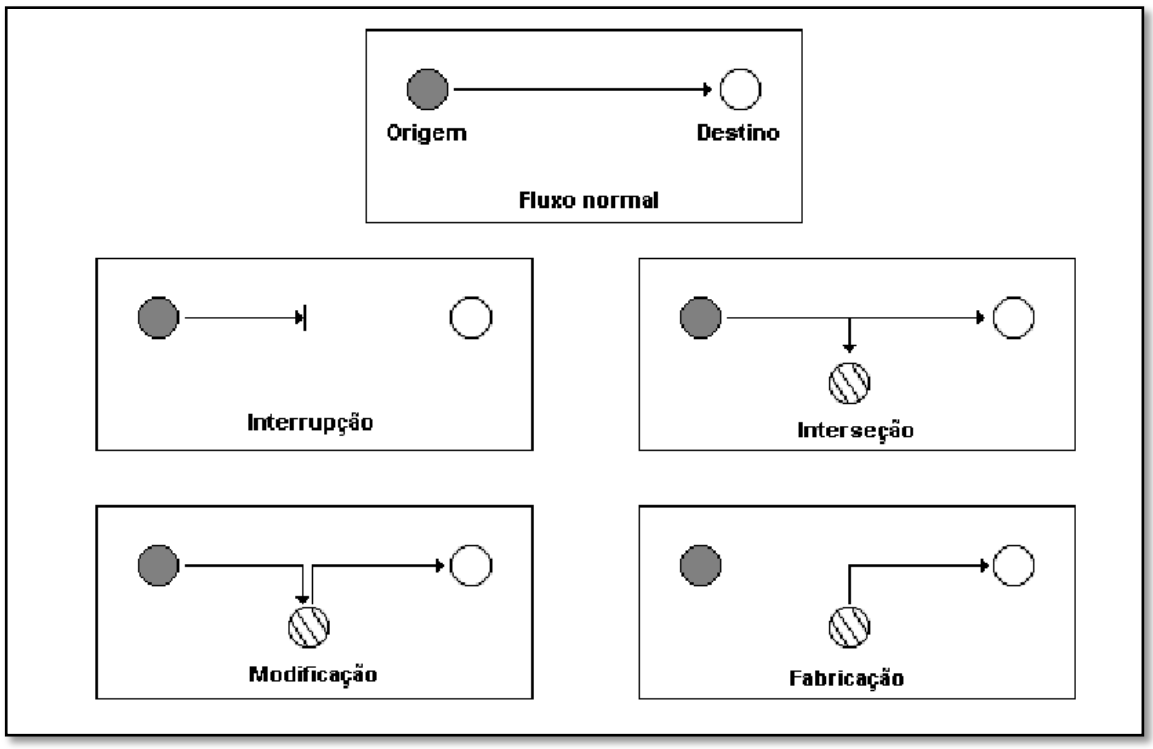
Tabela 3: Exemplos dos objetivos de alguns intrusos.

Intruso	**Objetivos**
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Hacker/Cracker	Testar o sistema de segurança de alguém; ou roubar dados
Representante de vendas	Tentar representar toda a Europa e não apenas a América
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se do ex-empregador
Contador	Desfalcar dinheiro de uma empresa
Corretor de valores	Causar prejuízo para lucrar no valor das ações
Vigarista	Roubar números de cartões de créditos e revendê-los
Espião	Descobrir a força militar do inimigo
Terrorista	Roubar segredos de guerra bacteriológica

Fonte: TANENBAUM, ANDREW S., 2003.

Os ataques também podem ser realizados de diversas formas e comportamentos. A figura 4 ilustra os tipos de comportamentos que o intruso pode ter num ataque em relação à origem e o destino num fluxo de envio de informações pela rede.

Figura 5: Comportamentos de ataque em relação à origem e o destino num fluxo de informações pela rede



Fonte: VERISSIMO, 2002.

Interrupção: O atacante tem como objetivo interromper o fluxo de dados trafegados na rede, impedindo que o destino receba os dados enviados pela origem.

Interseção: O atacante tem como objetivo apenas ter o conhecimento dos dados que trafegam pela rede.

Modificação: O atacante tem como objetivo interceptar os dados que estão sendo enviados pela origem, modificá-los e enviar os dados alterados ao destino.

Fabricação: O atacante tem como objetivo fabricar dados e enviá-los diretamente ao destino. O destino por sua vez, não sabe de qual origem são estes dados.

4.2 Engenharia Social

Existe um tipo de ataque realizado, que é chamado de engenharia social. Nestes ataques são utilizados meios de convencer pessoas a realizarem atitudes que elas não podem, ou não querem tomar, por exemplo, convencer uma pessoa a passar informações privilegiadas da rede. Este tipo de ataque é realizado, normalmente, em pessoas com baixo conhecimento das ameaças que uma rede pode estar sofrendo, e pessoas de "boa fé" que querem ajudar. Normalmente esta pessoa é um estagiário, uma secretária, empregados novos de uma empresa, que não tem muito conhecimento da rede (VERISSIMO, 2002).

Para darmos um exemplo deste tipo de ataque, vamos imaginar a situação em que uma pessoa mal-intencionada queira obter dados de determinada empresa, e convença uma pessoa que trabalha nesta empresa a desativar os *firewalls* dos computadores, e a passar dados privilegiados da rede. Com esses dados o atacante poderá se aproveitar dos recursos da rede.

É utilizada toda uma malicia por parte do atacante, para convencer pessoas a agirem a seu favor.

Este é um tipo de ataque muito perigoso em que não adianta possuirmos uma grande segurança em nossa rede, pois não são necessárias ferramentas de quebra de segurança, nem algoritmos complexos, apenas o que é utilizado é o proveito da falta de informação ou da "boa fé" de pessoas que tenham acesso dentro da rede.

4.3 Riscos da falta de segurança

Nos dias atuais como cada vez mais pessoas vêm utilizando redes de computadores, tanto em cenários corporativos como em cenários domésticos a segurança tornou-se primordial para que se possa utilizar com tranqüilidade e sem preocupações. Em qualquer cenário a segurança não pode ser deixada de lado, e os prejuízos podem ser enormes.

4.3.1 - Em redes Domésticas

Com a utilização da internet para realizar as mais diversas atividades que estão disponíveis atualmente, como compras *online*, movimentações bancarias, trocas de dados pessoais, dentre outras aplicações, as redes domesticas também se tornaram alvo dos hackers, e a cada dia são desenvolvidas ferramentas para quebrar a segurança, que normalmente

usuários convencionais não se preocupam ou, se possuem, é uma segurança muito baixa. Neste tipo de cenário a falta de segurança pode causar prejuízos como roubo de senhas bancárias, números de cartões de créditos, trabalhos importantes que podem não ter utilidade para outras pessoas, mas por diversão são apagados, roubo de arquivos pessoais, etc.

> *Grande parte do problema de segurança pode ter sua origem nos fabricantes de estações-base sem fio (pontos de acesso) que tentam tornar seus produtos amigáveis para o usuário. Em geral, se o usuário retirar o dispositivo da caixa e o conectar à tomada da rede elétrica, ele começará a operar de imediato – quase sempre sem qualquer segurança[...] (TANENBAUM, ANDREW S., 2003).*

4.3.2 Em redes Corporativas

Em redes coorporativas a falta de segurança pode trazer prejuízos maiores ainda, pelo fato de ser transportada pela rede uma variedade de informações. A maioria das empresas atualmente possui todo seu sistema automatizado, que cuidam desde a parte operacional, como financeira, administrativa, executiva, etc. Um intruso que consiga interceptar dados desta rede tem nas mãos informações privilegiadas e sigilosas, além de ter acesso às movimentações financeiras. Grandes prejuízos financeiros podem ser causados por um descuido. Muitas empresas ainda não se preocupam com esta segurança, diversas vezes por não terem noção do perigo que estão ficando expostos deixando toda a informação de seus negócios abertas a espiões ou hackers.

CAPITULO 5 – SEGURANÇA NAS REDES WIRELESS

As redes sem fio possuem seus problemas de vulnerabilidade e segurança quando utilizados através da configuração básica providas pelos equipamentos que implementam estas redes, mas utilizando ferramentas disponíveis pelo próprio padrão 802.11, conseguimos garantir maior segurança a rede e aos dados trafegados na mesma.

No decorrer dos anos diversas implementações foram criadas para suprir a deficiência de segurança que este tipo de rede possui.

O IEEE criou dois padrões para auxiliar na segurança das redes *wireless* 802.11, são eles o 802.1x e o 802.11i. O primeiro é o protocolo de controle de acesso (privacidade e autenticação), o segundo é um protocolo específico para funções de segurança, e opera junto com o padrão 802.1x.

Por causa das falhas nos sistemas de rede sem fio, um grupo elaborou o padrão 802.11i, na tentativa de estabelecer solução efetiva para os problemas das redes wireless. Este grupo criou o padrão RSN (Robust Security Network). Este padrão trabalha com algoritmo AES para criptografia dos dados transmitidos e o 802.1x para autenticação de usuário e gerenciamento de chaves.

O padrão IEEE 802.1x especifica um mecanismo para autenticação de dispositivos e/ou usuários através da utilização de variações do protocolo EAP (*Extensible Autentication Protocol*). O protocolo EAP, na sua definição, permite a utilização de uma grande variedade de mecanismos de autenticação. A forma de funcionamento deste protocolo é baseada na troca de mensagens do tipo texto-desafio (PERES e WEBER, 2002:06).

Seu funcionamento é simples, quando um cliente tenta acessar a rede, o cliente envia uma informação ao servidor de autenticação, que pode ser o próprio AP ou um servidor externo, este verifica se a informação é válida ou não. Caso as informações sejam corretas o cliente pode acessar a rede.

Para garantir a segurança nas redes *Wireless*, diversas ferramentas são desenvolvidas pelos próprios fabricantes dos equipamentos, e algumas já previstas no próprio padrão 802.11. Neste capitulo iremos estudar estas ferramentas.

5.1 Criptografia dos dados

Apenas o impedimento de determinado cliente acessar a rede não é o suficiente para garantir a segurança, devemos também proteger os dados trafegados nesta rede, de forma que indivíduos não interessados não enxerguem o que é transmitido. Para isso é utilizado a criptografia dos dados.

A palavra criptografia vem de palavras gregas que significam “escrita secreta”.

A criptografia é uma forma de proteger os dados que são trafegados na rede e somente quem tem a chave secreta pode ler os dados. Pode-se dizer que a criptografia é uma forma de um equipamento conversar com outro de uma maneira que os não interessados não entendam o que é dito. O transmissor pega o dado puro e criptografa utilizando uma chave de segurança, o dado será trafegado de modo cifrado e apenas o receptor que também possuir a mesma chave, poderá decifrar o código. Essa chave é construída com algum algoritmo que usa fórmulas matemáticas e operações lógicas para modificar o dado puro.

Segundo Guimarães a criptografia é importante para proteger o sistema quanto a ameaça de perda de confiabilidade e integridade e é utilizada para garantir sigilo, onde somente usuários autorizados tem acesso à informação, e integridade, garantindo que nenhum dado seja alterado durante o envio.

5.1.1 Algoritmos de Criptografia

Existem dois tipos de algoritmos de criptografia, são eles, criptografia de chave simétrica e chave assimétrica.

A criptografia de chave simétrica, também conhecido como de chave secreta, é um sistema antigo, por este motivo também é chamado de criptografia tradicional. É uma técnica que normalmente se utiliza uma única chave, tanto para cifragem como decifragem dos dados. No caso de possuir duas chaves, a segunda é deduzida em função da primeira. Desta forma na técnica de criptografia simétrica, mesmo que haja duas chaves, uma não é independente da outra, e em todo caso, a mesma chave deverá ser conhecida por todos os que quiserem realizar a decifragem dos dados (GUIMARÃES, 2001). Alguns dos algoritmos de criptografia simétricos mais conhecidos são: DES, AES, Triple-DES.

Um dos principais problemas em relação ao método de criptografia com chave simétrica é o fato de todos terem que conhecer a mesma chave para decifragem dos dados.

O DES (*Digital Encryption Standard*) é um algoritmo de criptografia de chave simétrica e única. É um algoritmo rápido para implementação em *Hardware* e lento para *Software*, e utilizam chaves de 56 bits.

O *Triple*-DES é a utilização de três vezes o DES com duas chaves diferentes sobre os mesmos dados, o que equivale a um algoritmo de 112 bits, aumentando a segurança em relação ao DES com chave de 56 bits.

O AES é um algoritmo de chave simétrica, que foi criado para substituir o DES, com chaves de 128 a 256 bits, é um dos algoritmos mais utilizados para criptografia de chave simétrica.

Na criptografia assimétrica, também chamada de criptografia de chave pública, não se utiliza uma única chave, mas um par delas. Uma é a chave pública, destinada a ser conhecida por todos, e a outra é a chave privada, mantida secreta pelo seu proprietário. Uma chave é independente da outra, de fato que o conhecimento de uma chave, não leve ao conhecimento da outra. Uma chave é utilizada para cifragem dos dados enquanto a outra para decifragem, quando uma criptografa, somente a outra poderá descriptografar (GUIMARÃES, 2001).

Um dos algoritmos de chave assimétrica, popularmente conhecido é o RSA.

RSA foi um algoritmo criado pelos fundadores da empresa RSA Data Security, Inc., que trabalha com chave assimétrica, possuindo uma chave pública e uma chave privada. É considerado um dos algoritmos mais seguros para criptografia.

5.2 WEP (Wired Equivalent Privacy)

O WEP é um protocolo de segurança que foi introduzido ao 802.11, com o intuito de garantir às redes sem fio uma maior segurança. Este protocolo provê métodos de autenticação para a rede. Ele utiliza CRC (*Cyclic Redundance Checks*), para garantir a integridade dos dados e algoritmo de criptografia RC4 (*Ron's Code* 4) para esconder os dados trafegados na rede. O WEP é provido pelo próprio AP (*Access point*) ou pelos próprios elementos, no caso de uma rede AD-HOC. O WEP possui dois métodos de autenticação, o Sistema Aberto (*Open System*) ou com Chave Compartilhada *(Shared Key*) (ALBUQUERQUE, 2008).

No Sistema Aberto qualquer cliente pode conectar-se a um AP apenas informando o SSID (*Service Set Identifier*) da rede. As informações passadas neste caso não serão

criptografadas e serão enviadas em forma de *Broadcast (*quando a mesma informação é transmitida para vários receptores ao mesmo tempo), para todos os clientes conectados ao AP.

No caso do Sistema com Chave Compartilhada, o cliente necessita possuir a mesma chave de segurança que o AP. Ao tentar conectar-se a rede, o cliente envia sua chave, o AP confere se sua chave está correta, se forem compatíveis o cliente ingressa na rede, caso contrário, o acesso é negado. A criptografia dos dados transmitidos é realizada através desta mesma chave compartilhada.

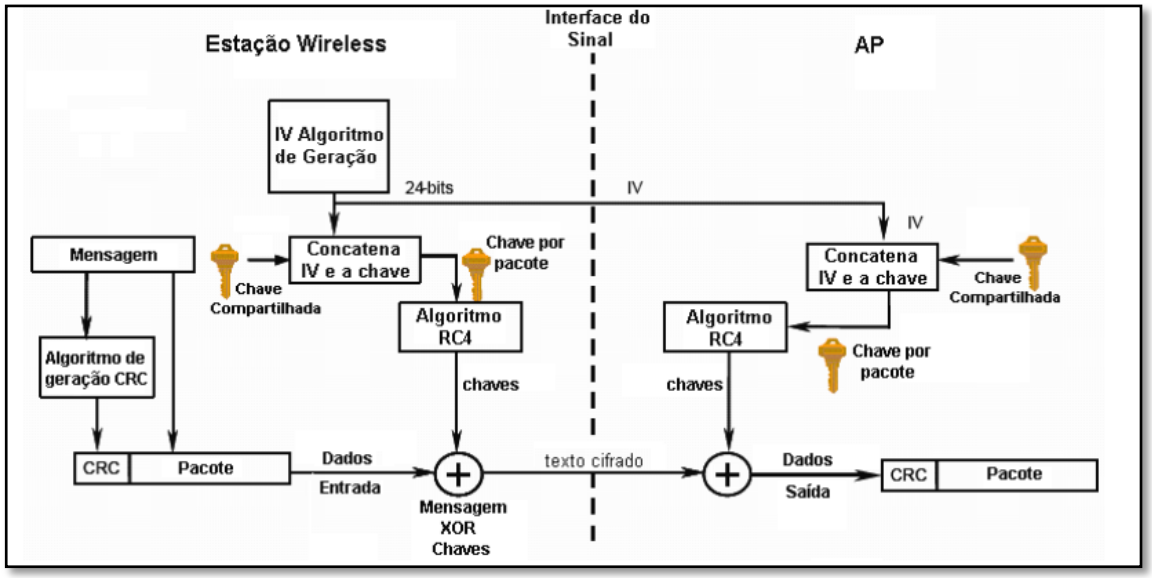
Este protocolo não é uma aplicação do IEEE 802.11, mas a maioria dos fabricantes já traz disponíveis em seus equipamentos *Wireless*.

Nos dois métodos de autenticação pode ser utilizado o controle de acesso por meio do endereço MAC (*Media Access Control*). Neste caso o AP possui uma lista com os endereços MAC dos clientes que podem conectar-se a rede, caso o MAC não esteja na lista, não consegue trafegar nesta rede.

O RC4 é, na verdade, uma maneira de se gerar bytes aleatórios, a partir de uma chave de tamanho variável. Estes bytes serão usados para encriptar uma mensagem através de combinações da operação lógica XOR. O destinatário executará o RC4 como o remetente, obtendo os mesmos bytes aleatórios, podendo assim desencriptar a mensagem (VERISSIMO, 2002).

A figura 5 mostra o funcionamento do WEP com o algoritmo de criptografia RC4.

Figura 6: Privacidade WEP utilizando algoritmo RC4



Fonte: AMARAL E MAESTRELLI, s.d.

Apesar de o WEP ser bastante utilizado para tornar a comunicação de uma rede sem fio mais segura, muitas falhas são apontadas. Uma das vulnerabilidades desse protocolo está associada à reutilização do vetor de inicialização (IV).

O IV possui 24 bits, podendo assumir valores entre 0 e 16M. Como são utilizadas as mesmas chaves por um longo período, o padrão WEP recomenda que o IV seja alterado para cada pacote enviado, evitando assim a reutilização do fluxo de chaves. Esse mecanismo tem dois problemas: o primeiro é que chegará um momento que o IV assumirá novamente o mesmo valor; e o segundo, é o fato de que as pessoas, freqüentemente, removem e reinserem os adaptadores de redes sem fio em seus computadores, fazendo com que o IV receba novamente o valor 0, tornando comuns os pacotes com IV com baixos valores.

Outra vulnerabilidade do WEP está relacionada ao CRC32. Como seu algoritmo de garantia de integridade é linear, possibilita que modificações sejam feitas no pacote sem que sejam detectadas. Apenas com o conhecimento da string de valores pseudo-aleatórios é possível alterar o conteúdo do pacote, comprometendo assim a integridade.

Uma das grandes fraquezas do WEP é a falta de gerenciamento de chaves, pois o padrão WEP não especifica como deve ser a distribuição das chaves, além desta ser concatenada ao dado enviado, o que torna fácil a descoberta. (VERISSIMO, 2002).

5.3 WPA (Wi-Fi Protected Access)

O protocolo WPA (*Wi-Fi Protected Access*) também conhecido como WEP2 ou TKIP (*Temporal Key Integrity Protocol* – protocolo de chave temporária) surgiu para corrigir os problemas de segurança encontrados no WEP, e implementou a autenticação e a cifragem do trabalho que estava sendo desenvolvido em outros padrões baseados no 802.11 (ALBUQUERQUE, 2008).

A tabela 4 mostra um quadro comparativo entre o WEP e o WPA.

Tabela 4: Quadro comparativo entre WEP e WPA.

Característica de segurança	WEP	WPA
Algoritmos de cifração	RC4	RC4
Gerenciamento de chaves	nenhum	Baseado em EAP
Tamanho de chaves	40 ou 104 bits	128 bits (64 bits para autenticação)
Chave do pacote	criada por concate-nação	criada por função de mistura
Integridade de da-dos/cabeçalho	CRC32/nenhum	MIC
Proteção contra re-produção	nenhuma	uso do VI

Fonte: WOLSKI, 2003.

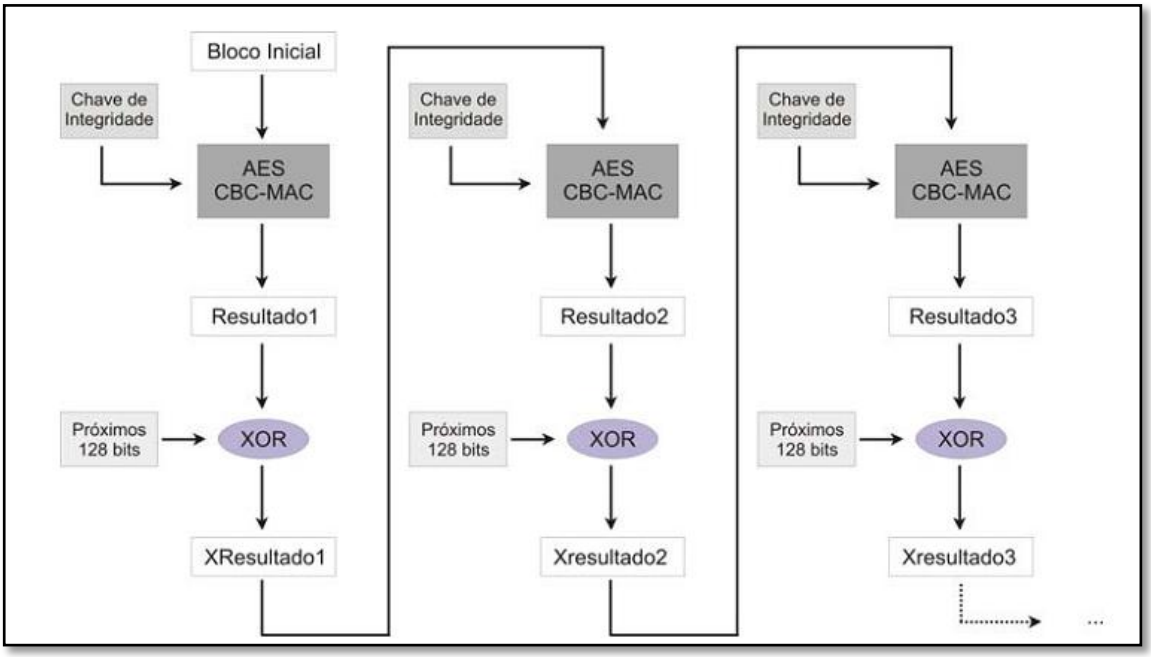
A primeira versão do WPA melhorou muito a segurança em redes *wireless*. O novo padrão possui o chamado PSK (*Pre-shared key*), no qual cada usuário tem uma senha frase. Assim como o WEP, o WPA também utiliza o algoritmo de criptografia RC4. O WPA combina dois componentes para prover forte segurança nas redes sem fio. O primeiro recurso é chamado de TKIP (*temporary key integrity protocol*), o qual embaralha uma mensagem sendo transmitida e envia de uma maneira rápida, não dando tempo para software de *sniffer* (interceptação de dados) interceptá-la. O segundo componente do padrão WPA é a segurança 802.1x, o qual verifica a autenticidade do usuário antes de ele entrar na rede. Antes qualquer usuário que tivesse acesso a senha poderia se logar na rede. Com o novo padrão é necessário ter autorização através do reconhecimento do hardware. Diferente do WEP, o segredo pré-compartilhado não é realmente a própria chave de criptografia. Em vez disso a chave é matematicamente derivada dessa senha. Naturalmente, se alguém obtém o segredo pré-compartilhado, ele ainda pode acessar a rede, mas os crackers não podem extrair a senha dos dados de rede, pelo fato desta estar misturada com os dados e não apenas concatenadas, como era o caso do WEP (MOREIRA E MALHEIROS, s.d.).

5.4 WPA2

Mesmo com a melhora significativa na segurança do protocolo WPA em relação ao WEP, ainda existe algumas falhas no algoritmo de criptografia. Para resolver estas falhas foi introduzido um novo protocolo intitulado de WPA 2. Os principais avanços do WPA 2 em relação ao WPA são, basicamente novos algoritmos de criptografia e de integridade, visto que o WPA é baseado no WPA2.

Neste caso o protocolo responsável pela integridade e confidência é o CCMP (*Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*) e é baseado no algoritmo de encriptação AES (*Advanced Encryption Standard*). A figura 6 mostra o funcionamento do AES no WPA2.

Figura 7: Integridade no WPA2



Fonte: LINHARES E GOLÇALVES, s.d.

O bloco inicial são os dados que serão criptografados. É realizada através do algoritmo AES a criptografia do dado e aplicada a operação lógica XOR entre o dado criptografado com o próximo bloco, que passa pelo mesmo processo sucessivamente.

Através deste sistema o WPA2 se tornou um protocolo extremamente seguro em que atualmente são conhecidas poucas vulnerabilidades.

5.5 Servidores de autenticação RADIUS

O RADIUS (*Remote Authentication Dial In User Service*), é um protocolo utilizado para disponibilizar acesso a redes com Autenticação, Autorização e Contabilização (*Authentication, Autorization e Accounting* – AAA). Foi inicialmente desenvolvido para utilização nos serviços de acesso discado, mas pela sua simplicidade e eficiência, hoje é utilizado por servidores de VPN, APs e outros tipos de acesso a redes (SILVA e DUARTE, s.d).

Uma forma de aumentar a segurança na rede é utilizar um servidor de autenticação externo RADIUS, em conjunto com o protocolo WPA ou WPA2. Este servidor RADIUS irá realizar a autenticação dos usuários que irão utilizar a rede. Esta autenticação pode ser realizada por um endereço físico do equipamento (MAC), ou por alguma senha.

Uma das formas de prevenir uma entrada indevida, ou uma invasão em uma rede sem fio, é cadastrando o endereço MAC de cada dispositivo da rede no controlador da rede, que pode ser um roteador, um ponto de acesso, entre outros. Esse controlador da rede, só permitirá a entrada dos cadastrados em sua base de dados, ignorando outros que porventura possa tentar entrar em sua área de atuação (RUFINO, 2005).

Quando uma estação tenta se conectar a uma WLAN com 802.1x, o AP autoriza a estação a se conectar, porém força a estação a um estado não autorizado no qual somente o trafego do EAP (Extensible Autentication Protocol) é passado pelo servidor RADIUS. Utilizando mensagens EAP ou mesmo senhas ou chaves publicas/privadas de criptografia, o servidor RADIUS autentica a estação. O servidor RADIUS então envia ao AP uma chave inicial de criptografia, que veio da estação através do processo de autenticação. O AP gera então uma segunda chave para o uso na comunicação com a estação, faz a criptografia da segunda chave com a chave inicial advinda do servidor RADIUS e envia de volta a estação. Em seguida, o AP envia novas chaves à estação com intervalos de tempo pré-definidos para assegurar que a chave não foi quebrada (AMARAL e MAESTRELLI, s.d.).

Este processo garantirá uma maior segurança, controlando o acesso de quem irá ingressar na rede.

5.6 Firewall

O *Firewall*, como o próprio nome sugere (Parede de Fogo), é uma barreira virtual entro dois pontos, ou duas redes, onde permitirá a passagem apenas de trafego autorizado, além da função de filtrar todo trafego da rede que passa por ele, e dizendo o que é permitido e o que é rejeitado (SIEWERT, s.d).

O *Firewall* fica no meio de uma via de trafego de dados, e todos os pacotes da rede, em ambos os sentidos, passam por ele, onde serão checados e autorizados a passar ou não. É uma forma de garantirmos segurança na rede, impedindo que pessoas não autorizadas acessem dados restritos.

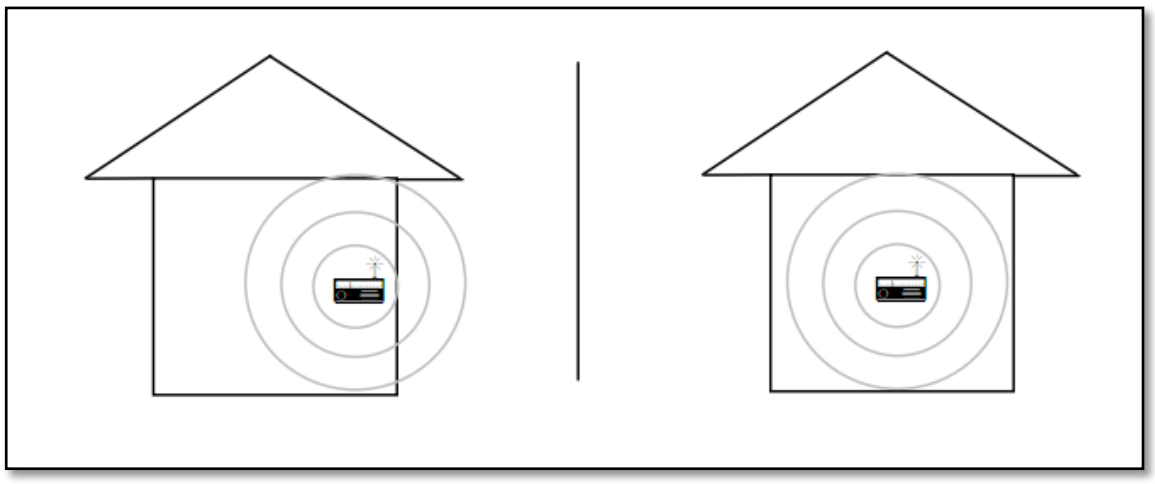
5.7 – Segurança Física

A segurança física de uma rede sem fio, muitas vezes não é lembrada e nem levada em consideração em muitos casos de implementação. Em uma rede cabeada, é um ponto importante que faz necessário a preocupação, e na rede sem fio não é diferente, pois a área de abrangência "física" aumenta substancialmente (RUFINO, 2005).

Os pontos de acesso que serão instalados para implementação da rede *wireless*, seja ele em cenário doméstico ou corporativo, deve ser estudado de forma minuciosa para que o sinal fique apenas ao alcance das delimitações do estabelecimento. Por exemplo, se instalarmos um ponto de acesso em um lugar bem alto terá um bom desempenho, porém seu alcance será maior, abrindo mais possibilidades de seu sinal ser interceptado.

Uma forma de resolvermos este problema é diminuindo a potência do sinal, e/ou posicionando os pontos de acesso em lugares onde o sinal será mais bem aproveitado dentro de determinada área, de tal forma que este fique a um alcance seguro dentro do estabelecimento onde é utilizada a rede *wireless*. A figura 7 ilustra um exemplo de posicionamento do ponto de acesso. A figura da esquerda mostra o ponto de acesso localizado próximo a parede, possibilitando que o sinal ultrapasse-a e aumentando as chances de ser interceptado. Na figura da direita, o ponto de acesso foi posicionado de tal maneira que o sinal não ultrapasse os limites físicos do estabelecimento (ALBUQUERQUE, 2008).

Figura 8: A posição física do ponto de acesso, grande importância na segurança da rede sem fio



Fonte: ALBUQUERQUE, 2008.

5.8 SSID

O SSID (*Service Set IDentifier* – Identificador do Domínio de Serviço), é o identificador da rede *wireless*. É através dele que dizemos em qual rede iremos conectar. Uma forma de aumentar a segurança e dificultar o acesso de intrusos é utilizando um recurso, geralmente disponível nos equipamentos de rede *wireless*, que é esconder este SSID, desta forma ele ficará oculto a scanners. Uma boa dica também é alterar este SSID periodicamente.

CAPITULO 6 – SEGURANÇA NAS REDES WIMAX

A tecnologia *Wimax* foi desenvolvida para utilização em redes de grande alcance, as WMANs (*Wireless Metropolitan Area Network*), conseguindo chegar a distâncias de até 50 km dependendo do tipo de utilização. Por este motivo houve grande preocupação com a segurança destas redes e foram desenvolvidas diversas ferramentas para garantir a proteção dos dados que serão trafegados por ela.

Características de privacidade e segurança estão previstas no padrão 802.16, tais características fazem parte de uma subcamada no padrão *Wimax* responsável por prover a segurança na troca de dados entre as estações base e cliente. Ela faz isso autenticando a estação cliente e criptografando os dados entre estas e a estação base. Esta subcamada de segurança possui recursos para evitar a interceptação dos dados e roubos de informações, evitando o acesso aos dados transmitidos por pessoas não autorizadas e forçando a criptografia dos recursos que trafegam na rede, podendo utilizar algoritmos como o *Triple*-DES (128 bits), o RSA (1024 bits), dentre outros. A autenticação é realizada através de utilização de certificados digitais do tipo X.509 e com o protocolo PKM *(privacy key management*) para troca de chaves entre as estações. (QUEIROZ, 2005).

6.1 O sistema de autenticação do Wimax

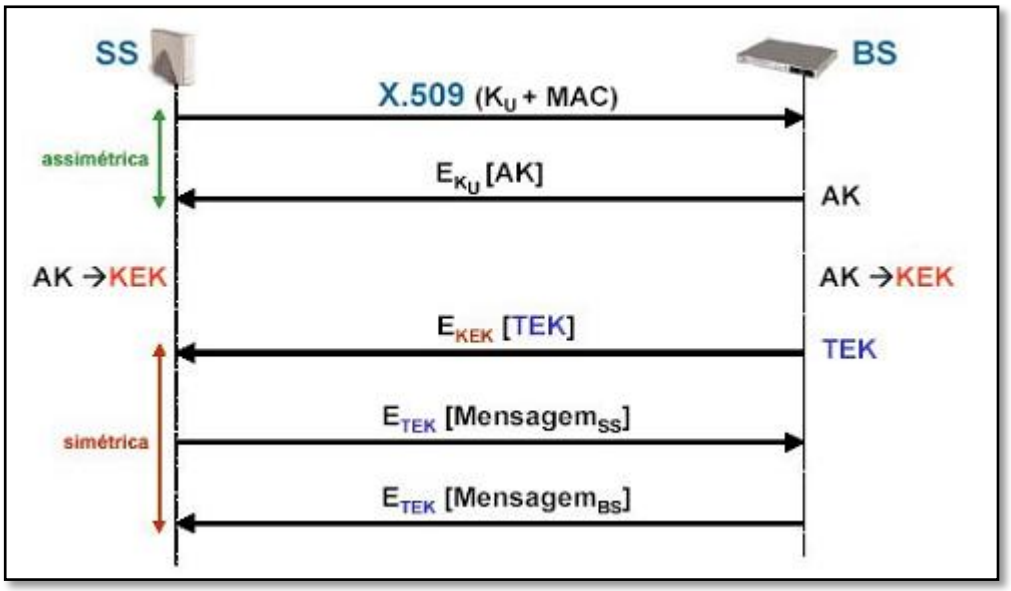
Conforme Barcelar (2006), o padrão 802.16 utiliza um sistema de criptografia hibrido, fazendo uso de criptografia assimétrica para autenticação e transporte de chaves e criptografia simétrica para cifragem e decifragem de dados. O certificado digital X.509 encontra-se na estação cliente e tem sua identidade autenticada na estação base. Neste certificado estão contidos o Endereço físico MAC e a chave publica (Ku).

Utilizando este modelo de autenticação, quando a estação solicita uma chave compartilhada (AK – *Authorization Key*) à estação base, ela fornece o certificado. A estação base verifica este certificado, e cria um segredo através da criptografia utilizando a chave publica que é enviada de volta a estação cliente. Como só aquela estação possui a chave privada, apenas ela poderá decodificar a mensagem e acessar o segredo. Toda estação cliente deve possuir duas chaves, privada e publica, através da própria construção de fábrica ou com algum algoritmo que as gera dinamicamente (QUEIROZ, 2005).

Através deste procedimento de autenticação a estação cliente poderá trocar informações criptografadas de forma segura.

Na figura X é ilustrado o funcionamento deste processo de autenticação entre a estação base e cliente.

Figura 9: Sistema de autenticação do padrão 802.16



Fonte: BARCELAR, 2006.

Basicamente o funcionamento deste processo é, quando a estação cliente vai realizar a autenticação, ela envia um certificado à estação base, onde esta analisa este certificado, validando-o, e pega a chave privada contida neste e gera uma chave compartilhada, que será utilizada para a codificação dos dados que serão trafegados. Como somente aquela estação cliente possui a chave privada, somente ela conseguirá decifrar a mensagem e ter acesso ao segredo. Esta é uma forma de autenticação de segurança muito eficiente, que garante a troca de informação entre estações clientes e base de forma muito segura e confiável.

A realização deste trabalho de autenticação, é feita pelo Protocolo de Gerenciamento de Chaves (PKM), responsável pela troca segura das chaves entre as estações contendo informações para autorização e cifragem dos dados.

6.2 Métodos de Criptografia

Nesta sessão vamos abordar os algoritmos de criptografia utilizados pelo protocolo PKM e para criptografia dos dados.

Há alguns algoritmos de criptografia que normalmente são utilizados para este tipo de aplicação no *Wimax*, são eles, o DES (*Data Encryption Standard*) e AES (*Advanced Encryption Standard*) para criptografia dos dados. E para a criptografia do TEK (*Traffic Encription Key* – Chave de criptografia de tráfego) pode ser feita pelo *Triple*-DES, RSA ou AES com chave de 128 bits.

6.3 VLANs nas redes Wimax

Como a rede *Wimax* será utilizada como rede metropolitana e diversos clientes de diferentes seguimentos estarão utilizando a mesma rede, uma forma de garantir maior segurança é através da utilização de VLANs (*Virtual Local Area Network*), onde cada usuário ficará em uma rede virtual específica para o seguimento que irá utilizar. Por exemplo, numa estrutura de uma cidade, toda sobre cobertura de uma rede *Wimax*, os clientes que enviarão dados para área da saúde, ficarão em uma VLAN especifica para esta área, e apenas enxergarão os dados que serão trafegados para a saúde. Do mesmo modo que um cliente que enviará dados para a área da educação, apenas terá acesso aos dados desta área e não conseguirá enxergar os dados da área da saúde. Esta é uma forma de garantirmos uma maior segurança, isolando os dados de determinado seguimento para que estes não fiquem trafegando pela mesma rede que os demais.

Uma VLAN é uma forma de criarmos, dentro de uma rede física, várias redes virtuais, de maneira que cada uma destas fique isolada umas das outras, como se fossem redes físicas separadas. A configuração destas VLANs normalmente é realizada nos switches que implementam a rede.

CAPITULO 7 – PROPOSTA PARA IMPLEMENTAÇÃO DE UMA REDE SEM FIO SEGURA

Através do estudo realizado no decorrer do trabalho sobre as tecnologias de redes sem fio, *Wireless* e *Wimax*, entendendo suas vulnerabilidades, formas de ataque e as ferramentas disponíveis para garantirem segurança na utilização destas redes, é realizada uma proposta de como implementar uma rede sem fio segura, que possa ser utilizada nos mais diversos cenários como, doméstico, público e até no cenário corporativo em que a segurança é fundamental.

7.1 Redes Locais Domésticas

Como foi descrito no capítulo 4, a segurança nas redes domesticas se tornam importante pela quantidade de serviços que podem ser utilizados pela internet e por pessoas mal intencionadas que desejam utilizar a falta de segurança na rede para realizar diversos tipos de ataques.

Na implementação das redes domésticas serão utilizadas apenas as ferramentas de segurança disponíveis nos equipamentos que fornecem o sinal *Wireless*, pois pelo perfil de usuários desta rede, não serão utilizados servidores, equipamentos auxiliares ou implementações mais complexas.

O primeiro passo na implementação da rede sem fio doméstica é, analisar o espaço físico. Levantar em quais cômodos será necessário a utilização da conexão e posicionar o AP em um local onde o sinal será bem distribuído nos pontos de interesse e que não exceda os limites físicos da residência, se estiver disponível no equipamento utilizado, ajustar a potência do sinal para conseguir tal feito. Com esse levantamento bem feito, já será obtida grande segurança, pois o sinal se restringirá apenas ao espaço físico que deverá ser utilizado, impedindo que pessoas de fora interceptem o sinal.

Os equipamentos que são utilizados para a implementação da rede *Wireless*, geralmente vem configurado por padrão com nenhum tipo de segurança ativado, para serem mais fáceis de utilizar e isso é um grande risco.

É fundamental a utilização dos protocolos de autenticação da rede (WPA ou WPA2). Como foi apresentado no capítulo 5, o WEP com chave compartilhada trará segurança se comparado ao sistema aberto, porém, como possui diversas vulnerabilidades e algoritmos

fáceis de serem quebrados, não deverá ser utilizado. Configurar o equipamento com um desses protocolos colando uma senha forte. Se os equipamentos que utilizarão esta rede são fixos, também utilizar o controle de acesso por MAC, cadastrando o endereço físico destes equipamentos. Isso garantirá uma segurança ainda maior.

Trocar o SSID que vem por padrão nos dispositivos das redes sem fio, e trocar a senha de acesso destes equipamentos, colocando senhas bem elaboradas misturando números e letras, pois atacantes tentam acesso por senhas padrões ou senhas fáceis, que usuários descuidados não alteram.

Deixar os APs desligados se não serão utilizados por determinado espaço de tempo.

Utilizando a rede da forma mencionada, a segurança na utilização desta rede doméstica já estará garantida e poderá ser utilizada sem preocupações.

7.2 Redes Corporativas

Nas redes coorporativas a segurança é fundamental, e brechas podem trazer prejuízos enormes, dados sigilosos podem ser interceptados e/ou alterados para utilização contra a empresa. Por esse motivo deveremos utilizar a maior quantidade de recursos possíveis para garantir a segurança.

Em muitas empresas, isto não é levado a sério, na maioria das vezes pelo fato do proprietário que irá utilizar este tipo de tecnologia não ter um conhecimento das vulnerabilidades das redes sem fio e dos riscos que é deixar uma rede aberta.

Primeiramente, na implementação da rede *Wireless* no cenário corporativo, assim como no cenário doméstico é muito importante o planejamento físico da rede, estabelecendo quantos pontos de acesso serão necessários para cobrir a área de interesse, e estudar locais para posicionamento dos mesmos, de forma que o sinal alcance apenas a área estipulada, e se necessário, ajustar a potência para que o sinal não ultrapasse os limites físicos da empresa. Isto já garantirá uma grande segurança, visto que pessoas externas não conseguirão interceptar o sinal, mas não é o suficiente para termos uma rede segura.

Configurar os APs com uma senha forte (utilizando letras, números e caracteres misturados). Alterar o SSID e deixá-lo oculto ajudará a dificultar interceptores.

Utilizar o protocolo de autenticação WPA2, visto que, como foi estudado no capítulo 5, é o protocolo de segurança mais seguro atualmente, sendo conhecidas poucas vulnerabilidades. Configurá-lo com uma senha bem elaborada para autenticação da rede, e,

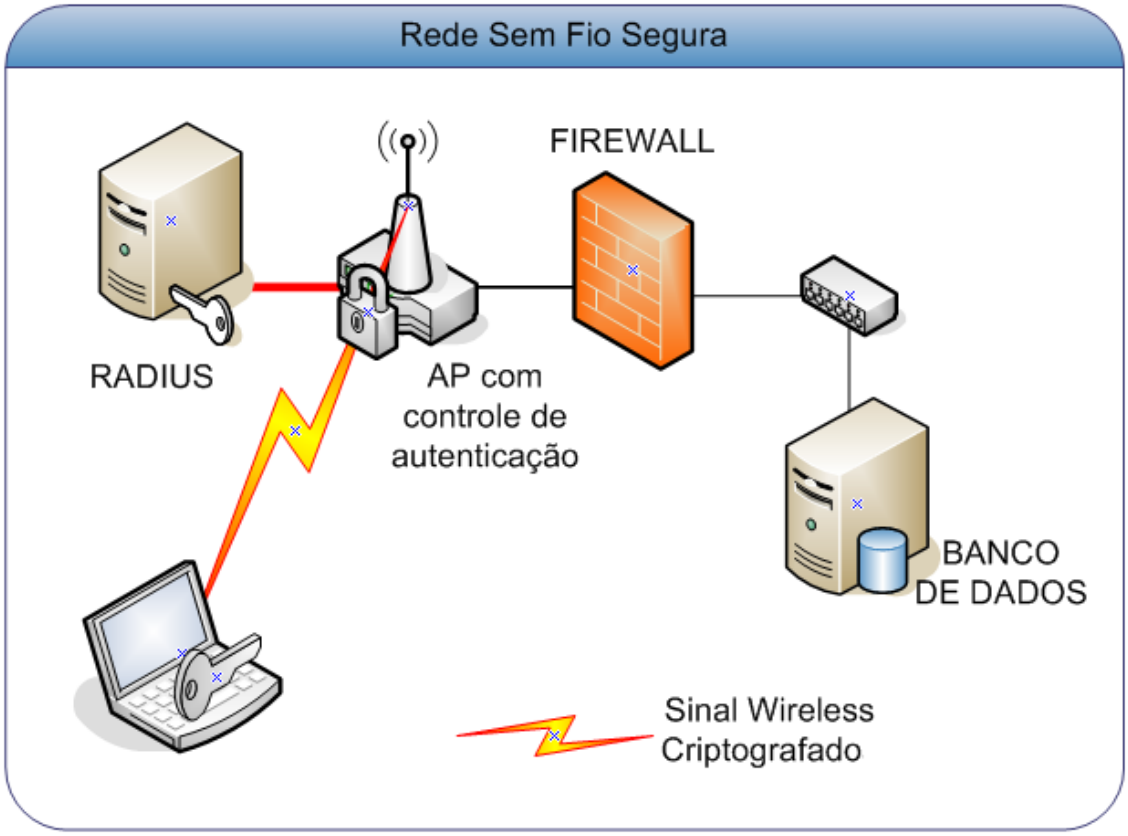
além disso, utilizar controle de acesso através de um servidor RADIUS externo, que será configurado e o banco de dados alimentado apenas com os endereços MACs das estações que utilizará a rede sem fio.

Uma situação importante numa rede corporativa é passar aos funcionários o mínimo de informações possíveis sobre a rede, como SSID, senha para acesso, informações sobre o servidor de autenticação deverão ser mantidos em segredo, evitando que possa sofrer um ataque do tipo "Engenharia Social", que foi abordado no capítulo 4, em que por convencimento do atacante, funcionários passarão informações privilegiadas sobre a rede.

A utilização de um *firewall* entre a rede *wireless* e a rede interna ajuda a filtrar os dados de quem for acessá-la, impedindo que pessoas não autorizadas acessem dados restritos.

A figura 9 ilustra um exemplo de utilização da rede como mencionado anteriormente.

Figura 10: Proposta de Rede Segura.



Alterar periodicamente o SSID e as senhas de acesso, para o caso de alguém descobrir-los, não utilizar por muito tempo.

Numa rede corporativa, a utilização das redes sem fio pode trazer comodidade e facilidades, mas tem-se que ficar cientes de que é necessário o investimento num

planejamento e com componentes que trarão maior segurança, para evitar problemas que tragam grandes prejuízos à empresa. Se a rede for configurada com as especificações passadas neste capítulo, a segurança estará garantida e poderá trafegar os mais diversos tipos de dados sem a preocupação de vazar alguma informação.

7.3 Redes Metropolitanas

As redes metropolitanas são as que mais exigem atenção em relação à segurança, pois o sinal alcançará grandes distâncias, ficará disponível em grande área de cobertura e serão transmitidos os mais diversos tipos de dados. Por esse motivo os equipamentos que implementam este tipo de rede já vêm equipados com os mais fortes sistemas de criptografia de dados e autenticação.

Será configurada nos equipamentos que farão a transmissão do sinal, a chave de segurança, que deverá ser uma senha forte, utilizando letras, números e símbolos, e de preferência utilizar algoritmo de criptografia AES que é um algoritmo muito forte e seguro. Através desta chave com o algoritmo de criptografia, que os dados transmitidos serão escondidos de pessoas não autorizadas.

Um servidor externo de controle de acesso deverá ser utilizado com o banco de dados contendo os endereços MACs das estações que poderão acessar a rede.

Como diferentes áreas dentro da rede utilizarão a comunicação pelo sistema sem fio, é fundamental a configuração de redes virtuais (VLANs) para cada segmento diferente, impedindo que determinado setor enxergue dados de outros setores. A rede virtual isolará as redes, que mesmo passando pelo mesmo canal de comunicação, ficarão separadas como se fossem redes distintas e independentes. Os equipamentos utilizados para as redes *Wimax*, geralmente possuem um recurso de criar SSIDs virtuais, e podendo no mesmo equipamento ter-se vários SSIDs e cada ligado a uma determinada rede virtual (VLAN), assim quando o cliente conectar ao SSID que possui autorização e acesso, já estará trafegando pela rede virtual conseguindo acessar apenas o que está disponível na mesma.

A utilização de *firewalls* para cada setor ajudará a filtrar os pacotes que saem e entram na rede, evitando o acesso não autorizado a dados importantes. Cada VLAN passará por um *firewall* diferente, intermediando o acesso do cliente a servidores e recursos da rede, como banco de dados, acesso a internet, dentre outros.

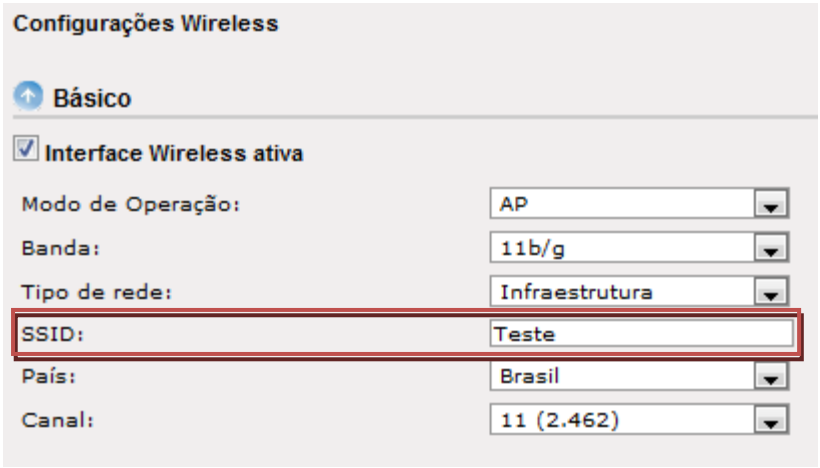
Este tipo de rede exige um planejamento bem elaborado, e um projeto dos pontos que terão acesso a determinados recursos de rede. Os equipamentos das redes *Wimax* já possuem um sistema de segurança forte, pelo próprio fato destas redes ficarem mais expostas e pela quantidade de trafego que será transportado. Os equipamentos para entrarem em funcionamento já exigem as configurações de segurança. Configurando os equipamentos com estas ferramentas e utilizando os recursos passados neste capítulo, conseguiremos garantir segurança também nas redes metropolitanas.

7.4 Estudo de caso

Foi realizado testes conforme a proposta feita para verificar os mecanismos de segurança provenientes nos equipamentos que fornecem sinal para a rede wireless.

Foi configurado o AP com SSID “Teste”.

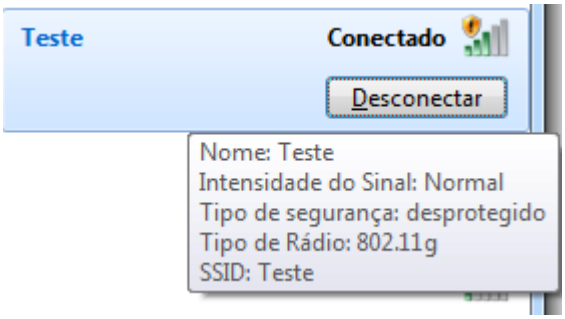
Figura 11 - Configuração do SSID



Quando se utiliza o AP configurado como Sistema Aberto, sem nenhum protocolo de autenticação, qualquer computador conectava-se a rede sem necessidade de informar senha e sem nenhuma restrição.

Figura 12 - Sistema de autenticação aberto

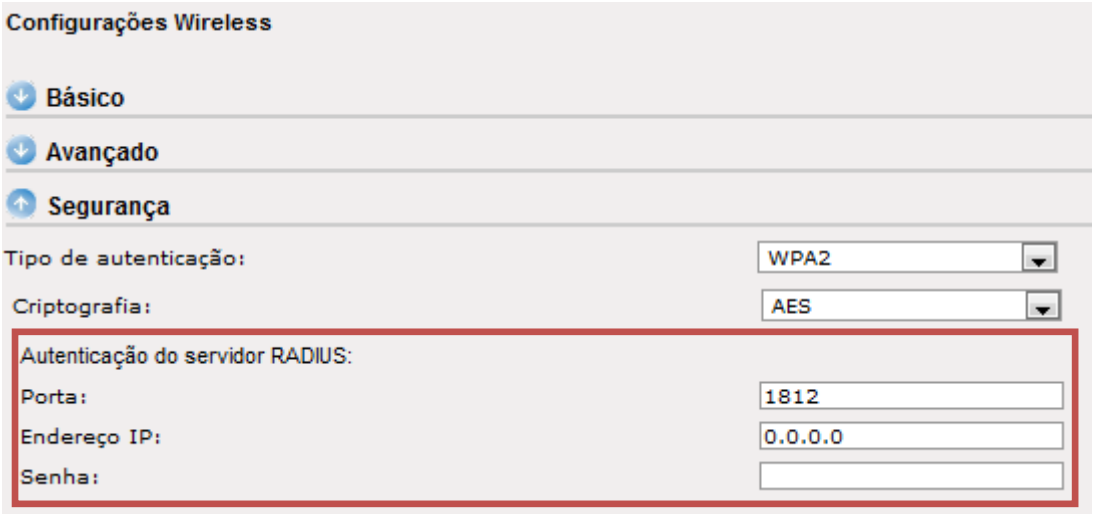
Figura 13 - Conexão com Sistema Aberto



Trocando o tipo de autenticação para WPA2, o AP possibilita a escolha de WPA2-PSK (Pré-Shared Key) com chave pré-compartilhada, para utilização com uma senha, ou através do WPA2 com autenticação num servidor RADIUS externo. Selecionado o WPA2-PSK com algoritmo de criptografia AES, foi colocado uma senha.

Figura 14 - Autenticação WPA2-PSK

Figura 15 - WPA2 com autenticação em Servidor RADIUS



Com autenticação WPA2, logo que se tenta se conectar a rede sem fio é solicitado a senha para acesso à rede.

Figura 16 - Conexão com autenticação

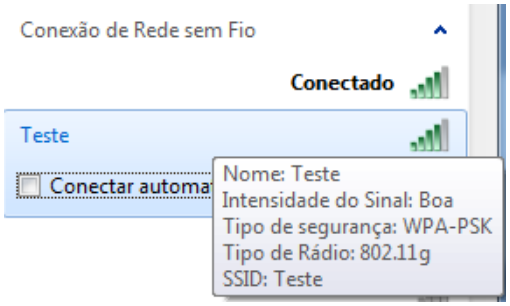
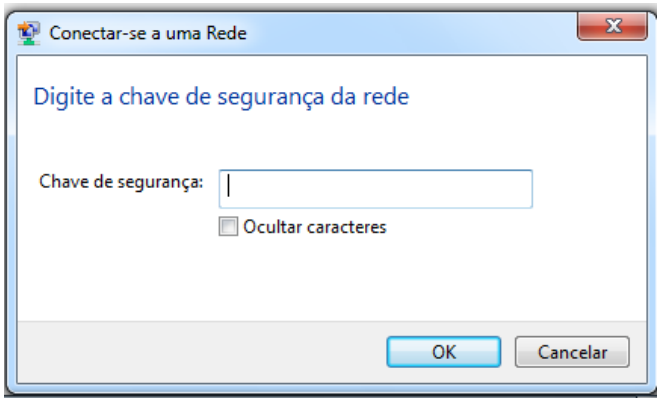
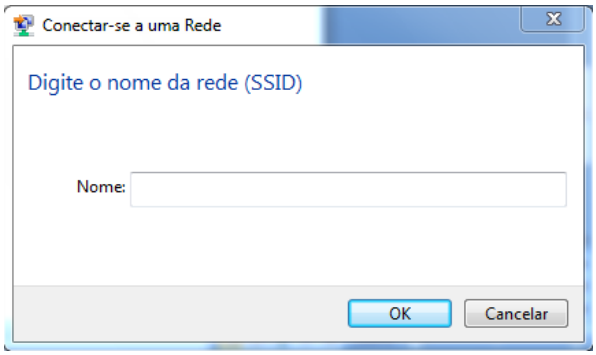


Figura 17 - Solicitação de senha para conexão com a rede



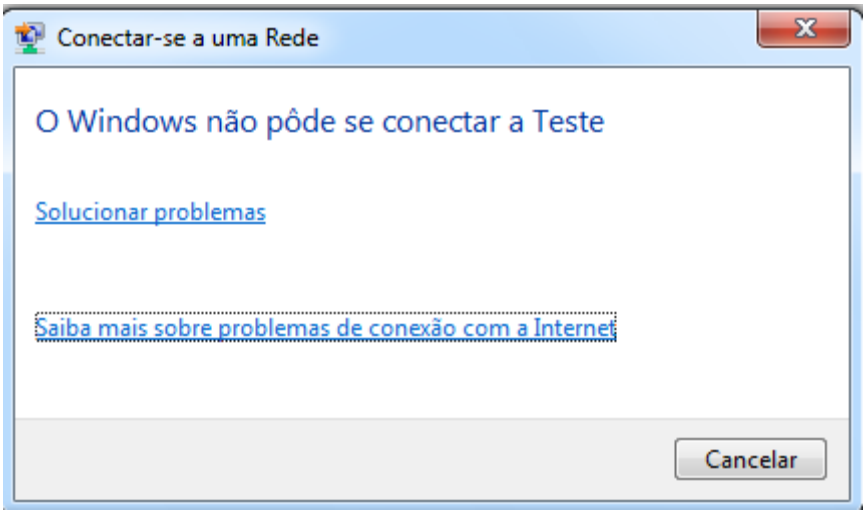
Outro teste realizado foi esconder o SSID. Com esta configuração, quando se tenta procurar redes sem fio ao alcance não é mostrado o nome da rede, mas apenas a identificação “Outra rede”, e ao tentar conectar-se é solicitado a inserção do SSID.

Figura 18 - Solicitação de SSID



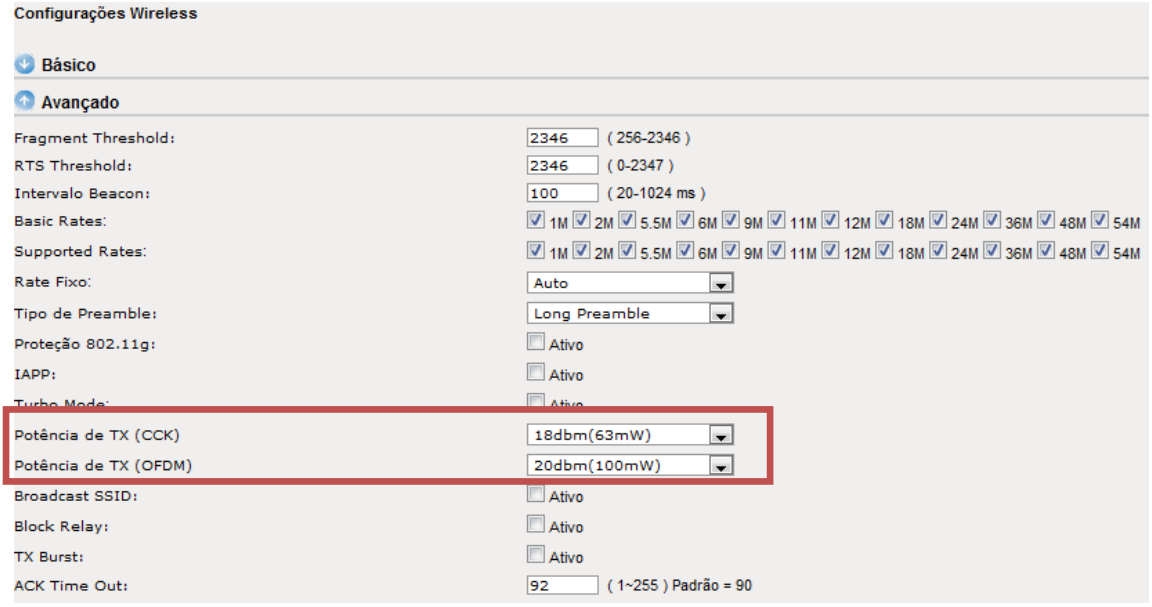
Com a utilização de autenticação de usuário via endereço físico (MAC), e não tendo o MAC do computador a ser utilizado cadastrado no AP, mesmo conhecendo a senha da rede, não é possível conectar-se a mesma.

Figura 19 - Não foi possivel a conexão com a rede



Utilizando um mecanismo provido pelos equipamentos que fornecerão sinal para a rede wireless, é possível ajustar a potência do sinal, para que consiga limitar o raio de alcance à apenas as limitações físicas do estabelecimento onde será utilizado a rede sem fio, garantindo que pessoas de fora não interceptem sinais da rede.

Figura 20 - Ajuste da potência do sinal



CAPITULO 8 – CONCLUSÃO

As redes sem fio vieram para trazer muitas facilidades e novas possibilidades para as redes, sejam elas no cenário doméstico, publico ou corporativo. A tecnologia *Wireless* já muito utilizada, trouxe facilidade para utilização das mesmas, e a tecnologia *Wimax* veio para ampliar ainda mais estas possibilidades para serem utilizadas nas redes metropolitanas. Desta forma pode-se ter maior mobilidade, comodidade, facilidade de instalação, podendo levar sinal onde a tradicional rede cabeada não possibilitaria e diversas outras aplicações.

Porém junto com as redes sem fio, vieram novas vulnerabilidades e brechas que cada vez mais vêem sendo exploradas por hackers e pessoas mal intencionadas para os mais diversos motivos. Essas vulnerabilidades se devem ao fato de o meio de transmissão dos dados ser o próprio ar, podendo ser interceptado por qualquer um que esteja ao alcance do sinal.

Por causa destas vulnerabilidades e para tornar o uso destas redes viáveis, foram criadas diversas ferramentas de segurança, como a criptografia, que esconde os dados que serão transmitidos, podendo ser visto apenas por quem possui a chave de acesso, e sistemas de autenticação que são utilizados para impedir o acesso de pessoas não autorizadas à rede. Junto com as ferramentas de segurança podem ser utilizados outros recursos como *firewalls* e servidores de autenticação externos, aumentando ainda mais a confiabilidade da rede.

Além destas ferramentas, algumas estratégias e precauções podem ser utilizadas para aumentar a segurança, como o próprio planejamento no posicionamento dos pontos de acesso, utilização de senhas mais seguras, ocultação do SSID e manutenção periódica nestas redes.

Foi visto que a falta segurança, ou segurança com níveis baixos, podem trazer sérios riscos e atrair invasores e pessoas mal intencionadas a realizarem ataques, que podem ocasionar sérios prejuízos em qualquer tipo de rede.

Com todo o conteúdo estudado, foi verificado que mesmo com as vulnerabilidades e maior sucessão a ataques, as redes sem fio podem ser utilizadas sem preocupações em qualquer tipo de cenário, desde que, sejam configuradas e planejadas de forma correta. Através disto foi realizado uma proposta de implementação de redes sem fio, para os diferentes cenários, de forma que as tornem seguras, podendo ser utilizadas para as mais diversas aplicações com o máximo de segurança.

Este trabalho poderá ser utilizado por pessoas que queiram saber mais sobre o assunto, por técnicos que realizarão implementações de redes sem fio, ou até por pessoas que

desejam utilizar esta tecnologia, mas ainda possuem algum medo ou dúvida quanto à utilização das redes sem fio.

É deixado como sugestão para trabalhos posteriores, a implementação de redes sem fio como foi proposto, e realização de testes de ataques e quebras da segurança desta rede.

REFERÊNCIAS BIBLIOGRAFICAS

ABELÉM, Antônio Jorge Gomes. Et. al. **Redes Mesh: Mobilidade, Qualidade de Serviço e Comunicação em Grupo**. S.d.

ALBUQUERQUE, Alessandro Ferreira. **Estudo de Métodos de Proteção de Redes Wireless**. 2008. 72 f. Monografia (Pós-Graduação) – Universidade Tecnológica Federal do Paraná. 2008.

AMARAL, Bruno Marques; MAESTRELLI, Marita. **Segurança em Rede Wireless 802.11**. Artigo. S.d.

BARCELAR, Ricardo Rodrigues. **Padrão IEEE 802.16**. Uma Visão Geral sobre o WIMAX. Artigo – União de Escolas Superiores de Rondonópolis. S.d.

DIAS, Gustavo Neves. **IEEE 802.16 – Wimax**. Artigo – Programa de Engenharia de Sistemas e Computação. 2005.

DUARTE, Luiz Otávio. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. 2003. 45 f. Monografia (Graduação) – Universidade Estadual Paulista Júlio de Mesquita Filho. 2003.

GUIMARÃES, Carla Rocha. **Criptografia para Segurança de Dados**. 2001. 37 f. Monografia (Graduação) – Centro Universitário do Triangulo – UNIT. 2001.

LIMA, Luciana dos Santos; SOARES, Luiz Fernando Gomes; Endler, Markus. **Wimax: Padrão 802.16 para Banda Larga Sem Fio**. Monografia – Pontifícia Universidade Católica do Rio de Janeiro. S.d.

LINHARES, André Guedes; GONÇALVES, Paulo André da S. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w**. Artigo – Universidade Federal de Pernambuco. S.d.

MOREIRA, Alexandre Monassa ; MALHEIROS, Eduardo Eber B. **Rede Wi-fi de computadores**. Artigo – Universidade Federal do Pará. S.d.

NICHOLS, Randall K.; LEKKAS, Panos C. **Wireless Security: Models, threats and soluctions**. McGraw-Hill Professional, 2001.

PERES, André; WEBER, Raul Fernando. **Considerações sobre Segurança em Redes Sem Fio**. ULBRA – Universidade Luterana do Brasil. 2002.

QUEIROZ, Leonardo Bastos. **Um Estudo Sobre o Padrão IEEE 802.16 – Wimax**. 2005. 69 f. Monografia (Graduação) – Universidade Federal da Bahia. 2005.

REZENDE, Pedro. A. D. **Criptografia e Segurança na Informática**. Monografia – Universidade de Brasília. S.d.

RUFINO, Nelson Murilo de O. **Segurança em Redes Sem Fio**. Editora Novatec, 2005.

SIEWERT, Vanderson C. **Firewall Suas Características e Vulnerabilidades**. Artigo – Faculdade de Tecnologia do SENAI de Florianópolis, s.d.

SILVA, Luiz Antonio F.; DUARTE, Otto Carlos M. B. **RADIUS em Redes Sem Fio.** S.d. Artigo – Universidade Federal do Rio de Janeiro, s.d.

TANENBAUM, Andrew S. **Redes de Computadores**. Tradução Vandenberg D. de Souza. 4 ed. Rio de Janeiro: Elsevier Editora, 2003.

VERISSIMO, Fernando. **Segurança em redes sem fio.** 2002. 90 f. Monografia – Universidade Federal do Rio de Janeiro. 2002.