FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE - FANESE
NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO – NPGE
CURSO DE PÓS-GRADUAÇÃO "LATO SENSU"
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

MARIA BENILDA BENTO SILVA

SEGURANÇA EM REDES SEM FIO

Aracaju – SE
2009

MARIA BENILDA BENTO SILVA

SEGURANÇA EM REDES SEM FIO

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão da FANESE, como requisito para obtenção do título de Especialista em Redes de Computadores.

Orientador: Sérgio Andrade Galvão

Aracaju – SE
2009

MARIA BENILDA BENTO SILVA

SEGURANÇA EM REDES SEM FIO

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão – NPGE, da Faculdade de Administração de Negócios de Sergipe – FANESE, como requisito para a obtenção do título de Especialista em Redes de Computadores.

Sérgio Andrade Galvão

Mário Vasconcelos Andrade

Maria Benilda Bento Silva

Maria Benilda Bento Silva

Aprovado (a) com média: _____

Aracaju (SE), 17 de Dezembro de 2009.

RESUMO

As reflexões deste artigo concentram-se na análise da tecnologia das Redes Sem Fio, discutindo seus benefícios e sua segurança. Redes Sem Fio têm se tornado um dos meios de acesso à *Internet* mais popular no mundo. Para acessá-la bastam os requisitos: equipamento com dispositivo de recepção do sinal da rede; local de alcance e permissão de acesso à rede pelo usuário.

Palavras-chave: Tecnologia. Redes Sem Fio. Segurança. *Internet*.

ABSTRACT

The reflections of this article focus on the analysis of the technology of wireless networks, discussing their benefits and their safety. Wireless Networks have become a means of access to the Internet more popular in the world. To access it suffice the requirements: hardware device to signal reception of the network; local range and allowed access to the network by the user.

Keywords: Technology. Wireless Network. Security. Internet.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A tecnologia evolui numa velocidade muitas vezes difícil de ser acompanhada, e a cada momento surge uma novidade nesta área.

> O ciberespaço é o novo meio de comunicação que surge da interconexão mundial dos computadores. Não somente a infra-estrutura da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo (LÉVY, 1999, p. 130).

Segundo LÉVY, a maneira como o universo é explorado, bem como as técnicas utilizadas, as atitudes, modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço representam a cibercultura, portanto, a cultura praticada dentro do ciberespaço.

Partindo deste conceito, existem várias formas de conexão de redes à *Internet* no mundo, sejam elas cabeadas ou sem fios, cada qual com suas peculiaridades e importância no mundo da informática, assim, as pessoas podem se comunicar, comprar/vender produtos/serviços, pesquisar, realizar pagamentos, etc., a *Internet* oferece uma série de serviços que podem ser realizados sem a necessidade de deslocamento das pessoas para irem aos *shoppings*, restaurantes, lojas, supermercados, etc.

Mas, a comunicação está indo muito além, pois, com o advento das Redes Sem Fio, qualquer pessoa poderá acessar a *Internet* em qualquer lugar, bastando que esta possua uma máquina equipada com placa de rede *wireless*, esteja em uma área de cobertura da rede e tenha permissão para acessá-la.

As Redes Sem Fio são um sistema de comunicação de dados de fácil mobilidade que utiliza tecnologia de ondas de rádio (MORAES, 2008). Essas redes estão sendo amplamente difundidas, devido, principalmente, à facilidade de uso e de instalação.

Para que se tenha uma Rede Sem Fio é necessário que haja um ponto de acesso, um equipamento (seja *notebook*, *palmtop*, celular, etc.) que possua placa *wireless* e que esteja em uma área de cobertura da rede.

Utiliza-se Redes Sem Fio quando há a necessidade de acesso à *Internet* em qualquer local (com conexão disponível e permissão para acesso); quando não é possível instalar os cabos tradicionais (*UTP*, fibra óptica, etc.) e, quando não existe viabilidade na instalação dos cabos (parede de concreto, tubulações, etc.).

São vários os benefícios que as redes *Wi-Fi* proporcionam comparadas às redes tradicionais, entre eles a mobilidade, a rápida e simples instalação, a escalabilidade, a redução de custo na instalação (em alguns casos). Essa tecnologia possui uma grande quantidade de aplicações em quase todos os setores: hospitais, universidades, fábricas, lojas, bancos, escritório, etc.

São vários os fatores externos que ocasionam interferências nas Redes Sem Fio. Isso ocorre porque não existe proteção em relação ao meio por onde os dados trafegam, já que o sinal é transmitido pelo ar, por isso estas redes precisam estar bem instaladas, com uma configuração de segurança bem implementada, pois, caso contrário, qualquer pessoa que disponha de um *notebook* e algum programa de captura de tráfego poderá facilmente se infiltrar na rede e ter total acesso.

A adoção de Redes *Wi-Fi* pode trazer muitas vantagens, além de ser de fácil instalação. A pesquisa visa identificar os problemas decorrentes das Redes Sem Fio, mostrando que ao projetar esse tipo de tecnologia recomenda-se que as medidas de segurança sejam tomadas, a fim de que não ocorram problemas de acesso por pessoas mal intencionadas.

O objetivo principal desta pesquisa é demonstrar que Redes Sem Fio é uma excelente ferramenta de acesso à *Internet* existente no mundo, visto que é possível conectar-se a *Internet* em qualquer lugar que esteja. Para isto, buscou-se revisar os conceitos dos padrões das Redes Sem Fio; verificar como é possível obter segurança utilizando determinada rede; conhecer algumas ferramentas de ataque, de forma a precaver acesso mal intencionado; e apresentar as vantagens e desvantagens, demonstrando a sua utilidade e importância como ferramenta de acesso à *Internet*.

Esta pesquisa se justifica porque Redes Sem Fio é algo novo na vida da maioria das pessoas. Para instalar uma Rede Sem Fio são necessários alguns cuidados de segurança, a fim de que a rede não fique vulnerável a riscos e ameaças

externas. Os riscos das Redes Sem Fio precisam ser conhecidos para, então, serem minimizados por meio do entendimento das soluções disponíveis e de aplicação de boas práticas.

A metodologia utilizada foi pesquisa exploratória, de natureza bibliográfica, porque se procurou ampliar o conhecimento sobre Redes Sem Fio.

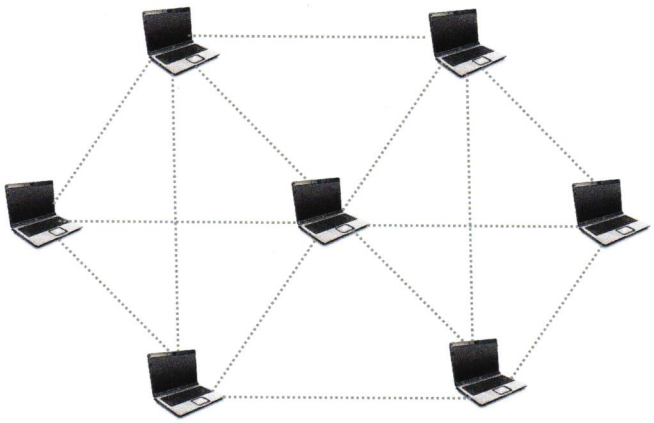
2 REDES WI-FI

O Instituto de Engenheiros Elétricos e Eletrônicos (*IEEE*), responsável pela aprovação de padrões e normas de Redes Sem Fio em todo o mundo, formou um grupo de trabalho com o objetivo de definir padrões de uso em Redes Sem Fio. Um desses grupos de trabalho foi denominado 802.11, que reúne uma série de especificações, onde define como deve ser a comunicação entre um dispositivo cliente e um ponto de acesso. Ao longo do tempo foram criadas várias extensões, onde foram incluídas novas características operacionais e técnicas (RUFINO, 2007).

Comparado com as outras redes, a vantagem desse tipo de conexão é a mobilidade, ou seja, a possibilidade dos usuários poderem se conectar a *Internet* fora de seus escritórios, residências, etc., bastando apenas que estes disponham, por exemplo, de um *notebook*, estejam na área de cobertura da rede e conseqüentemente que tenham permissão para acessá-la.

O *Access Point* é um equipamento que transmite o sinal da rede *Wi-Fi* através de ondas de rádio, por isso, fatores externos ocasionam muito mais interferência nas Redes Sem Fio que as redes convencionais. Nas redes Wi-Fi os dados não dispõem de nenhuma proteção física, no entanto, podem atingir locais de difícil acesso.

Uma das formas de conexão na Rede Sem Fio é utilizando a tecnologia Ad-*Hoc*, onde os equipamentos se conectam diretamente uns aos outros.



Fonte: Elaboração da autora

FIGURA 1 – Arquitetura *Ad-Hoc*

2.1 Padrões atuais

2.1.1 Padrão 802.11b

É o mais conhecido de todos os protocolos, opera a uma faixa de freqüência de 2.4 GHz e permite taxas de transferência de até 11Mbps.

2.1.2 Padrão 802.11a

Opera a uma freqüência de 5 GHz, bem maior que as demais, no entanto, chega a reduzir o alcance para uma mesma potência de transmissão da 802.11b.

2.1.3 Padrão 802.11g

Compatível com a 802.11b, opera a 2,4 GHz e pode alcançar a velocidade de 54 Mbps. Hoje em dia é a mais utilizada entre os demais protocolos de redes *Wi-Fi*.

2.1.4 Padrão 802.11i

Segundo Rufino (2007), este padrão diz respeito a mecanismos de autenticação e privacidade, e pode ser implementado em vários de seus aspectos aos protocolos existentes.

2.1.5 Padrão 802.1n

Foi aprovada em setembro de 2009 pelo *IEEE* a nova norma *wireless* 802.11n. Comparado com os padrões antecessores, 802.11b, 802.11a, 802.11g, o 802.11n é o padrão para alta velocidade que vem atender à demanda de Redes Sem Fio permitindo alcançar velocidades de até 300 Mbps; opera nas faixas de freqüência 2,4 Ghz e 5 Ghz e utiliza a tecnologia *MIMO* (Múltiplas Entradas e Múltiplas Saídas), ou seja, o uso de múltiplos canais simultaneamente (MORAES, 2008).

A freqüência 2,4 GHz é utilizada por uma grande quantidade de equipamentos e serviços, por isso se diz que é poluída, justamente por ser usada também em aparelhos de telefone sem fio, *bluetooth*, forno de microondas, babás eletrônicas e pelos padrões 802.11b e 802.11g. A freqüência 5 GHz não está homogolada no Brasil pela *ANATEL*, agência reguladora governamental, que é o órgão responsável pela licença no Brasil.

Como a taxa de velocidade pode alcançar até 300 Mbps significa que a área de abrangência é maior que os demais padrões, logo, é necessário que tenha maior segurança, pois os riscos de intrusão crescem da mesma forma.

2.1.6 Padrão 802.1x

Esse padrão é baseado na autenticação do usuário pelo endereço *MAC* do adaptador *wireless*.

3 SEGURANÇA DAS REDES WI-FI

Segurança é um dos pontos sobre Redes Sem Fio que ainda está em discussão.

Uma das técnicas nas Redes Sem Fio é o uso de WPA (Acesso Protegido da Redes Sem Fio). No 802.11i é o padrão do *IEEE* que cuida da segurança e possui todas as características do *WPA* e adiciona o requisito de se usar *AES* (Nível de Criptografia Avançado) para criptografia dos dados (ABDULRAHMAN, 2007).

Os grupos do *IEEE* estão procurando formas de melhorar o *WPA* de maneira que ele venha complementar às aplicações *MIMO*. Uma das preocupações é que aumentando o alcance dos sinais, também aumentará a proximidade de atacantes que não precisam estar tão próximos a fim de comprometer a rede (ABDULRAHMAN, 2007).

Outra preocupação é o uso de transmissores de 40MHz na banda de 2.4GHz.

O problema é a interferência dos sinais entre os padrões, por exemplo, no 802.11b e 802.11g. A compatibilidade do padrão 802.11n pode oferecer aos atacantes uma oportunidade de entrar em uma rede através desses sistemas transmitidos. Uma vez lançado o padrão 802.11n, com certeza haverá várias atualizações (ABDULRAHMAN, 2007).

Devido a maior largura de banda e um maior alcance do padrão 802.11n, detecção de intrusões será duas vezes mais longa. Assim, *hackers* terão duas vezes mais tempo para explorar vulnerabilidades (ORTIZ, 2009).

3.1 Endereçamento *MAC*

Para o bom funcionamento de uma rede padrão *Ethernet* ou *Wi-Fi*, cada dispositivo dela deve ter um número único, definido pelo fabricante e controlado pelo *IEEE*, dessa forma pode-se cadastrar o endereço MAC para ter acesso a rede.

3.2 *Wired Equivalent Privacy* (*WEP*)

Conforme Rufino (2007), *WEP* é um protocolo que utiliza algoritmos simétricos, portanto, existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens trafegadas.

3.3 Acesso Protegido da Redes Sem Fio (*WPA*)

O WAP trata de cifração dos dados objetivando garantir a privacidade das informações trafegadas, além de ter como foco a autenticação dos usuários.

3.4 Autenticação

Promove a autenticação do usuário e/ou do equipamento que deseja utilizar recursos de rede. Pode por exemplo, exigir que o usuário use um navegador para promover sua autenticação via protocolo *HTTP*, onde o mesmo deverá digitar o *login* e a senha para se ter acesso à rede *Wi-Fi*.

4 RISCOS E AMEAÇAS

Em se tratando de Redes Sem Fio, os riscos estão mais associados aos aspectos físicos, e da mesma forma que estas ampliam as fronteiras da rede, a área a ser agora vigiada aumenta na mesma proporção.

4.1 Configuração de fábrica

Praticamente todos os equipamentos saem de fábrica com senhas de administração e endereço *IP* padrão. Caso estes não sejam trocados, poderão permitir a um atacante que se utilize delas em uma rede-alvo e tenha condições de identificar todas as configurações feitas, podendo até mesmo modificá-las.

4.2 Envio e recepção de sinal

De acordo com RUFINO (2007) o posicionamento dos componentes da Rede *Wi-fi* pode ser determinante na qualidade da rede e na segurança, pois dependendo de onde se localiza o concentrador dentro do ambiente, este poderá enviar sinal tanto para dentro como para fora da área de abrangência.

4.3 Negação de serviço

Alguns equipamentos, como *Bluetooth,* conseguem ter potência suficiente para enviar um sinal que ocupe toda ou grande parte da faixa usada pela rede, mesmo se o protocolo detectar a existência de ruído em um determinado canal, não restará nenhum outro intervalo disponível para transmissão, visto que esta foi toda ocupada pelo sinal atacante.

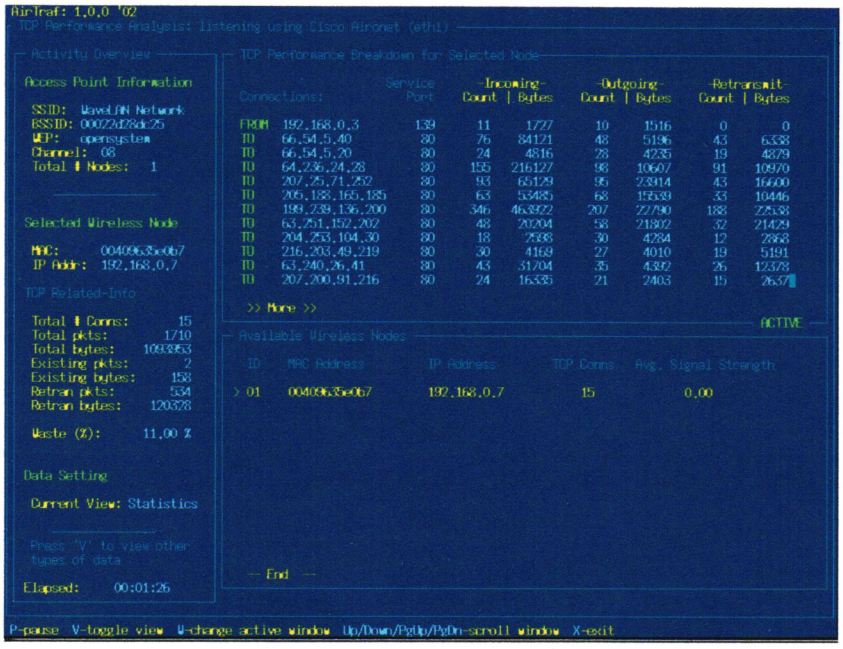
4.4 Captura de tráfego

As redes *Wi-Fi* são propagadas pelo ar por ondas de radiofreqüência, então, nada mais normal serem passíveis de captura. Desta forma, tudo que um atacante precisa fazer é estar na mesma área de cobertura do sinal e munido de um *notebook* e uma ferramenta de captura de tráfego.

5 TÉCNICAS E FERRAMENTAS DE ATAQUE

De acordo com RUFINO (2007), a maioria dos ataques para Redes Sem Fio pode ser efetuada utilizando ferramentas específicas, tais como: *Airtraf*, *Netstumbler*, *Kismet*.

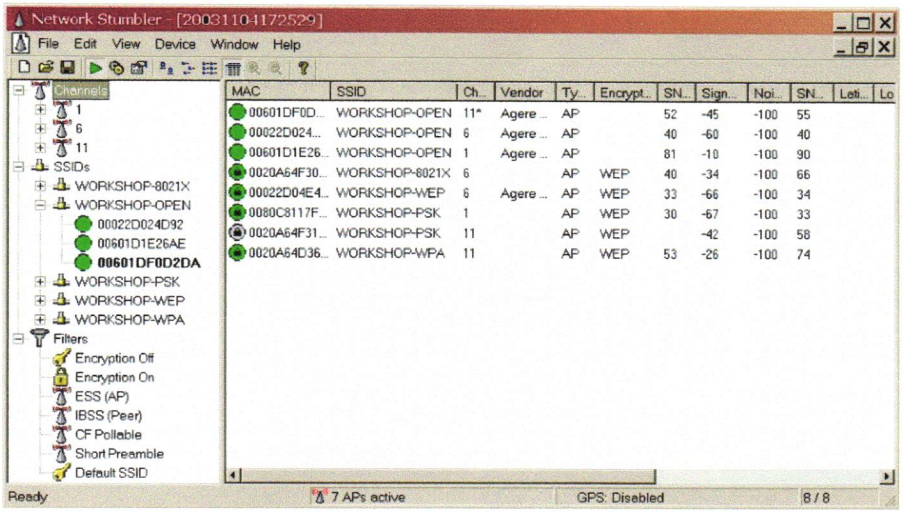
O *Airtraf* permite coletar informações em Redes Sem Fio em tempo real, exibindo clientes conectados e serviços utilizados.



Fonte: http://www.elixar.com/corporate/history/airtraf-1.0/airtraf_screenshots.php

FIGURA 2 – Tela do *Airtraf*

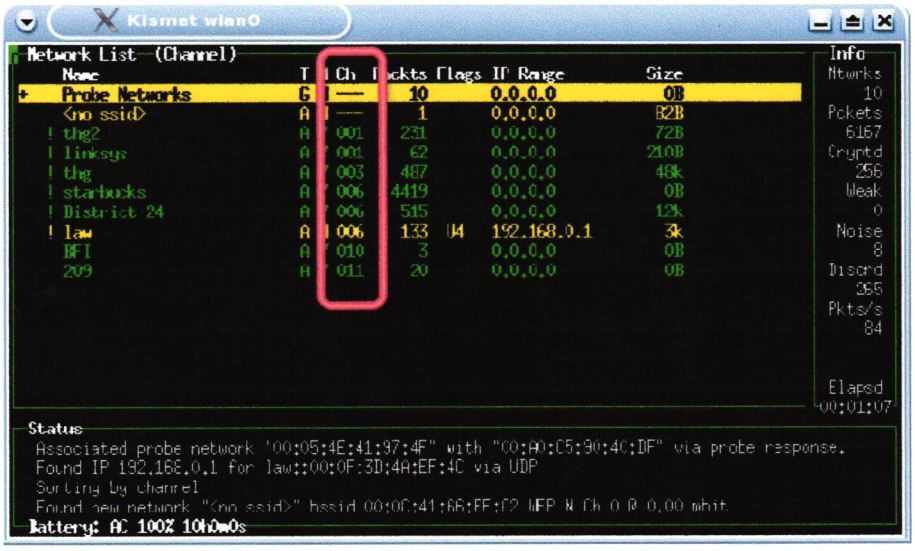
O *Netstumbler* mapea e identifica Redes Sem Fio em ambiente *Windows*, o programa permite integração com equipamentos *GPS* e obtém um mapa preciso de pontos de acesso identificados.



Fonte: http://www.isp-planet.com/technology/2004/security_toolkit_analysis_2.html

FIGURA 3 – Tela do *Netstumbler*

O *Kismet* é uma ferramenta que permite identificar não somente os concentradores, mas também redes *Ad-Hoc* e obter informações detalhadas sobre as redes encontradas: nome da rede; nível de sinal, etc.



Fonte: http://manhaswireless.3forum.biz/downloads-f1/download-kismet-t9.htm

FIGURA 4 – Tela do *Kismet*

6 VANTAGENS E DESVANTAGENS

Como em qualquer tecnologia, existem vantagens e desvantagens que podem ser analisadas antes de se adquirir determinado tipo de tecnologia.

6.1 Vantagens

A mobilidade de acesso à *Internet*, sem precisar estar necessariamente dentro de casa ou escritório, é a grande vantagem;

Hoje, na maioria dos *notebooks,* já vem integrada a placa de dispositivo para conexão a rede *Wi-Fi*;

Compartilhar a rede para outros computadores. Custo mais baixo, haja vista que é possível compartilhar a rede para outros computadores;

Facilidade de instalação. No projeto mais simples, basta obter um ponto de acesso, no caso do computador *desktop* uma placa *wireless*, que pode ser externa ou interna.

Flexibilidade, visto que não é preciso perfurar paredes para fazer tubulação de cabos.

6.2 Desvantagens

São vários materiais que podem causar interferência no sinal da rede *Wi-Fi*, tais como:

- Telefones sem fio que operam a frequência de 2,4GHz, a mesma utilizada pelas maiores das Redes Sem Fio;
- Computador no chão, quanto mais alto, melhor para captar o sinal da rede;
- Reservatórios de água (como aquários, bebedores, etc.);
- Microondas, visto que eles também operam a 2,4GHz, o ideal é que eles fiquem em ambientes isolados do ambiente onde se encontra a rede;

- Metal;
- Vidro;
- Parede de concreto;
- Árvores;
- Cobre;
- Madeiras pesadas;
- Grandes pilhas de papel.

E ainda mais, se o ponto de acesso não estiver em um lugar central da casa, pode haver perda de sinal, o ideal é que o *Access Point* esteja em um local aberto, não havendo nenhuma barreira que possa interferir na propagação da rede.

7 CONSIDERAÇÕES FINAIS

As redes *wireless* apresentam uma série de benefícios se comparadas às redes tradicionais, entre eles, a mobilidade, a rápida e simples instalação e de ser uma solução completa para grandes, médias e pequenas empresas.

São vários os fatores externos que ocasionam mais interferências nas Redes Sem Fio que as Redes Cabeadas. Isso ocorre porque não existe proteção em relação ao meio por onde os dados trafegam, já que o sinal é transmitido pelo ar. P por isso, estas redes precisam estar bem instaladas, com uma configuração de segurança necessária, pois caso não ocorra, qualquer pessoa que disponha de um *notebook* e com algum programa de captura de tráfego poderá facilmente se infiltrar na rede e ter total acesso. Então, ao instalar uma Redes Sem Fio é necessário fazer uma análise do tipo: saber se no ambiente que se pretende instalar as Redes Sem Fio possui alguma interferência na faixa de operação da rede; implementar os mecanismos de segurança (com criptografia); verificar se existe rede cabeada para realizar a integração; se o padrão 802.11 é compatível com as aplicações existentes; se é financeiramente viável instalar a Redes Sem Fio.

Redes *Wi-Fi* tem suas vantagens no que diz respeito ao custo-benefício se comparadas com as redes cabeadas, estas limitadas aos tamanhos de cabos; espaço em que será realizado o cabeamento estruturado; além de contratar um técnico que realize o trabalho físico, analisar a parede, saber se dentro dela existe algum material que possivelmente irá causar interrupção do sinal, etc, ao utilizar uma Redes Sem Fio, praticamente não existe problemas em espaço físico, apenas será preciso investir em um ponto de acesso e ter cuidado com a segurança da rede.

Como todas as tecnologias, existem pontos negativos e pontos positivos. Dentre os negativos estão: maior consumo de energia elétrica dos dispositivos, devido às antenas e maiores facilidades para os ataques externos.

Este artigo apresentou as características, funcionamento, algumas ferramentas de ataque e segurança utilizadas pelos padrões das Redes *Wireless* (Sem Fio).

REFERÊNCIAS

ABDULRAHMAN, Y. et al. **802.11n - The New Wave in WLAN Technology**. Murray State University, USA, 2007.

KUROSE, James F. ET al. **Redes de Computadores e a Internet: Uma abordagem Top-down**. São Paulo: Pearson, 2006.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

MORAES, Alexandre Fernandes de. **Redes de Computadores: Fundamentos**. São Paulo: Érica, 2008.

ORTIZ, S. **IEEE 802.11n - The Road Ahead**. Technology News, 2009.

RUFINO, Nelson Murilo de O. **Segurança em Redes Sem Fio: aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**. São Paulo: Novatec, 2007.

GLOSSÁRIO

Ad-Hoc – Arquitetura de rede.

Airtraf – Ferramenta de acesso indevido a Redes Sem Fio.

Netstumbler – Ferramenta de acesso indevido a Redes Sem Fio.

Kisnet – Ferramenta de acesso indevido a Redes Sem Fio.

Wireless – Redes Sem Fio.

Wi-Fi – Acrônimo para *wireless fidelity* (fidelidade sem fios).

Mbps – Taxa de transmissão de dados.

ANATEL – Agência Nacional de Telecomunicações.

MAC – Endereço físico da placa de rede do computador.

WPA – Acesso Protegido da Rede Sem Fio.

AES – Nível de Criptografia Avançado.

MIMO – Tecnologia da Rede Sem Fio que serve para alcançar uma distancia de sinal maior.

Hackers – Especialistas em violar sistemas de computação.

Ethernet – Tecnologia de interconexão para redes locais.

HTTP – Protocolo de comunicação na internet.

Login – Qualquer nome para identificar o acesso à internet, rede, computador, etc.

IP – Protocolo da internet.

GPS - Sistema de rádionavegação baseado em satélites.

Access Point – Concentrador que propaga o sinal da Rede Sem Fio.

Cabo UTP – Cabo com 8 fios trançados para conexão do micro na rede.