# SEGURANÇA EM REDES *WIRELESS* 802.11 INFRAESTRUTURADAS

*Helio Brilhante Pereira*[1]

Curso de Especialização em Administração em Redes Linux (ARL)

Universidade Federal de Lavras - MG (UFLA)

## RESUMO

As redes *wireless*, baseadas no conjunto de padrões IEEE 802.11 (*Institute of Electrical and Electronics Engineers*), têm se expandido vertiginosamente nos últimos anos, tanto no meio empresarial quanto doméstico. Paralelamente à sua popularização, multiplicaram-se os problemas de segurança, fazendo-se imprescindível uma análise cuidadosa dos riscos inerentes a essa tecnologia, bem como das formas de proteção disponíveis.

**Palavras-chave**: redes *wireless*, segurança, tecnologia

## INTRODUÇÃO

Dentre os tipos de rede existentes, as redes sem fio, também conhecidas como *Wireless*, Wi-Fi (*Wireless Fidelity*) e WLANs (*Wireless Local Access Network*), têm adquirido grande destaque pelas suas características de mobilidade, flexibilidade, simplicidade de instalação e baixo custo. Todavia, essa facilidade traz consigo riscos importantes à segurança, principalmente devido à instalação dos equipamentos sem as configurações adequadas [1], o que deixa muitas redes domésticas e até mesmo de empresas, completamente vulneráveis. Segundo Nakamura [2], e só para que se tenha uma dimensão do problema, há pouco tempo um estudo de análise de segurança em redes realizado nos Estados Unidos nos aeroportos internacionais de *Denver* e *San Jose*, detectou que a *American Airlines* operava uma rede sem fio totalmente

1 Email: hbrilhante@gmail.com

desprotegida, tendo sido possível inclusive monitorar o tráfego de operações de *check-in* na mesma.

Outro fator que afeta diretamente a segurança das redes Wi-Fi é o próprio meio de transmissão que torna essas redes mais expostas, vez que os dados são transmitidos através de ondas de rádio pelo espaço. Como o meio de transmissão é compartilhado entre todas as estações conectadas à rede, todo o tráfego fica visível para todos [1], o que representa um grande risco, pois para capturar qualquer pacote de dados, o atacante não precisa sequer estar no mesmo ambiente físico, podendo estar em qualquer local dentro da área de cobertura do sinal. Propagado dessa forma, o sinal pode alcançar até três quilômetros de raio [3, 4], na ausência de obstáculos importantes, podendo ser rastreado com uma antena de alto ganho [4], possível de ser construída até mesmo com materiais simples como uma lata de batatas *Pringles* [5]. Eis então outra vulnerabilidade inerente à tecnologia das redes sem fio. Não há como controlar o alcance do sinal da rede, sendo possível a qualquer pessoa com poucos conhecimentos técnicos e uma antena adequada, conectar-se a ela, usufruir do acesso à Internet e até mesmo alcançar arquivos e outros recursos compartilhados na rede local [4], caso ela não esteja devidamente configurada.

Visando amenizar esse cenário tão hostil, foram desenvolvidos algoritmos de criptografia para uso nas redes Wi-Fi que embaralham os dados, tornando-os incompreensíveis para quem não possui a chave de acesso [4]. Tais algoritmos, se utilizados de modo adequado, garantem razoável nível de segurança para os dados que trafegam nas WLANs. Outra ferramenta de defesa importante para ambientes que requerem um nível mais elevado de proteção são as VPNs (*Virtual Private Network*) [6 - 8], que criam uma espécie de túnel por onde os dados trafegam de forma criptografada. Juntamente com a VPN é importante o uso de um *firewall* [8], uma espécie de filtro que trabalha analisando pacotes de dados que chegam, decidindo o que pode passar e o que deve ser retido, baseado em um conjunto de regras predefinidas. Estas

duas tecnologias combinadas produzem um ótimo nível de segurança, dificultando sobremaneira as tentativas de acesso indevido.

Para Tanenbaum [9], no contexto das redes domésticas a segurança deve ser de fácil utilização, mesmo para usuários inexperientes e arremata: “Isso é algo mais fácil de dizer do que fazer, até mesmo no caso de usuários altamente sofisticados.”. Em resumo, Tanenbaum [9] acredita que o futuro das redes sem fio é promissor, mais ainda apresenta alguns desafios como a necessidade de ser fácil de administrar, confiável e segura, mesmo para usuários não técnicos.

Considerando que o termo “redes *wireless*” abrange vários tipos de redes sem fio, desde telefonia celular, passando por redes de pequeno alcance como as redes *Bluetooth* e chegando até às redes metropolitanas conhecidas como WiMAX (*Worldwide Interoperability for Microwave Access*), é importante frisar que o presente trabalho tem como objetivo a análise, sob o aspecto da segurança, das redes *wireless* baseadas nos padrões 802.11. Mais especificamente, serão analisadas as redes de topologia infraestruturada, que necessitam de um equipamento concentrador para a distribuição do sinal e que representam a grande maioria das redes domésticas e de pequenos escritórios, além de ser comum em aeroportos, *shoppings* e *cyber cafés*.

O presente trabalho visa, além de fazer uma análise acurada das vulnerabilidades que cercam a tecnologia das redes sem fio, alertar técnicos e usuários para o risco de configurações inadequadas e do uso dessas redes sem os cuidados básicos.

## Fundamentos das Redes *Wireless*

### Modo de Transmissão

No Brasil, o órgão responsável pelo licenciamento de frequências de

radiotransmissão é a ANATEL (Agência Nacional de Telecomunicações) que, seguindo convenções internacionais, disponibiliza três segmentos de radiofrequência para uso sem necessidade de licenciamento [1], conforme resolução n.º 365 de maio de 2004 e seu anexo, que trata dos equipamentos de radiocomunicação [10]. As frequências disponíveis em cada uma das três faixas são: 902 – 928 MHz; 2,4 – 2,5 GHz e 5,150 – 5,825 GHz. Dentre essas faixas de frequência, as de nosso interesse são as duas últimas, posto que são as faixas utilizadas pelos padrões 802.11b, 802.11g (2,4 GHz) e 802.11n (5 GHz) que representam quase a totalidade dos equipamentos para redes sem fio disponíveis atualmente.

Segundo Haykin e Moher [11], a transmissão sem fio ocorre com a geração de um sinal elétrico contendo as informações desejadas no transmissor e propagação das ondas de rádio correspondentes. No outro polo, o receptor se incumbe de recuperar o sinal elétrico gerado no transmissor. Em síntese, o sinal elétrico é convertido pela antena em onda de rádio, que então é propagado através do ar e depois convertido novamente em sinal elétrico pelo receptor.

### Padrão IEEE 802.11

Iniciado em 1997, o padrão 802.11 usa a faixa de 2.4 GHz e previa taxas de transmissão de 1 e 2 megabits. Em 1999 o instituto publicou as especificações do padrão 802.11b que podia chegar a 11 megabits e foi o responsável direto pela popularização da tecnologia [4]. Paralelamente, a equipe de engenheiros do IEEE trabalhava no padrão 802.11a, que foi publicado logo em seguida e utiliza a faixa de frequência de 5 GHz, aumentando a velocidade nominal para 54 megabits, porém, alcançando somente a metade da distância atingida pelo padrão 802.11b ao usar o mesmo tipo de antena. Por existirem menos dispositivos operando na faixa dos 5 GHz, essa é uma faixa menos sujeita a interferências, todavia, perdeu espaço no mercado devido ao lançamento antecipado de equipamentos no padrão

802.11b, que usam a faixa de 2.4 GHz. Em seguida foram publicadas as especificações do padrão 802.11g que incorporou novas tecnologias de modulação do sinal, sendo o mais utilizado atualmente, funcionando também na frequência de 2,4 GHz e suportando velocidade nominal de 54 megabits [12, 13]. Dispositivos mais recentes são capazes de funcionar nos padrões 802.11b, 802.11g e 802.11a simultaneamente.

A partir de 2004 o IEEE vem trabalhando numa nova especificação que visa alcançar taxas de transmissão superiores às redes cabeadas de 100 megabits. Para tal, vem adicionando melhorias no algoritmo de transmissão, combinado com o uso de MIMO (*Multiple-Input Multiple-Output*), que permite o uso de vários fluxos de transmissão simultâneas, utilizando-se para isso de mais de um conjunto de receptores, transmissores e antenas. Este novo padrão chama-se 802.11n e, apesar de ainda não estar completamente concluído, alguns fabricantes lançaram, ainda em 2008, alguns equipamentos com a denominação "*draft n*" que conseguem chegar a incríveis 300 megabits nominais de velocidade, mantendo ainda a compatibilidade reversa com os padrões 802.11b e 802.11g [4].

## Segurança no Padrão 802.11

A primeira iniciativa do IEEE visando tornar as redes sem fio seguras foi o padrão WEP (*Wired-Equivalent Privacy)* que, como o próprio nome sugere, pretendia prover às redes Wi-Fi, um nível de segurança equivalente ao das redes cabeadas [4], o que obviamente mostrou-se falso dada a grande facilidade com que a criptografia desse protocolo pode ser quebrada. De fato, o uso de chaves estáticas e vetores de inicialização que são transmitidos em claro, combinado com outras vulnerabilidades do WEP [2], tornam essas chaves muito fáceis de ser quebradas, tanto as de 64 bits, que podem ser quebradas em poucos segundos, quanto às de 128 bits que podem ser quebradas em pouco mais de dez minutos. Segundo Morimoto [4], "Usar WEP em uma rede atual é como fechar a porta de casa com um arame".

Visando eliminar dois dos principais problemas do WEP, a saber, uso de chave estática e criptografia fraca [2], novos padrões de segurança para as redes sem fio foram especificados e receberam o nome de 802.11i, que não é um novo padrão de rede, mas sim um padrão de segurança para as redes *wireless* [4] já existentes. Nesse diapasão, a *Wi-Fi Alliance*, como medida emergencial e baseada no padrão 802.11i, ainda em fase de finalização em 2003, especificou o WPA (*Wi-Fi Protected Access)*, com criptografia feita por TKIP (*Temporal Key Integrity Protocol*), cuja chave de criptografia é trocada periodicamente, o que, combinado com outras melhorias, tornou o WPA relativamente seguro.

Com a versão final do padrão 802.11i, ratificada em 2004, foi lançado o padrão WPA2 [4], que utiliza o sistema de criptografia AES (*Advanced Encryption Standard*), muito mais robusto e baseado no uso de chaves de 128 a 256 bits, o mesmo usado pelo governo dos Estados Unidos. O único inconveniente é que esse padrão é mais complexo e exige maior poder de processamento dos equipamentos, o que pode ser um problema para roteadores sem fio mais antigos ou mais baratos.

Segundo Morimoto [4], ao usar TKIP (WPA) ou AES (WPA2), é importante definir uma boa *passfrase*, com pelo menos 20 caracteres aleatórios, o que torna quase impossível a quebra desses protocolos.

Por fim, há duas possibilidades de uso do WPA, o WPA *Personal* (WPA-PSK) (*Pre-Shared Key*), que usa uma chave previamente compartilhada e o WPA *Enterprise* (WPA-RADIUS) (*Remote Authentication Dial In User Service*), onde há a necessidade de um servidor de autenticação RADIUS (podendo ser um computador rodando Linux com o FreeRADIUS) para controlar a autenticação dos usuários [4].

## Topologia de Redes *Wireless*

### *Ad-Hoc*

Nesse tipo de topologia não há um equipamento concentrador e a comunicação é estabelecida diretamente entre os clientes [1]. Utilizada de modo esporádico e temporário, com fins específicos como troca de arquivos em reuniões, esse tipo de rede possui alcance reduzido e pouca utilização.

### Infraestruturada

Nas redes infraestruturadas (figura 01), que são o foco deste trabalho, há a presença obrigatória de um equipamento concentrador chamado Ponto de Acesso e não é permitida a comunicação direta entre os clientes, pois tudo deve passar pelo concentrador, também conhecido como AP (*Access Point*) [1], ou roteador *wireless*. Essa topologia apresenta duas vantagens importantes: a) todo o controle da rede é feito de forma centralizada como autenticação, limitação de banda, efetuação de bloqueios, habilitação de criptografia, dentre outros; e b) facilidade de interligação da rede *wireless* com redes cabeadas pré-existentes e à Internet.

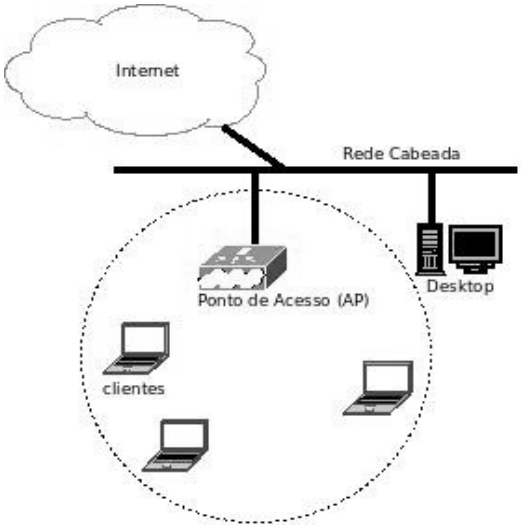


Figura 01: Rede Infraestruturada

## VULNERABILIDADES INERENTES À TECNOLOGIA

### Configuração de Fábrica

Esta é sem dúvidas uma das principais vulnerabilidades detectadas em um grande número de redes Wi-Fi. A grande maioria dos Pontos de Acesso saem de fábrica com ESSID (*Extended Service Set Identifier*), senha de administração e endereçamento IP (*Internet Protocol*) padrões [1], sendo que essas informações encontram-se disponíveis nos manuais dos equipamentos e nas páginas WEB dos respectivos fabricantes. Sendo assim, caso não sejam trocadas, permitem fácil acesso de estranhos à rede, inclusive com a possibilidade de modificá-las posteriormente.

### Configuração Aberta

Trata-se de uma falha de segurança bastante comum, principalmente para quem não tem noção dos riscos inerentes às redes sem fio [1], uma vez que, mesmo alterando as configurações de fábrica, o Ponto de Acesso é deixado no modo aberto, que é o padrão de fábrica, onde aceita conexões sem exigir autenticação alguma. Para piorar a situação, se o servidor DHCP (*Dynamic Host Configuration Protocol*) estiver ativo no equipamento, basta que o invasor ligue seu equipamento e associe-se à rede para receber um endereço IP válido e passe a compartilhar o acesso à Internet e a todos os recursos disponíveis na mesma. Sendo assim, é imprescindível que o modo de segurança do equipamento seja ativado para que exija autenticação para associação à rede.

### Área de Cobertura do Sinal

Como vimos, não há meios eficientes, na grande maioria dos equipamentos atuais, para restringir o alcance do sinal de radiofrequência emitido pelo *Access Point*, mas, segundo Rufino [1], podemos minimizar o problema posicionando o AP de forma centralizada no ambiente, afastado de

janelas e paredes externas. Tal procedimento melhora a distribuição do sinal e impede que ele vaze com grande intensidade, o que facilitaria o trabalho de um possível invasor, que poderia, com alguns conhecimentos, mapear todo o ambiente da rede e usar essas informações para desferir um ataque eficiente, com objetivos variados como simplesmente compartilhar o acesso à Internet, desferir ataques a terceiros, obter informações sigilosas, etc. Como todo o tráfego nas redes *wireless* está sujeito a ser capturado e copiado, todas as informações podem ser conhecidas, caso não estejam cifradas, não havendo nem mesmo a necessidade do atacante estar associado à rede alvo. Essa fragilidade é particularmente preocupante quando usuários incautos acessam redes sem fio públicas em aeroportos, *shoppings* ou cafés.

## Tipos de Ataques Frequentes

Conforme Uchôa [14], os tipos de ataque mais comuns a que as redes sem fio estão sujeitas são basicamente os mesmos sofridos pelas redes cabeadas como *scanning*, *sniffers*, *spoofing* e *denial of service*. A seguir analisaremos os ataques mais frequentes que podem ocorrer tanto nas redes cabeadas quanto nas redes *wireless* com algumas adaptações, sendo mais efetivos nas redes sem fio pelas vulnerabilidades intrínsecas à tecnologia destas.

### MAC *spoofing*

Este tipo de ataque é geralmente desferido contra redes *wireless* cujo concentrador foi habilitado para permitir a autenticação baseada em uma tabela de endereços MAC (*Media Access Control*) autorizados. Consiste basicamente no atacante clonar o endereço de MAC de uma interface de rede válida, fazendo-se passar por ela, ganhando com isso acesso à rede. Isso pode ser conseguido de diversas formas, sendo as mais comuns a captura e análise de tráfego ou um ataque de força bruta via *software,* que gera números aleatórios

no padrão de endereços MAC até que algum seja reconhecido pela rede [13].

### Negação de Serviço - DoS (*Denial of Service*)

Segundo Uchôa [14], os ataques de negação de serviço haviam recebido pouca atenção até a derrubada completa de servidores importantes como *Amazon*, *Yahoo* e UOL.

Nas redes *wireless* o atacante, usando um *notebook* ou mesmo um PDA (*Personal Digital Assistant*), desfere uma enxurrada de tentativas de associação ao *Access Point* até bloquear todos os *slots* livres, impedindo assim a associação de usuários legítimos [13]. Alternativamente, o atacante pode inundar o concentrador com pacotes de desassociação, forçando os usuários legítimos a fecharem suas conexões [13], tomando posse da rede. Outra forma ainda, deste tipo de ataque, consiste em puro vandalismo [1], onde o atacante impinge um sinal de ruído com potência suficiente para preencher toda a faixa de frequência da rede (2.4 ou 5 GHz), de modo a paralisá-la completamente.

### Associação Maliciosa

Neste tipo de ataque o agressor configura sua placa de rede *wireless* para funcionar como um *Access Point* aberto [13], posicionando-se em locais públicos com grande concentração de pessoas, como aeroportos ou *shoppings centers.* Feito isto, basta esperar que usuários incautos conectem-se à rede "aberta", com o intuito de navegar na Internet e, sem o saber, passam a ter seus passos monitorados, sendo esta uma preparação para o ataque seguinte, *man-in-the-middle*. Uma variação extremamente perigosa e eficaz desse ataque consiste na substituição de um *Access Point* válido por outro controlado pelo atacante. Essa substituição pode ser efetivada através de um ataque de negação de serviços no equipamento válido, sendo em seguida oferecido acesso ao equipamento controlado pelo atacante. Desse modo, os usuários são levados a crer que estão conectados a um Ponto de Acesso confiável, quando na verdade estão nas mãos do atacante.

### *Man-in-the-Middle*

Este tipo de ataque pode ser iniciado através de um ataque de negação de serviço (DoS), que força o usuário a se desassociar do concentrador verdadeiro. Pode também partir de um ataque de associação maliciosa, como visto acima. Nos dois casos, após a desconexão dos usuários, é oferecido para nova conexão, um concentrador falso controlado pelo atacante [13]. Obtendo sucesso nesta fase, o agressor passa então a intermediar a comunicação da vítima com a Internet, capturando todas as informações disponibilizadas pelo usuário como *logins*, senhas e arquivos. Um exemplo prático pode ser observado quando o usuário tenta acessar sua conta bancária através dessa conexão. Se um ataque *man-in-the-meadle* estiver em curso, o usuário é conduzido a uma página falsa, onde é solicitado a fornecer sua senha de acesso que, paralelamente, é utilizada pelo atacante na página verdadeira do banco. Desse modo o atacante obtém acesso total e irrestrito à conta bancária da vítima.

## RECOMENDAÇÕES DE SEGURANÇA

Neste tópico serão apresentadas recomendações genéricas de segurança que podem ser implementadas ou ativadas diretamente nas configurações dos equipamentos da rede, independente do sistema operacional utilizado, bem como recomendações de segurança para uso de redes *wireless* públicas. As recomendações apresentadas devem ser adicionadas em camadas sucessivas, provendo desta forma, níveis cada vez maiores de defesa.

Das recomendações apresentadas a seguir, as duas primeiras provêem um tipo de proteção conhecida como “segurança por obscuridade” [1], que não representam um mecanismo de defesa efetivo, pois baseiam-se apenas no fato do atacante desconhecer algumas informações da rede, o que faz com que

estes sejam considerados métodos  frágeis. Todavia, quando combinados com outros mecanismos de defesa, inibem os ataques mais simples e dificultam sobremaneira o êxito dos ataques mais sofisticados.

### Não Divulgação do ESSID

O ESSID nada mais é que o nome da rede. Esta regra, que é configurada no próprio concentrador, procura dificultar ataques escondendo o nome da rede [1], ou seja, não divulgando-o através de requisições de *broadcast*. Em termos práticos, significa que o atacante teria que saber de antemão o nome da rede alvo para poder promover um ataque. É considerado um procedimento frágil de segurança devido ao fato de que o nome da rede pode ser obtido pela captura e análise de pacotes da própria rede, utilizando-se para isto, programas facilmente encontrados na Internet como o Kismet [15].

### Alteração do ESSID Padrão

Como o ESSID padrão consta dos manuais e das páginas dos fabricantes na Internet, sua alteração inibe tentativas de ataque menos sofisticadas, não sendo de todo efetivo pelo fato de que o novo ESSID também pode ser capturado pela captura e análise do tráfego da rede.

### Modificação da Senha Padrão de Administrador

Esta recomendação parece óbvia, mas é incrivelmente grande o número de administradores que negligenciam esta regra tão básica, deixando o *Access Point* com a senha de administrador padrão que vem de fábrica [2]. Nunca é demais enfatizar a importância de usar uma boa política de senhas no momento da troca.

### Desabilitação do Serviço de DHCP

Em redes domésticas ou de pequenos escritórios, onde o número de equipamentos é reduzido, é aconselhável atribuir endereços IP fixos aos clientes e desabilitar essa funcionalidade que atribui endereços IP

dinamicamente aos equipamentos que se associam ao *Access Point*.

### Controle de Acesso por MAC

Este procedimento incrementa o nível de segurança ao permitir que apenas clientes com endereço MAC da placa de rede cadastrados no *access point,* possam se associar e acessar a WLAN [2]. Lembrando que através de um ataque de MAC *spoofing* é possível driblar esse controle e usar um endereço de uma placa cadastrada no concentrador.

### Criptografia de autenticação WPA/WPA2/802.11i

Atualmente os padrões de segurança WPA e WPA2 são os únicos que provêem um nível aceitável de segurança para autenticação nas redes *wireless*. É recomendado o WPA-PSK (*Personal*) para uso doméstico e pequenos escritórios e o WPA2-RADIUS para empresas que podem dispor de um computador com características de servidor, para instalação do FreeRADIUS que se encarregará da autenticação dos usuários [4].

### Utilização de Redes *Wireless* Públicas

Esta recomendação refere-se aos procedimentos de segurança a serem observados por usuários de redes Wi-Fi públicas disponíveis em *shoppings*, *cyber cafés*, aeroportos, dentre outros locais. Ao conectar-se a essas redes, é imprescindível que o equipamento do usuário esteja com seu sistema operacional atualizado, um bom anti-vírus ativo, um *firewall* configurado adequadamente e com o recurso de compartilhamento de pastas e arquivos desativado. É importante também lembrar que não é seguro utilizar essas redes para acessar sistemas remotos sensíveis que exijam autenticação com *login* e senha, muito menos efetuar operações de acesso a contas bancárias.

## Considerações Finais

Indiscutivelmente as redes *wireless* conquistaram seu espaço e vieram para ficar. Sua imensa popularização é sem dúvida fruto dos vários benefícios que elas propiciam aos usuários, como flexibilidade, acessibilidade, mobilidade e baixo custo. Porém, trouxeram também consigo, riscos importantes à segurança, que podem restringir sua utilização em ambientes que manipulam informações sensíveis.

Como sabemos, não existem redes *wireless* cem por cento seguras, mas os atuais padrões permitem a implementação de níveis aceitáveis de segurança, exigindo porém, conhecimentos adequados das peculiaridades da tecnologia utilizada. Ainda como forma de redução de riscos residuais, é recomendável a implementação de uma camada extra de proteção via *software*, com uso de um túnel VPN, maximizando sobremaneira o nível de segurança adotado.

Por fim, conclui-se que o futuro das redes sem fio está intimamente relacionado ao desenvolvimento de padrões de segurança cada vez mais robustos que garantam a confiabilidade, integridade e confidencialidade das informações.

## Referências


[1] **Rufino**, N. M. de O.; **Segurança em Redes sem Fio**; São Paulo; Novatec; 2.ª ed.; 2005.

[2] **Nakamura**, E. T.E; Geus, P. L.; **Segurança de Redes em Ambientes Cooperativos**; São Paulo; Novatec; 2007.

[3] **Engst**, A.E; Fleishman, G.; **Kit do iniciante em redes sem fio: o guia prático sobre redes Wi-Fi para Windows e Macintosh** – 2.ª ed.; Tradução Edson Furmankiewicz; Título original: The Wireless Networking: starter kit; São Paulo; Pearson Makron Books; 2005.

[4] **Morimoto**, C. E.; **Redes, Guia Prático**. Porto Alegre; Sul Editores; 2008.

[5] http://www.oreillynet.com/cs/weblog/view/wlg/448. Acessado em janeiro de 2009.

[6] **Farias**, P. C. B.; **Treinamento Profissional em Redes Wireless;** São Paulo; Digerati Books; 2006.

[7] **Leitner**, A.; **Segredos sem fio**. Linux Magazine Especial n.º 01; Janeiro de 2007; p 68 – 72.

[8] **Morimoto**, C. E.; **Servidores Linux, Guia Prático**; Porto Alegre; Sul Editores; 2008.

[9] **Tanenbaum**, A. S.; **Redes de Computadores**. 4.ª ed.; Tradução Vandenberg D. de Souza; Rio de Janeiro; Elsevier; 2003.

[10] http://www.anatel.gov.br/Portal/documentos/biblioteca/Resolucao/2004/Anexo_res_365_2004.pdf. Acessado em janeiro de 2009.

[11] **Haykin**, S.E; Moher, M.; **Sistemas Modernos de Comunicações Wireless;** Tradução de Figueiredo, G. E.E; Nascimento, J. L.; Porto Alegre; Bookman; 2008.

[12] **Edney**, J.; Arbaugh, W. A.; **Real 802,11 security: Wi-Fi protected access and 802,11i;** New York; Hamilton in Castleton; 2008.

[13] **Vacca**, J. R.; **Guide to Wireless Netowrk Security**; New York; Springer Science+Business Media; 2006.

[14] **Uchôa**, J. Q.; **Segurança Computacional**. 2.ª ed.; Lavras-MG; UFLA/FAEPE; 2005.

[15] http://www.kismetwireless.net/. Acessado em fevereiro de 2009.