UNIVERSIDADE SÃO FRANCISCO

CURSO DE ENGENHARIA ELÉTRICA

SEGURANÇA EM REDES WIRELESS 802.11B

Engenharia Elétrica

por

Renato Dian

Peter Jandl Junior, Mestre
Orientador

Itatiba (SP), Dezembro de 2005.

UNIVERSIDADE SÃO FRANCISCO

CURSO DE ENGENHARIA ELÉTRICA

SEGURANÇA EM REDES WIRELESS 802.11B

Engenharia Elétrica

por

Renato Dian

Trabalho de Conclusão do Curso apresentado à Banca Examinadora como requisito parcial para a obtenção do Certificado de Conclusão do Curso de Engenharia Elétrica.
Orientador: Peter Jandl Junior, Ms.

Itatiba (SP), Dezembro de 2005.

Dedico este trabalho especialmente à minha família que permitiram a realização deste Curso de Graduação que sempre estiveram me apoiando e me incentivando a superar os obstáculos e a seguir em frente com garra e dedicação, encorajando-me à cada batalha perdida à fim de vencer a guerra.

AGRADECIMENTOS

A realização deste trabalho se tornou possível devido à colaboração de pessoas e instituições. A todos manifesto a minha gratidão. E de modo especial:

ao Prof. Ms. Peter Jandl Junior pela orientação e pelo incentivo à desenvoltura deste trabalho, estimulando-me e auxiliando-me a cada etapa concretizada;

ao Engenheiro em Telecomunicações da NORTEL NETWORKS, Fernando Marcus Miwa, pela orientação científica e pelas discussões e críticas que, em muito, enriqueceram a realização deste trabalho;

aos professores do curso de Engenharia Elétrica que tanto contribuíram para o meu crescimento, profissional, intelectual e pessoal;

aos meus amigos de sala pelo companheirismo durante os cinco anos da graduação e pelo incentivo para que eu pudesse chegar até aqui e;

aos meus familiares que sempre me deram forças, me admiraram e sempre estiveram ao meu lado.

Mire e Veja: O importante e bonito do mundo é isto: que as pessoas não estão sempre iguais, ainda não foram terminadas, mas que elas vão sempre mudando.

(GUIMARÃES ROSA)

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

AP: Access Point
ARP: Address Resolution Protocol
BSS: Basic Service Set
CRC: Cyclic Redundancy Check
CSMA/CA: Carrier Sense Multiple Access – Collision Avoidance
DCF: Distributed Coordination Function
ESS: Extended Service Set
FCC: Federal Communications Commission
ISM: Industrial Scientifical Medical
IBSS: Independent Basic Service Set
IEEE: Institute of Electrical and Electronic Engineers
ID: Identification
IP: Internet Protocol
FCC: Federal Communicaations Commissions
FHSS: Frequency Hopping Spread Spectrum
GPS: Global Positioning Site
MAC: Medium Access Layer
NIC: Network Interface Card
OFMD: Orthogonal Frequency Division Multiplexing
OSI: Open System Interconnect
PCF: Point Coordination Function
PHY: Physical Layer
PRNG: Pseudo-Random Number Generator
RC4: Rom Ciphe 4
RF: Radio Frequency
SSID: Service Set Identifier
USB: Universal Serial Bus
VI: Vetor de Inicialização
VPN: Virtual Private Network
WECA: Wireless Ethernet Compatibility Alliance
WEP: Wired Equivalent Privacy
Wi-Fi: Wireless Fidelity
WLAN: Wireless Local Area Network
WPAN: Wireless Personal Area Network
WWAN: Wireless Wide Area Network
XOR: Extended OR

LISTA DE TABELAS

LISTA DE FIGURAS

DIAN, Renato. Segurança em redes wireless. Itatiba, 2005. 35f. Trabalho de Conclusão de Curso, Universidade São Francisco, Itatiba, 2005.

RESUMO

Nos últimos anos, uma nova tecnologia de comunicações, denominada rede wireless, vem tomando grandes proporções de mercado e apresenta algumas vantagens sobre as tradicionais redes. A sua utilização está associada a diversos meios, podendo realizar coberturas de pequenos escritórios até grandes indústrias. Porém, devido à vulnerabilidade existente, pessoas mal intencionadas utilizam este novo cenário para ganhar acesso à rede e comprometem a segurança dos dados trafegados. Baseado em fundamentos do padrão 802.11 da IEEE, este trabalho apresenta as falhas e propõe opções de segurança existente.

DIAN, Renato. Wireless network security. 2005, Itatiba. 35f.Graduate Report, São Francisco University, 2005, Itatiba.

ABSTRACT

In last years, a new communication technology, called wireless network, is growing in the market and it shows some advantages over tradicional networks. Its utilization is associated with several ways, and it can cover small office´s area until big industries. However, with a existent vulnerability, bad intentioned people uses the new scenery to gain network access and pledges the trade information security. Rely on 802.11 pattern basis, from IEEE, this work shows the failures and proposes the existent security options.

1. INTRODUÇÃO

A grande competitividade em busca de redes com alta performance, confiavéis e sem necessidade de grandes infra-estruturas, envolvendo os maiores fabricante e pesquisadores, deram origem as redes WPANs (Wireless Personal Area Network), WLANs (Wireless Local Area Network) e WWANs (Wireless Wide Area Network). Com o objetivo de proporcionar maior mobilidade e fácil instalação física, surgem as *wireless networking*. O padrão 802.11b é o foco deste trabalho, pois é o mais utilizado. A teoria básica para entender o funcionamento das redes *wireless* e identificar falhas de segurança presentes no padrão 802.11b e propor possíveis soluções para as possíveis falhas detectadas foram relatadas neste trabalho. Dentre os tópicos apresentados, tem-se o padrão 802.11b, contendo o modo de funcionamento, uma breve comparação com outros padrões e os dispositivos utilizados. A fim de proteger contra as vulnerabilidades existentes nas redes *wireless* e fornecer um nível de segurança idêntico ao das redes com fio, foi criado o protocolo WEP (Wired Equivalent Privacy). Estão explicado os conceitos introdutórios do WEP, assim como o seu funcionamento, sem deixar de discutir possíveis soluções para as falhas.

2. PADRÃO 802.11

2.1. TECNOLOGIA WIRELESS

A tecnologia *wireless* é um dos padrões atuais de conexão de dispositivos que permite a comunicação sem a necessidade do uso de fios. A vantagem deste tipo de conexão está na mobilidade, sendo que o usuário pode acessar informações de qualquer área onde exista a abrangência da rede. A grande desvantagem é a baixa largura de banda e o excesso de *overhead*, que chega a passar de 50 %. [1]

Exitem diversos tipos de redes *wireless*, mas é comum classificá-las em três grupos, conforme a área de abrangência: [2]

-WWAN: redes de grande cobertura.

-WLAN: redes *wireless* de cobertura local

-WPAN: redes de uso pessoal de pequena abrangência. Ex.: Bluetooth e Infra-vermelho.

As redes *wireless* proporcionam flexibilidade e portabilidade muito maior do que as redes cabeadas. Utiliza sinais de rádio freqüência para possibilitar a comunicação entre os dispositivos.

Para controle e o ingresso de novos dispositivos na rede cabeada, fazemos uso de um equipamento denominado *hub*. Já as redes *wireless*, o equipamento que tem essa função é o AP (Access Point). Também pode atuar como um *bridge* entre a rede sem fio e a rede guiada. O uso de um adaptador de rede *wireless* (NIC - Network Interface Card) é indispensável para os dispositivos integrantes desta rede.

Para um conjunto de dispositivos controlado por um único AP denominamos BSS (Basic Service Set). Rede onde as estações comunicam-se sem a necessidade de um AP são conhecidas IBSS (Independent Basic Service Set). Podem ser conhecidas também por *ad-hoc*.

A área de cobertura de uma rede *wireless*, denominamos de células. Dentro desta célula, os usuários podem se locomover livremente com os seus dispositivos. A interligação de outras células, permite que os usuários se desloquem por diferentes áreas de abrangência sem perder conexão e a isso denominamos *roaming*.

2.2. VANTAGENS

O uso de redes *wireless* proporciona vários benefícios, dentre os quais destacam-se: [1]

-Rápida instalação: o fato de não usar fios para as conexões, a instalação física requer menos tempo.

-Mobilidade: é o ponto mais significante. O usuário consegue acessar todos os recursos da rede desde que esteja dentro da área de cobertura.

-Escalabilidade: permite que as redes de computadores aumentem de tamanho (estrutura física), de acordo com as necessidades do usuário.

-Custo Agregado : apesar de ter um custo inicial elevado, apresenta benefícios como a robustez (ex: resistência a fenômenos naturais, como terremotos) e menor tempo gasto com a manutenção. [3]

Como já era de se imaginar, as redes *wireless* também possuem algumas desvantagens. O alto custo dos dispositivos é um deles, visto que ainda são produtos novos no mercado. Uma outra desvantagem é a insegurança física destas redes, já que podem ser facilmente interceptadas.

2.3. O PADRÃO 802.11

Datada de meados dos anos 80, quando a FCC (Federal Communications Commissions) disponibilizou faixas de freqüência de rádio para utilização, surgiu a tecnologia *wireless*. Em 1990, foi lançado um projeto em que a tecnologia *wireless* abrangesse as camadas MAC (Medium Access Control) e física (PHY), conforme a Figura 1, do modelo OSI (Open System Interconnect). Em 1997 foi aprovado o padrão internacional de interoperabilidade 802.11 e em seguida, 1999, o IEEE aprovou os padrões 802.11a e 802.11b. Criar uma base de padrões que englobasse diferentes tipos de codificações físicas, freqüências e aplicações era o objetivo buscado. [1]

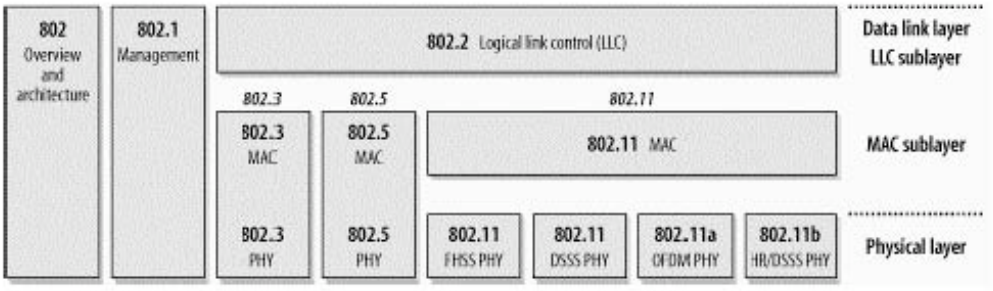

Figura 1 - Padrão 802 e o modelo OSI.

A Tabela 1 apresenta algumas características do padrão 802.11:

Característica	Descrição
Camada Física	**DSSS, FHSS ou IR**
Frequência	**2.4 e 5 GHz**
Taxas de Transmissão	**1, 2, 5.5, 11 e 54 Mbps**
Alcance	**50 metros em ambientes fechados e 450 metros em ambientes abertos**

Tabela 1 - Características do padrão 802.11

2.4. PRINCIPAIS PADRÕES 802.11

Os principais padrões 802.11 serão brevemente apresentados abaixo: [4]

IEEE 802.11: é o primeiro padrão criado para redes sem fio. Apresenta suporte a WEP e a implementação do sistema de rádio na banda ISM (Industrial Scientifical Medical) de 900 MHz e 2.4 GHz com taxa de 2 Mbps canalizado em FHSS (Frequency Hopping Spread Spectrum).

IEEE 802.11a: é o padrão que descreve as especificações da camada de enlace lógico e física para redes sem fio que atuam no ISM de 5 GHz com taxas de transferência de dados entre 6 e 54 Mbps. Não existem muitos dispositivos que atuam nesta freqüência. Utiliza a tecnologia de OFMD (Orthogonal Frequency Division Multiplexing).

IEEE 802.11b: descreve a implementação dos produtos WLAN mais comuns em uso atualmente. Inclui aspectos da implementação do sistema de rádio e especificação de segurança. Apto a operar em 2.4 GHz, provê 1, 2, 5.5 e 11 Mbps de taxa. Sua aprovação foi concedida em julho de 2003 e é certificado para operar com outros dispositivos Wi-Fi (Wireless Fidelity) da WECA (Wireless Ethernet Compatibility Alliance), fundado a fim de garantir um padrão único.

IEEE 802.11g: é uma derivação do padrão 802.11b e descreve o mais recente padrão para redes sem fio, operando na mesma freqüência, porém, com taxas de transferências podendo chegar a 54 Mbps. Utiliza a tecnologia de OFMD.

Também existem os padrões 802.11c, 802.11d, 802.11e, 802.11f, 802.11h, 802.11i e 802.11n.

2.5. ESTRUTURA

Podemos definir duas arquiteturas de funcionamento: *ad-hoc* e infra-estruturada. O modelo de operação da *ad-hoc* nada mais é que cada cliente comunicar-se com os outros da mesma rede diretamente, sem uso de AP (Figura 2). É facilmente implementada quando os dispositivos estão próximos geograficamente. [5]

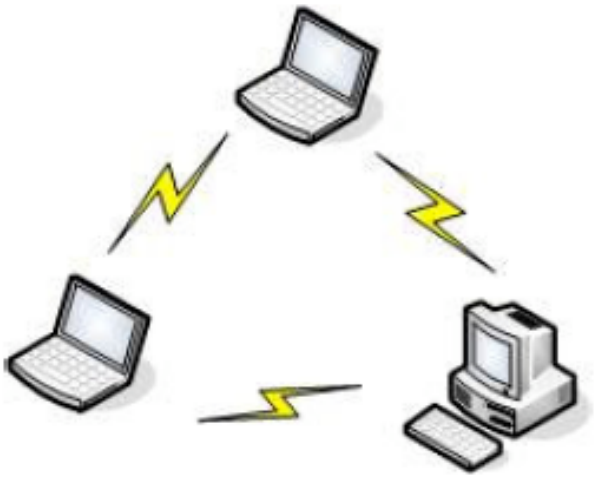

Figura 2 - Topologia *Ad-hoc*

Constituídas por diversas estações *wireless*, as quais devem estar obrigatoriamente conectadas a um AP para se comunicar (Figura 3), denominamos de redes infra-estruturadas. [6]

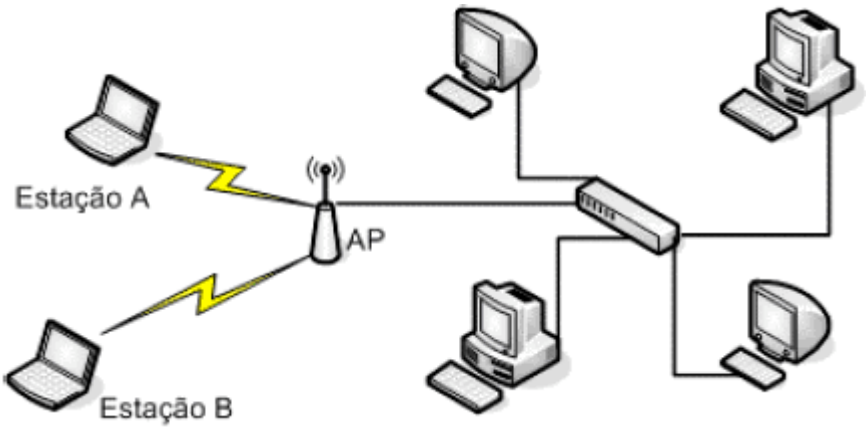

Figura 3 - Topologia Infra-estruturada.

Quando dentro da área de abrangência do AP (célula), todo equipamento que participar da infra-estrutura poderá acessar os dados da rede. O conjunto de células de uma rede BSS é chamada de ESS (Extended Service Set). A Figura 4, exemplifica como os usuários se deslocam entre diferentes células, sem perder a conexão. [7]

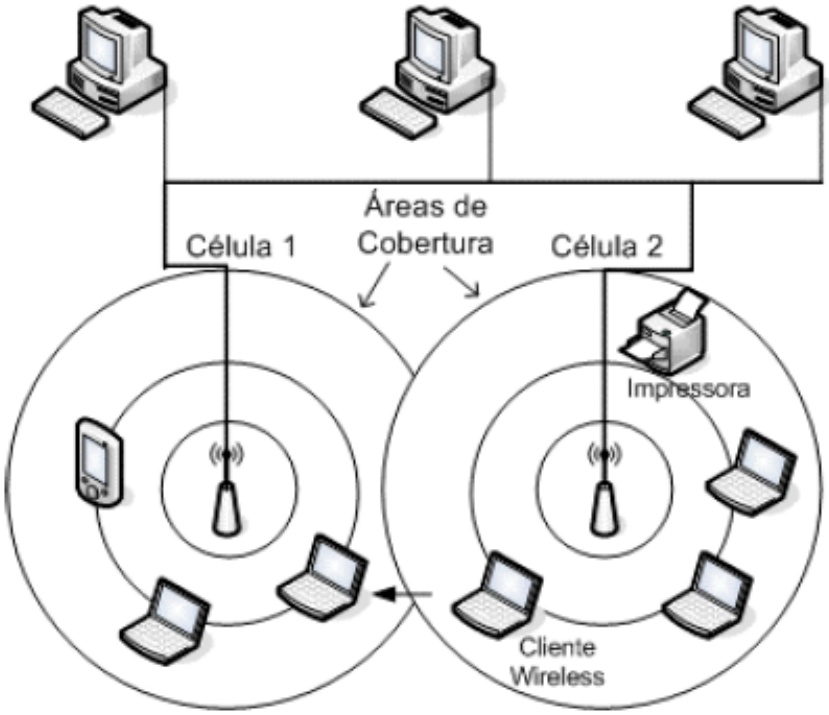

Figura 4 - Estrutura ESS.

Para se ter uma estrutura de rede *wireless*, dois equipamentos são obrigatórios: o AP e estações *wireless*. [4]

O AP possui uma interface 802.11 e um software de *bridging*. Funciona como um ponto base para as outras estações da rede, atuando como intermediador das diversas estações, além de possibilitar a ligação entre redes cabeadas e *wireless*.

A estação *wireless* (cliente) necessita de um NIC instalado. Os equipamentos que mais utilizam os NIC, são os *laptops*.

As antenas são de grande importância para o funcionamento da WLAN. Sua função é converter os sinais elétricos em ondas de rádio e vice-versa. Possibilita o aumento da área de abrangência (maior recepção de sinais) de um AP. Temos dispositivos que possuem antenas integradas e outros com antenas removíveis. Classificam-se as antenas em dois tipos:

- Omni-direcionais: propagam sinais de RF igualmente em todas as direções (espalhamento espectral).

- Direcionais: transmitem sinais de RF para apenas uma direção.

2.6. SINAL DE TRANSMISSÃO

O alcance de uma rede *wireless* é variável, visto que depende de uma combinação de diversos fatores (interferências, características físicas do meio, conectividade, uso de antena, atenuações). O uso correto de antenas apropriadas e amplificadores podem melhorar o alcance. Grande parte dos APs que são oferecidos no mercado possuem uma antena omni-direcional acoplada, isto é, se o AP estiver posicionado no centro de uma sala, a probabilidade do sinal alcançar toda a sala será muito grande. [4]

Os sinais transmitidos tendem a ser atenuados e é representado numa escala de decibéis (dB), pois encontram diversos obstáculos no seu caminho. Em ambientes abertos, a atenuação é fácil de ser medida, visto que não possui nenhum obstáculo (janela, porta, parede, objetos diversos), contudo, em ambientes fechados, a situação não é a mesma. Na Tabela 2, podem se ver alguns exemplos comuns de atenuação de sinal em ambientes fechados:

Obstáculo	Escala
Parede divisória	**3 dB**
Janela	**3 dB**
Parede de Concreto	**4 dB**
Vidraça com borda de metal	**6 dB**
Porta de Metal	**6 dB**
Porta de Metal em uma parede de tijolos	**12,4 dB**

Tabela 2 - Exemplos de atenuação no sinal

2.7. BRIDGING

Definida como a interligação física de duas ou mais WLANs. Os AP que possuem esta função, permitem a troca de dados entre diferentes redes, conforme Figura 5. Possibilita 2 tipos de configurações:

- Ponto-a-ponto: duas redes são ligadas através dos respectivos AP. [1]

- Multiponto: uma sub-rede está conectada a diversas outras sub-redes, por meio do AP de cada sub-rede.

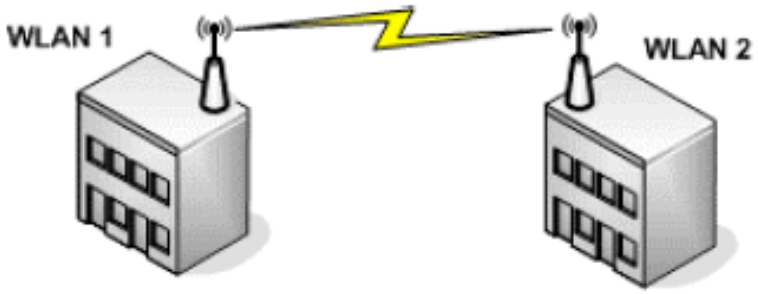

Figura 5 – Bridging entre redes *wireless*.

2.8. CAMADA FÍSICA E DE ENLACE

O MAC é a camada de controle de acesso ao meio especificada pelo padrão 802.11 dentro da camada de enlace. Toda estação deve obter algum tipo de acesso ao meio para transmitir os pacotes. Para o padrão 802.11, tem-se duas formas de acesso ao meio: [4]

- Distributed Coordination Function (DCF): se uma estação está transmitindo dados na rede, as demais estações aguardam o término da operação, para que não haja colisões de pacotes (utiliza o protocolo CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance).

- Point Coordination Function (PCF): permite acesso ao meio para uma estação específica, sendo assim, as demais estações não podem começar a transmitir até que sejam escolhidas pelo AP.

Especificamente a camada física do 802.11b possui algumas características:

- Scanning: tem o *scanning* passivo e ativo. O modo passivo faz com que cada NIC busque canais individuais para encontrar o AP com melhor sinal. Realizando *broadcast* de um *beacon frame* que contém informações do AP, o NIC do rádio recebe estes *beacons* enquanto esta realizando *scanning* e registra a intensidade dos sinais correspondentes. No modo ativo, o funcionamento é semelhante. O NIC do rádio envia em *broadcast* um *probe frame* (pacote de teste) para que os APs que estejam dentro da faixa correspondente respondam com um *probe response* (pacote de resposta). Este método tem uma desvantagem, visto que causa um maior tráfego na rede.

- **Autenticação:** tem duas formas de autenticação, que será apresentada adiante.

- **Associação:** antes de enviar os pacotes, o NIC rádio deve associar-se ao AP. Um pedido de associação é realizado através do envio de um *frame*. O AP responde com um pacote de confirmação ou recusa.

- **Criptografia WEP:** possibilita o uso de criptografia na troca de pacotes. Discuteremos o WEP com detalhes adiante**.**

- **Modo de Economia de Energia (Power Save Mode):** esse modo encontra-se ativo quando o NIC deseja hibernar, isto é, não vai mais enviar pacotes. Quando o AP recebe um pacote endereçado a um NIC hibernado, armazena os pacotes, para enviá-los posteriormente. O AP registra os NIC que estão hibernando para facilitar o armazenamento.

- **Fragmentação:** em pequenos *frames*, fragmenta os pacotes de dados. Quando um pacote é perdido, evita a necessidade de retransmitir todo um grande pacote.

2.9. AUTENTICAÇÃO

A autenticação sem criptografia é bastante utilizada nas redes, sendo assim, existem duas maneiras de autenticar, mas lembrando, são consideradas primitivas e inseguras: [5]

- **Sistema de Autenticação Aberto (Open System):** para ser aceita pelo AP, a estação deve responder o SSID (Service Set Identifier) com uma *string* vazia (nula).

O SSID é um identificador da rede. Sem ele os clientes não conseguem se conectar a rede.

- **Sistema de Autenticação Fechado (Closed System):** para ser autenticado pelo AP, precisa informar o SSID correto da rede.

O outro método de autenticação, conhecido como Shared Key (Chave Compartilhada), utiliza um mecanismo de criptografia. A Figura 6 ilustra o funcionamento deste método de autenticação: [8]

Figura 6 – Autenticação com o método Shared Key.

Na autenticação shared key o AP autentica o cliente, mas o cliente não tem a garantia da autenticação no AP desejado.

2.10.TIPOS DE FRAMES

Os *frames* utilizados entre o NIC e o AP são compostos por um campo de controle, que contém a versão do protocolo 802.11b, tipo do *frame* e vários outros indicadores. Tem também o endereço MAC do emissor e do destino, um número seqüencial, o corpo e uma seqüência de verificação (presença de erros).

2.10.1. Frames de Gerenciamento

Para que os dispositivos *wireless* estabeleçam e sustentem as suas conexões, existem os *frames* de gerenciamento. Os principais *frames* estão representados abaixo: [4]

- **Frames de Autenticação (Authentication Frame):** é usado na autenticação de um cliente.

- **Deauthentication Frame**: é usado para encerrar a comunicação de uma forma segura.

- **Frame de Pedido de Associação (Association Request Frame):** é usado para que o AP reserve recursos e sincronize com o NIC do cliente, no processo de associação.

- **Frame de Resposta de Associação (Association Response Frame):** é usado para que o AP envie a resposta da solicitação contendo informações de ID da associação e as taxas de transferência suportadas.

- **Frame de Pedido de Re-associação (Reassociation Request Frame):** é usado quando o cliente realiza um *handoff*. O NIC *wireless* envia um pedido de re-associação a este outro AP.

- **Frame de Resposta de Reassociação (Reassociation Response Frame):** contém a resposta do pedido (aceitação ou rejeição).

- **Frame de Desassociação (Disassociation Frame):** é usado quando se deseja terminar uma associação. O AP remove o NIC da tabela de associação e libera a memória alocada pelo dispositivo.

- **Beacon Frame:** o AP envia periodicamente para divulgar a sua presença e transmitir informações contendo o SSID. Os NICs realizam varreduras nos canais de transmissão para receber *beacons* e determinar qual é o melhor AP para se associar.

- **Frame de Pedido de Investigação (Probe Resquest Frame):** é usado quando necessário obter informações de outros dispositivos da WLAN.

- **Frame de Resposta de Investigação (Probe Response Frame):** contém a resposta de um *probe request*.

2.10.2. Frames de Controle

Os *frames* de controle auxiliam a entrega dos *frames* de dados. Temos três tipos:

- Request to Send frame (RTS): O RTS/CTS (Figura 7), tem como função reduzir as colisões de *frames* dos dispositivos associados no mesmo AP. Para enviar um *frame* de dados, o primeiro passo é enviar um *frame* RTS.

- Clear to Send frame (CTS): indica que o dispositivo pode enviar o seu *frame* sem causar colisões. É a resposta para um RTS.

- Acknowledgement frame (ACK): sempre que um dispositivo recebe um *frame* de dados, utiliza-se de um processo chamado *error checking*. Se o dispositivo recebe um *frame* sem

erros, envia um *frame* ACK para o dispositivo emissor. Se o emissor não receber o *frame* de ACK, ocorrerá uma retransmissão automaticamente. [9]

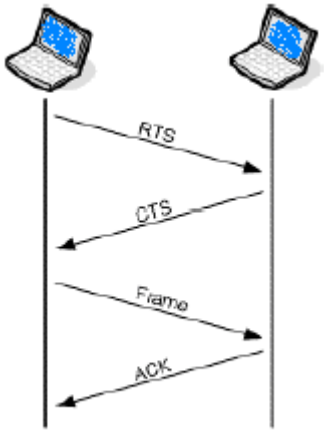

Figura 7 – Mecanismo RTS/CTS.

2.10.3. Frames de Dados

Constituído pelos pacotes de camadas mais altas, são os principais tipos de *frame* existente no padrão 802.11b. Ex: Uma página WEB.

2.11.FRAGMENTAÇÃO

Esta operação consiste em dividir os *frames* que deseja transmitir em pequenas partes, os quais são enviados separadamente até o seu destino final. Cada fragmento de um *frame* é composto de um cabeçalho MAC, de uma seqüência de verificação (FCS) e de um número indicando a posição deste fragmento (ordem da posição na transmissão). É importante salientar que a fragmentação é utilizada somente em *frames unicast* (com apenas um destino). [4]

3. PROTOCOLO WEP

WEP é um protocolo de segurança de redes *wireless*, desenvolvido para garantir autenticidade e confidencialidade nos serviços oferecidos pelas redes 802.11b. O objetivo do WEP é fornecer um controle de acesso à rede. Na rede *wireless* não existem pontos de acesso fixos, mas sim uma área de abrangência e basta que um usuário esteja dentro desta área para obter acesso.

Baseado no uso de criptografia de chaves simétricas, o 802.11b define um mecanismo para criptografar o conteúdo dos *frames* de dados, contendo alguns elementos: [10]

- É um segredo compartilhado entre todos os membros do BSS;
- Um algoritmo XOR (*Extended OR*) para criptografrar e descriptografar cada *frame*.
- Um algoritmo RC4 para gerar a chave. O RC4 é um algoritmo de fluxo criado em 1987.
- Um VI (Vetor de Inicialização) de 24 bits. O VI é utilizado como entrada para o RC4 para a geração das chaves.

3.1. FUNCIONAMENTO

Se o WEP estiver ativo, o NIC irá criptografar o *payload* (carga do pacote) de cada *frame* antes de enviá-lo para outro dispositivo. Quando chegar até o dispositivo receptor, será descriptografado. Caso ocorra de um *frame* passar de uma rede *wireless* para uma rede cabeada, o mesmo não mais estará protegido pelo WEP, pois o WEP só criptografa dados entre estações com o padrão 802.11b. A Figura 8 ilustra o funcionamento do WEP: [2]

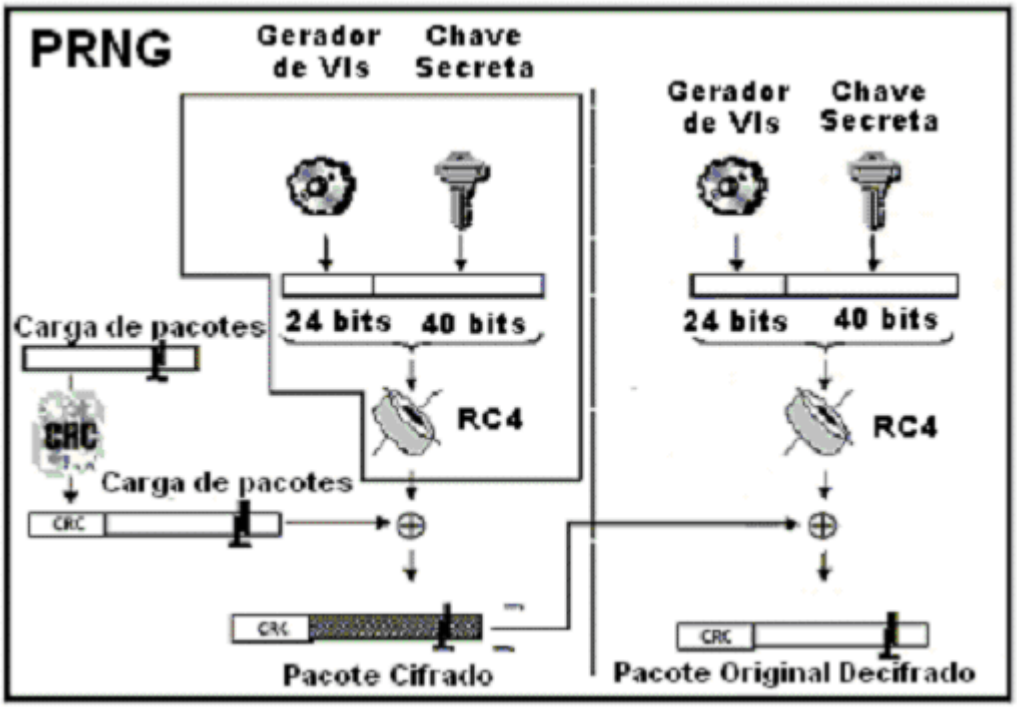

Figura 8 - Esquema do Funcionamento do WEP.

Cada *frame* tem um vetor de inicialização (VI) de 24 bits gerado aleatoriamente e através da concatenação do segredo compartilhado fornecido pelo usuário, o protocolo WEP realiza um *seed* ou semente (agendamento de chaves). O VI tem como objetivo evitar que todos os *frames* tenham a mesma chave de criptografia. O WEP usa o VI agregado ao segredo como entrada para o gerador de números pseudo-aleatórios (PRNG) do RC4, assim, cria uma chave cujo tamanho é igual aos dados a serem criptografados.

Com a chave gerada no passo anterior, o *payload* do *frame* somado com mais 32 bits que é utilizado para detecção de erro (CRC), é criptografado através de uma operação XOR. O transmissor e o receptor devem conhecer a mesma chave, uma vez que a criptografia e a descriptografia utilizam a mesma chave. O VI é transmitido no cabeçalho de cada *frame* criptografado, sendo que cada *frame* tem o seu VI gerado aleatoriamente. Os principais problemas de segurança relacionados ao WEP, que serão discutidos adiante, surgem disso.

3.2. UTILIZAÇÃO DO WEP

O WEP utiliza uma chave secreta compartilhada, de tamanho variável (varia de acordo com fabricante), para que seja possível criptografrar os dados na camada de link de dados. [10]

Dois parâmetros servem de entrada para o algoritmo RC4: a chave secreta de 40 bits ou 104 bits e um vetor de inicialização de 24 bits. A partir desses dois parâmetros, o algoritmo gera uma seqüência criptografada RC4.

Abaixo, encontram-se algumas falhas de implementação do WEP que o tornam suscetíveis a ataques:

- **Utilização de chaves estáticas:** compartilhar a mesma chave por um longo intervalo de tempo entre diversos usuários, representa uma falha de segurança. Isto ocorre devido à falta de um gerenciador de chaves no protocolo WEP.

- **Envio do Vetor de inicialização (VI) na parte não cifrada da mensagem:** a *string* de 24 bits gerada pelo RC4 é pequena quando usada para criptografia. Essa *string* é utilizada na inicialização da *key stream* gerada. A reutilização de um VI, produzirá *key streams* idênticas para proteger os dados. Os atacantes podem capturar o tráfego da rede quando o VI é pequeno, pois eles repetirão após um curto intervalo de tempo. Após capturar o trafego, basta descobrir o *key stream* e utiliza-lá para descobrir o texto cifrado.

- **VI faz parte da chave de criptografia:** a fraqueza do agendamento de chaves RC4 associado o fato de um intruso conhecer 24 bits de cada chave existente no pacote, resulta em um perigo de ataque, pois recupera a chave, após interceptar e analisar uma porção do tráfego.

3.3. VULNERABILIDADES E SOLUÇÕES

O anonimato que a rede *wireless* proporciona, é uma das maiores diferenças entre uma rede cabeada e uma *wireless*. As áreas de cobertura são desprotegidas fisicamente. As redes *wireless* são mais vulneráveis e assim possibilita aos invasores realizarem ataque de forma rápida e fácil. As redes *wireless* herdam as vulnerabilidades já existentes nas redes cabeada, assim, sendo passíveis dos mesmos ataques (ARP e DNS spoofing, DoS, etc). [11]

Para amenizar as vulnerabilidades existentes nas redes *wireless*, exitem alguma técnicas e ferramentas. As soluções que serão apresentadas não resolvem por completo os problemas, mas servem para aumentar a segurança de uma WLAN.

O Open System (usuário não precisa de autenticação para acessar a rede) está presente em alguns equipamentos comercializados, visto que é o modo de autenticação padrão. O *shared key* é aconselhado como método de autenticação, apesar de não ser muito confiável. Desta forma, tem-se um nível mínimo de segurança.

Todos equipamentos contêm uma senha para efetuar configurações necessárias. A senha padrão do fabricante nos APs comercializados é um problema comum de segurança, visto que essas senhas são padrões para diversos equipamentos.

O SSID padrão é um outro problema existente. Um usuário deve conhecer o SSID correto para se conectar em uma rede *wireless*, visto que é uma espécie de nome da rede. Semelhante ao problema das senhas padrão, os fabricantes configuram os equipamentos com SSIDs padrões e em algumas vezes deixam até desabilitado.

A definição do *broadcast* de *beacon frames* pelo AP, com a finalidade de anunciar as configurações que ele suporta e que este AP está disponível, fazem parte da especificação do 802.11 da IEEE. Definidos pelo administrador da WLAN ou pelo fabricante do aparelho, os *beacons frames* são enviados em intervalos regulares. O objetivo deste *broadcast* é que os usuários possam diferenciar os APs quando estão em areas que tenham diversos APs em funcionamento.

Identificar o SSID dentro de WLANs em que o AP faz *broadcast* do SSID para qualquer cliente, dentro da área de cobertura é possível através de alguns passos;

Segue abaixo, alguns passos para identificar o SSID;

1. Dentro da área de cobertura da rede, o NIC *wireless* identifica o SSID automaticamente;

2. Através de ferramentas que possibilitam a identificação da faixa de IP, *gateway* e o servidor DNS da rede, deve-se obter esses dados;

3. Reconfigurar a interface *wireless*. Neste ponto o usuário já estará autenticado e associado na WLAN;

Quando o AP não está configurado para transmitir o SSID, a dificuldade é maior, porém, ainda é possível descobrir o SSID e conseqüentemente, penetrar na rede.

1. Como o AP envia pacotes do tipo probe request/response, para os outros APs, deve-se capturar estes pacotes através de um software específico, assim é possível obter o SSID, mesmo que ele tenha sido desativado nos *beacons frame*.

2. Configurar a interface com o SSID obtido.

3. Descobrir um IP não utilizado;

4. Com as informações obtidas, reconfigurar a interface *wireless*.

Conclui-se que mesmo que seja alterado o SSID padrão ou desabilitado o *broadcast*, um atacante pode obter o SSID através do uso de alguma técnica ou ferramenta apropriada.

3.4. ALGORITMO RC4

Um algoritmo é uma transformação matemática. Ele converte uma mensagem não cifrada em uma mensagem cifrada e vice-versa. Mais utilizado em aplicações que necessitam de criptografia dos dados, sendo otimizado especificamente para implementação rápida em software [12]. O RC4 é definido com um algoritmo de fluxo, pois é simétrico (usa a mesma chave para criptografar e descriptografar) e cifra um fluxo continuo de bits na comunicação de dados. A chave pode ter tamanhos de até 2048 bits. [13]

3.5. ALGORITMO XOR

XOR ou OU exclusivo, é um operador binário que compara dois bits, e então retorna 1 se os dois bits forem diferentes, ou 0 se eles forem iguais.

3.6. ENDEREÇO MAC

Um endereço de hardware composto por 48 bits permite identificar cada equipamento conectado a uma rede. Este endereço é chamado de MAC (Medium Access Control). O endereço MAC é atribuído na etapa de fabricação, pelo próprio fabricante. [1]

O recurso de restringir o acesso baseado em ACLs (Access Control List) por endereços MAC consultando uma lista com todos os MACs. Disponível em alguns APs comercializados.

Uma estação utiliza o formato clear text para transmitir o endereço MAC para o AP. Desta forma, capturando o tráfego da rede o MAC pode ser obtido. Realizando *spoofing* de endereços MAC, é possível modifica-ló manualmente. Seguindo os passos abaixo, seria possível invadir a rede se o filtro de MAC estiver habilitado:

1. Descobrir o SSID;

2. Devido ao fato de poder existir dois endereços MAC iguais na mesma rede, basta descobrir um endereço MAC de algum cliente que esteja associado;

3. Atribuir o MAC;

Um nível de segurança razoável é obtido através do controle de acesso baseado em endereços MAC, mas deve ser utilizado em conjunto com outras precauções. Existem ferramentas que auxiliam no processo de gerenciamento de listas de endereços MAC, assim, quando um MAC desconhecido é detectado, um alerta é enviado ao administrador.

3.7. FERRAMENTAS

3.7.1. Scanning

A exposição da rede a usuários anônimos é um dos maiores problemas das redes *wireless*. Sem que os administradores percebam a sua presença, o atacante pode interceptar os sinais transmitidos e capturar o tráfego da rede. Este ataque é difícil de ser prevenido e detectado.

Vem se tornando uma atividade muito comum a prática de *scanning* nas redes. A área de abrangência da rede, limita a ação dos atacantes. O uso de antenas e amplificadores de sinais auxiliam os atacantes a aumentar esta área. Para que o ataque seja bem sucedido, a captura do tráfego de uma rede é um dos primeiros passos para o atacante (obtém informações como usuários, senhas, equipamentos). Após serem obtidas todas estas informações, o atacante pode parar o scanning e partir para o ataque da WLAN. [14]

3.7.2. Wardriving

O *wardriving* consiste em sair de carro pelas ruas, equipado com um *notebook* com suporte a dispositivos *wireless* em busca de WLANs desprotegidas. [11]

Na medida em que as pessoas vão coletando informações das redes *wireless*, conforme Figura 9, algumas delas constroem mapas para facilitar a visualização dos pontos encontrados com o auxílio de GPS (Global Positioning Site).

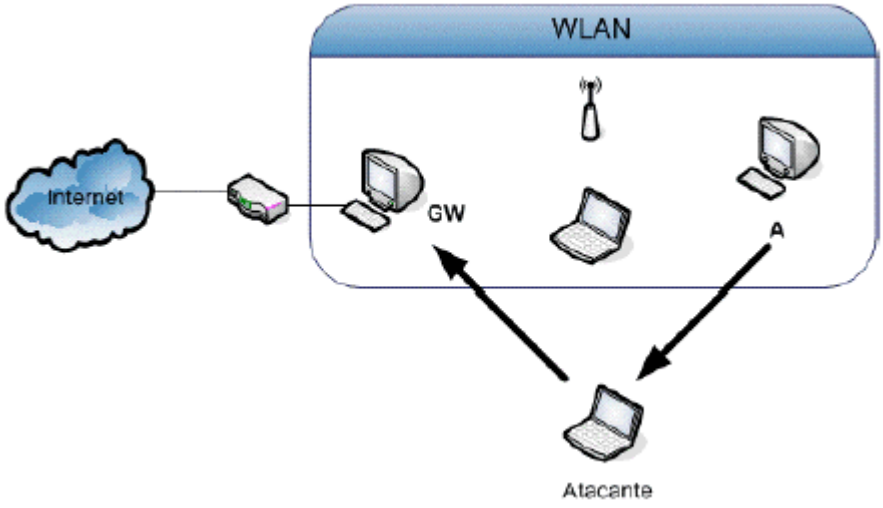

Figura 9 – Ataque em trânsito

3.8. ARP

Integrante do protocolo TCP/IP, é utilizada pelos atacantes como meio de vasculhar os pacotes de uma rede com equipamentos do tipo *switch*. O ARP (Address Resolution Protocol) é conhecido também como MAC Spoofing ou ARP Poisoning. É realizado na camada de enlace de dados. O ARP é um protocolo para que máquinas de uma rede localizem outros *hosts*. Desta foma, realizando um *broadcast* de um pacote ARP e aguardando a resposta da máquina detentora do IP e endereço MAC solicitado, um endereço IP especifico é facilmente identificado.

3.9. VPN

As VPNs (Virtual Private Network) foram criadas para oferecer um conexão segura e privada através de uma rede pública (como a Internet) e foram adaptados para proporcionar comunicações super seguras em uma LAN sem fios. VPNs de LANs sem fios incorporam criptografia e autenticação mútua em um único sistema. São geralmente descritas como “túneis ” seguros através dos quais o tráfego de rede pode viajar sem perigo de intercepção. Os dados que estiverem dentro do túnel VPN são criptografados e isolados do restante do tráfego da rede. Existem três usos para a VPN: acesso remoto, conectividade entre LAN (site-to-site) e *extranets*. [1]

O protocolo IPsec é utilizado na maioria das VPNs para constituir um canal seguro. Confidencialidade e integridade das conexões é fornecida pelo IPsec. O protocolo IPsec tem como sua principal tarefa fazer o roteamento das mensagens por um túnel cifrado, inserindo dois cabeçalhos especiais, após o cabeçalho IP de cada mensagem. Um exemplo do IPsec em redes *wireless* está ilustrado na Figura 10. Neste exemplo, através de um túnel seguro, a comunicação entre o cliente e o AP é realizada.

É possível o uso de protocolos IPsec e WEP em conjunto, pois são independentes.

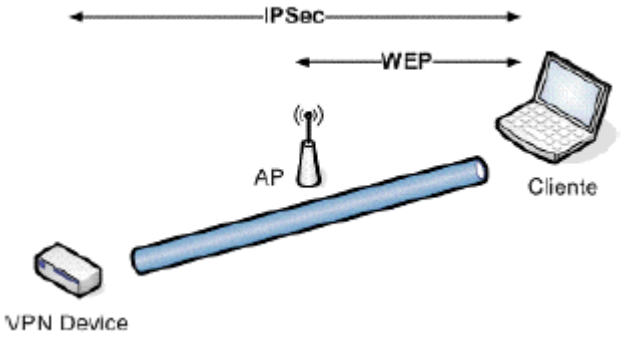

Figura 10 - VPN e WEP em conjunto.

O uso de VPN está presente em outro exemplo na Figura 11. Através de um *gateway* VPN , clientes conseguem efetuar conexões seguras (com o IPsec). O *gateway* VPN tem como opção ter um *firewall* para filtrar e restringir o tráfego da rede.

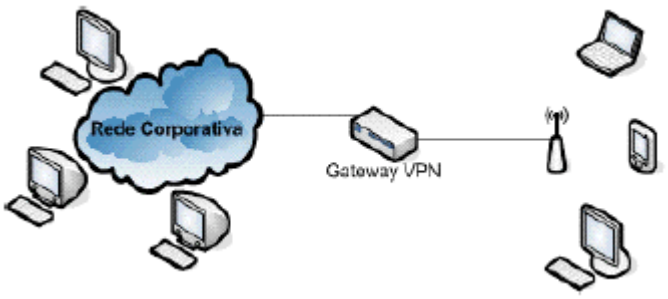

Figura 11 - WLAN com VPN.

O uso de VPN previne a coleta do tráfego da rede interna. Um exemplo disto é o ataque de ARP *spoofing*, pois não consegue atingir a rede interna devido o *gateway* VPN atuar roteando pacotes IP e não *frames* da camada de enlace.

CONCLUSÕES

Este trabalho envolveu o estudo de protocolos, comportamentos ofensivos em redes e o uso de ferramentas para "burlar" a segurança. A segurança de qualquer sistema não depende somente do algoritmo de criptografia empregado, mas também de diversas outras variáveis, como por exemplo, o controle de acesso ao recinto, proteção física dos equipamentos, políticas de segurança rígidas dentro da empresa, entre outras. A tecnologia *wireless* apresenta-se como uma nova tendência no mercado de redes, visto que proporciona uma grande mobilidade aos computadores, além de ser facilmente instalada. O padrão 802.11b faz uso do protocolo WEP, o qual utiliza uma chave secreta compartilhada de tamanho variável, que foi desenvolvido para garantir uma segurança mínima às redes *wireless*. Porém, devido às falhas de implementação e definição, o WEP não cumpre a sua tarefa, deixando muito a desejar no quesito de proteção para as redes *wireless*. Verificou-se que a criptografia fornecida pelo WEP é facilmente quebrada, utilizando ferramentas de conhecimento público disponíveis na Internet. Além do WEP, existem outros mecanismos que se propõem a aumentar a segurança das WLANs, como é o caso do filtro de MAC. Porém, todos mecanismos apresentaram alguma deficiência, com exceção da tecnologia VPN, que se mostrou muito robusta, apesar do impacto negativo no desempenho da rede. Com base nos estudos realizados, conclui-se que não existe uma solução única para garantir a segurança da WLAN. Contudo, no presente momento, a melhor alternativa ainda é usar todo o conjunto de mecanismos disponíveis, na tentativa de construir uma segurança em profundidade.

Portanto, é de extrema importância e relevante a realização de pesquisas visando o desenvolvimento de mecanismos de controle mais eficientes para as redes *wireless*, tecnologia esta que cada vez mais está sendo utilizada para os mais diversos fins.

CONTRIBUIÇÕES E EXTENSÕES

Este trabalho contribuiu apresentando o padrão 802.11b e o uso do protocolo WEP para implementação das características básicas de segurança.

Pode ser continuado através de um estudo do protocolo WPA e sua comparação com o WEP

REFERÊNCIAS BIBLIOGRÁFICAS

[1] KARYGIANNIS, Tom; OWEWS, Les; Special Publication 80-48: "DRAFT – Wireless Network Security 82.11 – Bluetooth an Handheld Devices". Disponível em http://csrc.nist.org/publications/draft.html. Acesso em 28 aug. 2005

[2] CARNUT, Marco; "Segurança em Redes Wireless 802.11b. Ataques e defesas". Disponível em: http:/www.tempest.com.br. Acesso em: 10 out 2005.

[3] MATHIAS, Andre Pimenta; TABACH, Jack Josef; IEEE 802.11: Redes Wireless. Disponível em http://www.gta.ufrj.br/~rezende/cursos/ee1879/trabalhos2003. Acesso em 13 nov. 2005

[4] GEIER, Jim. "2.4 GHz vs. 5GHz. Deployment Considerations". Disponível em: http://www.80211-planet.com/tutorials/article.php/1569271. Acesso em 2 out. 2005.

[5] ARBAUGH, Willian A; SHANKAR, Narendar; WAN, Y. C. Justin; "Your 802.11 Wireless Network has no Clothes". Disponível em: http://www.cs.umd.edu/waa/wireless.pdf. Acesso em: 3 nov. 2005.

[6] MACAULAY, Tyson; "Hardening IEEE 802.11 Wireless Networks". Disponível em http://www.e-secure_db.us/dscgi/dspy/view/collection-903. Acesso em 07 set. 2005

[7] MARIANO, Antonio; "Wireless Networks". Disponível em http://www.enterasy.com.br/products/whitepapers/wp-wireless-network.html Acesso em 13 set. 2005

[8] MARTINS, Marcelo; "Protegendo Redes Wireless 802.11b" Disponível em http://www.modulo.com.br Acesso em 29 aug 2005

[9] GAST, Mathew; "802.11 Wireless Networks". The Definitive Guide. O'Reilly & Associates, 2002.

[10] WALKER, Jesse R; Unsafe at many key size. An analysis of the WEP encapsulation. Disponível em http://grouper.ieee.org/groups/802/11/documents Acesso em 15 set. 2005

[11] FLECK, Bob; POTTER, "Bruce; 802.11 Security". O'Reilly & Associates, 2002.

[12] SCHNEIER, Bruce. "Applied Criptography – Protocols, Algorithms and Source Code in C. 2". New York. John Wiley & Sons, 1995

[13] RIVEST, Ruan; "RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4", RSA Data Security, Inc., Disponível em http://www.rsasecurity.com/rsalabs/technotes/wep.html Acesso em 01 nov. 2005

[14] MAXIUM, Merrit; POLLINO, David; "Wireless Security". Mc Graw-Hill Companies. 2002