CENTRO UNIVERSITÁRIO FEEVALE

FELIPE LUCCHESE

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

Novo Hamburgo, junho 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, junho 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 é concebido; 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 e, além disso, criar uma relação de comparabilidade entre estes protocolos. Ainda neste, descreve-se o *wardriving*, relatando seus propósitos e suas origens, ressaltando a questão legal e ética desta prática.

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. In addition to describe the wardriving, relating its purposes and its origins, emphasizing the legal and ethical questions of this practice.

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
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
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
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
OFDM	Orthogonal Frequency Division Multiplexing/Modulation
OSI	Open Systems Interconnection
PAP	Password Authentication Protocol
PDA	Personal Digital Assistan
PEAP	Protected EAP
PMK	Pairwise Master Key
PRNG	Pseudo Random Number Generator
PSK	Preshared Key
PTK	Pairwise Temporal Keys
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher version 4
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
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
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 *Wireless* (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 é 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], 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 operam nas faixas de freqüência de 2,4GHz ou 5GHz, 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 refere ao uso dessas redes em locais fechados (com pouco alcance) e aplicações *outdoor*, que se refere ao uso dessas redes em locais abertos (com superior alcance).

O transporte de dados através de uma rede *wireless* envolve três elementos: o meio físico 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 transmitidos através de ondas. 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 *wireless* (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 w*i-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. 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).

Sendo assim, o presente trabalho tem como objetivo abordar as questões técnicas sobre as redes *wi-fi*, apresentando os principais componentes destas e suas características. Após isso, descrever os protocolos de segurança e criptografia WEP e WPA, analisando suas estruturas, características e funcionamento e apresentar 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 e, além disso, criar uma relação de comparabilidade entre estes protocolos. Ainda neste, pretende-se descrever o *wardriving*, relatando seus propósitos e suas origens, ressaltando a questão legal e ética desta prática.

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.

Este trabalho está dividido em três 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 as redes *wi-fi*, 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. Por fim,

no capítulo três, são abordadas as características a respeito do *wardriving*, demonstrando os princípios e implicações legais deste modelo de mapeamento de pontos de acesso.

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:

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.

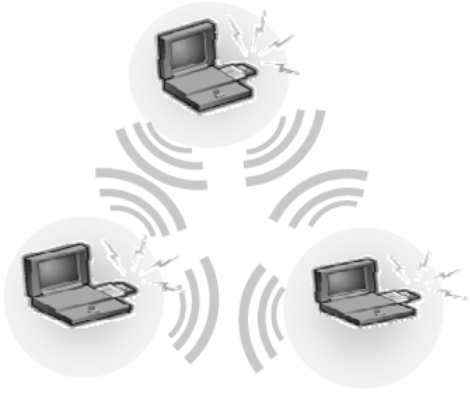

Figura 1.1 - Estrutura de rede Ad-Hoc (IBSS).
Fonte: http://www.babooforum.com.br.

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.

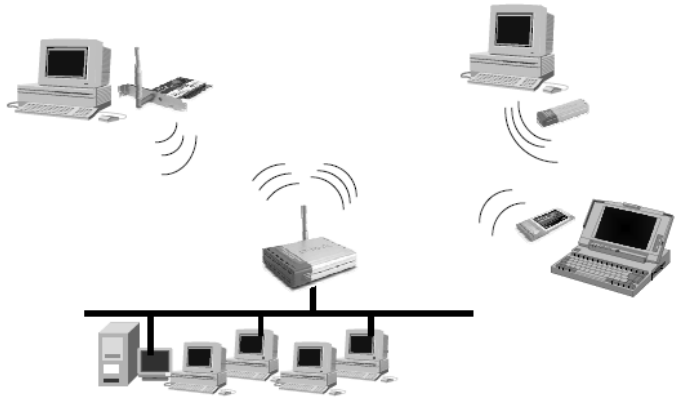

Figura 1.2 - Estrutura de rede BSS.
Fonte: http://www.babooforum.com.br.

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

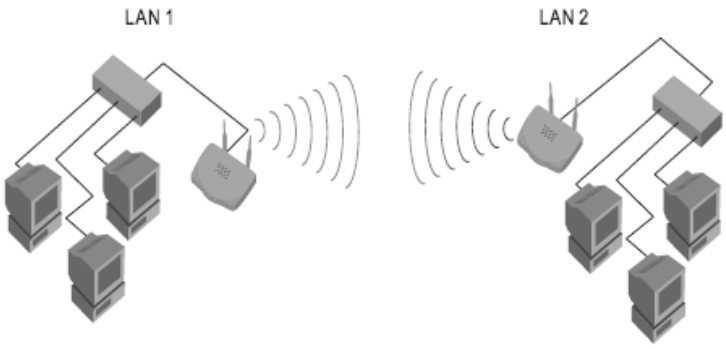

Figura 1.3 - Estrutura de rede ESS.
Fonte: http://www.babooforum.com.br.

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	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. 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 suas subdivisões) 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.

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. 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 *wireless*, 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.

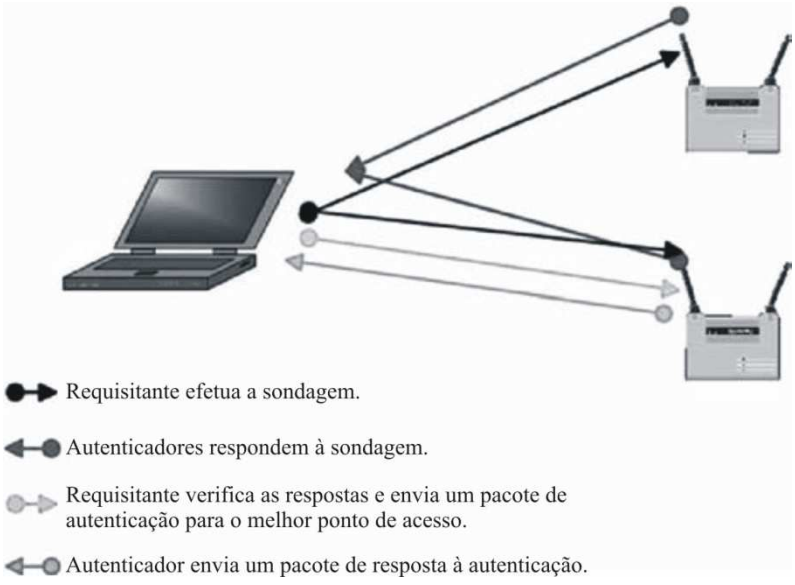

Figura 1.4 - *Open Key Authentication.*
Fonte: EARLE (2006, p.186).

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 *wireless* 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.

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*)

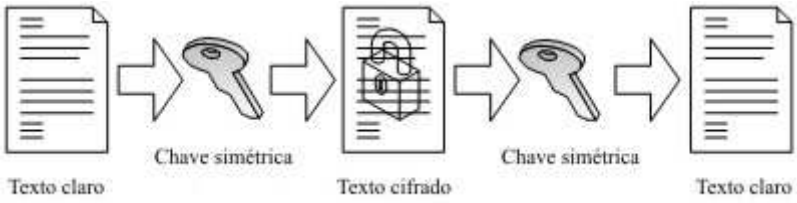

Figura 1.6 - Criptografia Simétrica.
Fonte: http://www.microsoft.com.

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.

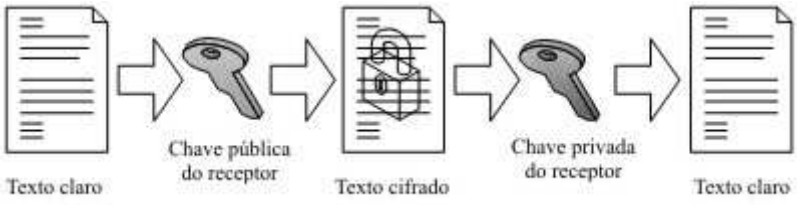

Figura 1.7 - Criptografia Assimétrica.
Fonte: http://www.microsoft.com.

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 ruído 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.

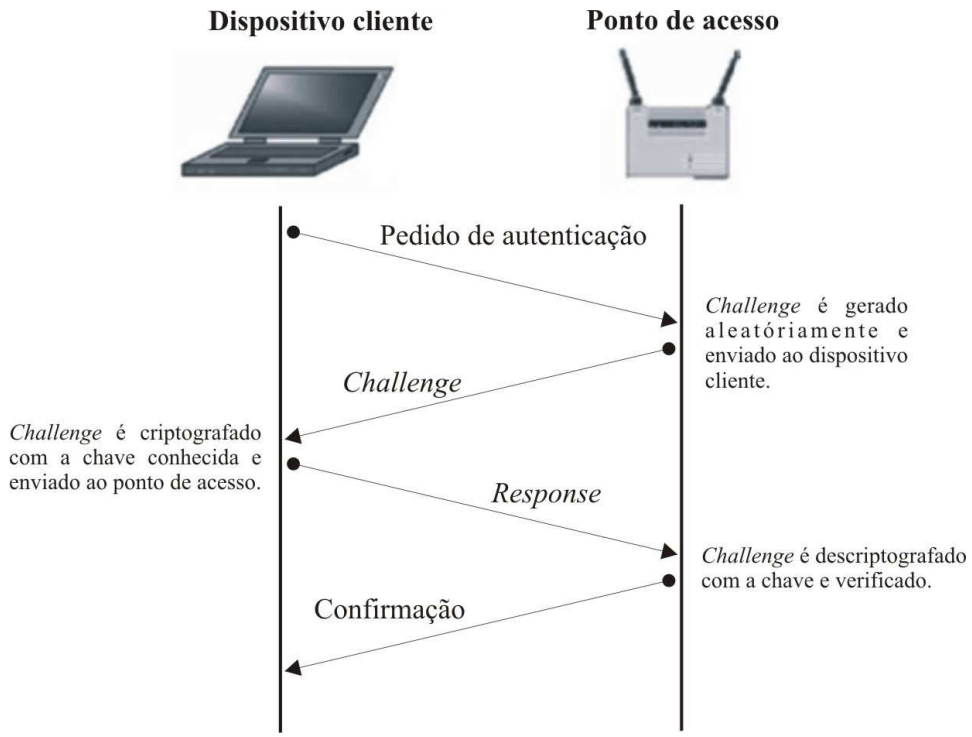

Figura 2.1 - Autenticação *shared key* utilizando WEP.

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). Apartir 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.

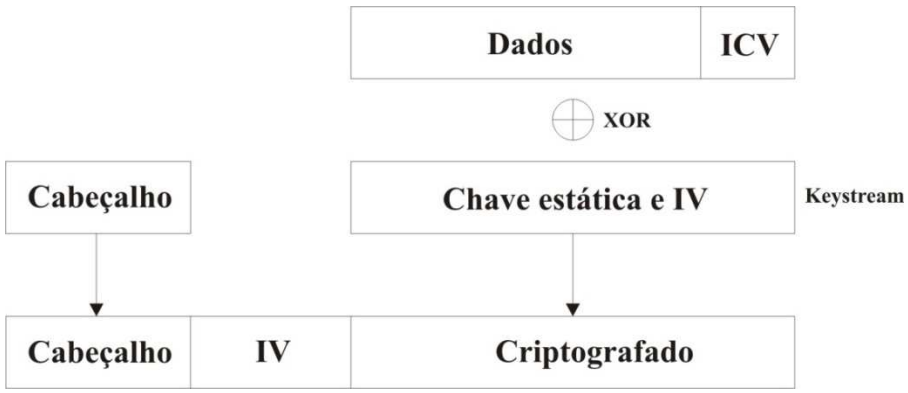

Figura 2.2 - Detalhamento do processo WEP.
Fonte: EARLE (2006, p.190).

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.

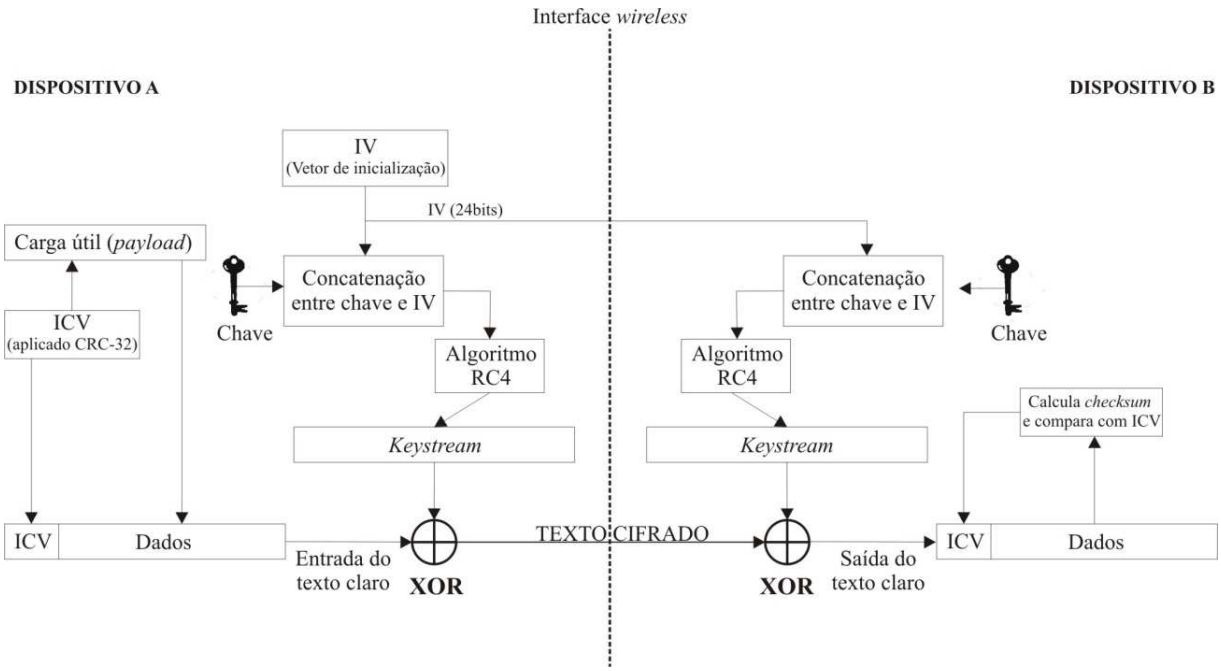

Figura 2.3 - Esquema de cifragem, transmissão e decifragem utilizando WEP.

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.

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. Detalhes acerca destes serão abordados na segunda parte do presente trabalho (TC2).

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*). 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.

[5] *Microsoft Corporation*. Disponível em http://www.microsoft.com.

- 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.

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

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

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.

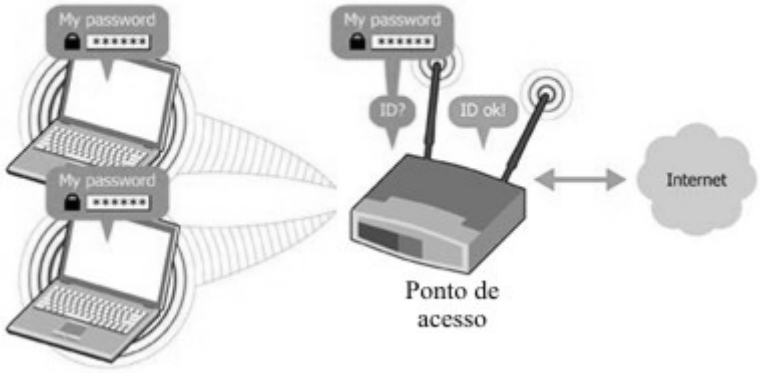

Figura 2.5 - Autenticação utilizando WPA-PSK.
Fonte: WPA (2003, p.6).

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*.

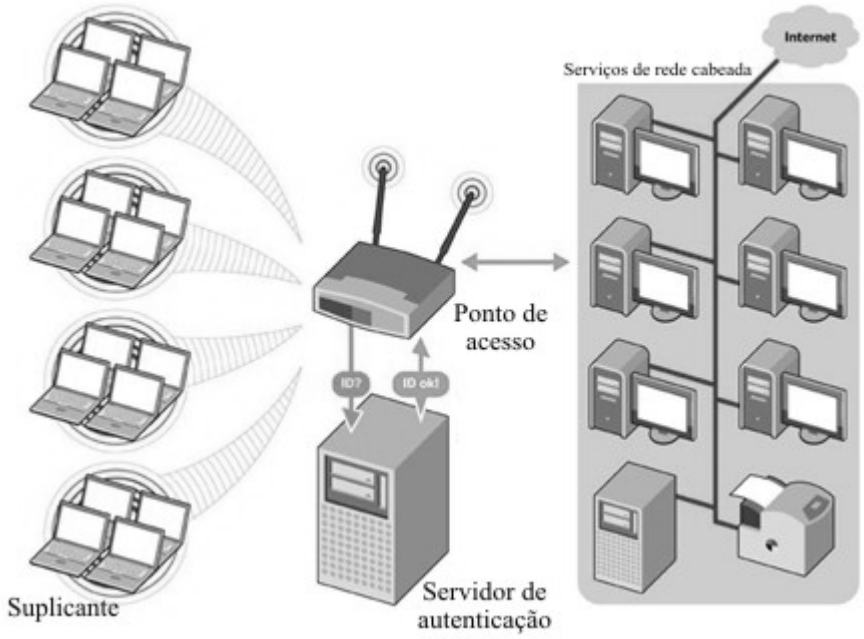

Figura 2.6 - Autenticação WPA-*Enterprise*.
Fonte: WPA (2003, p.5).

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).

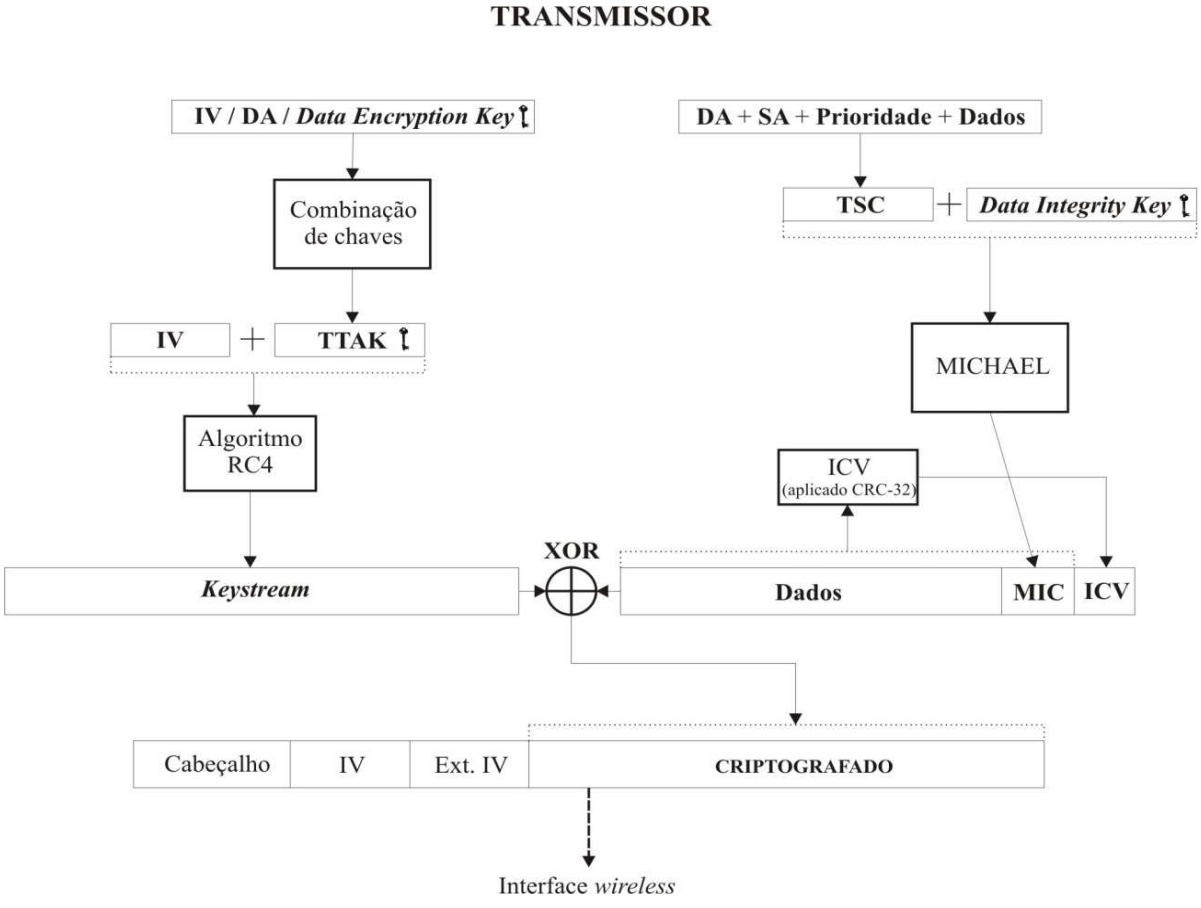

Figura 2.7 - Esquema de criptografia e integridade do WPA (Transmissor).

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).

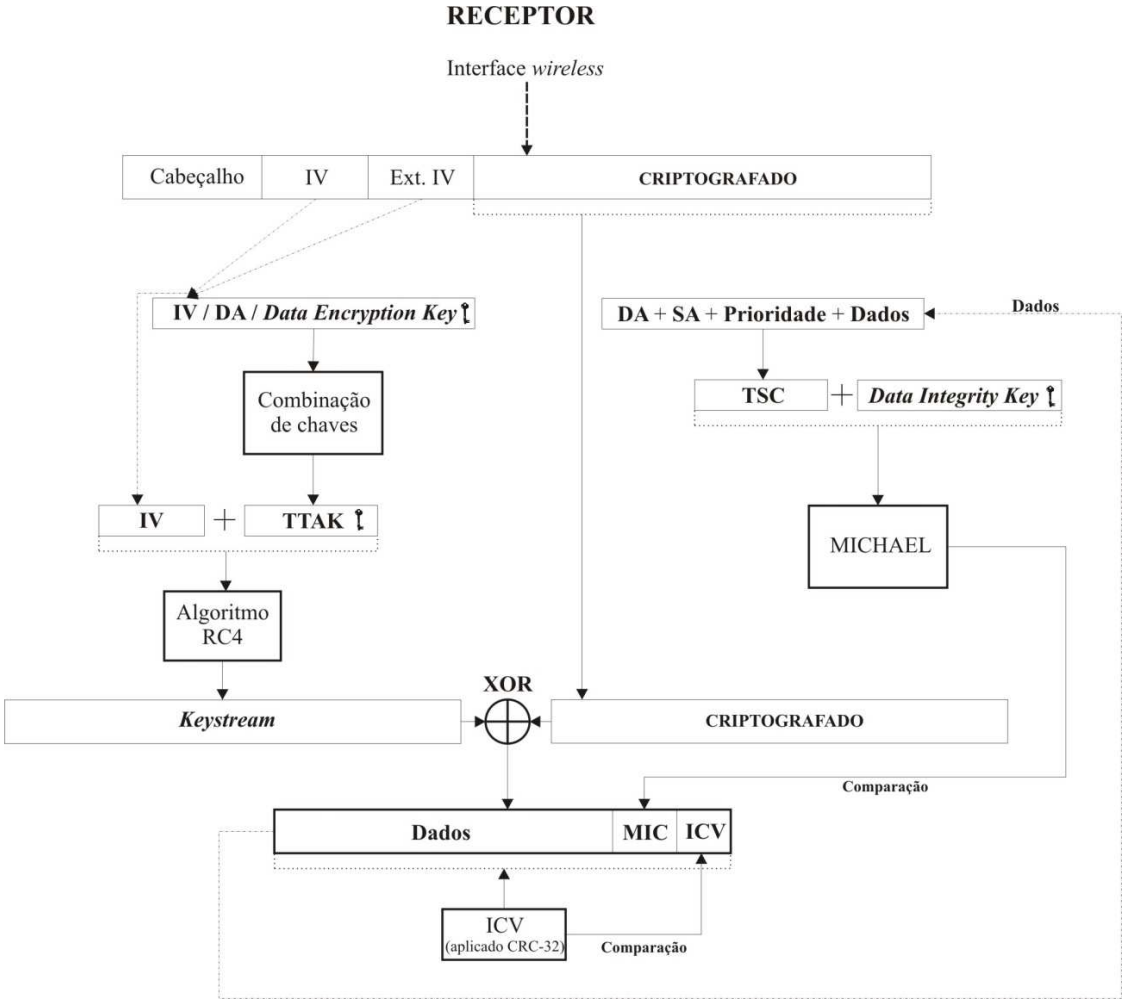

Figura 2.8 - Esquema de criptografia e integridade do WPA (Receptor).

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 minuto, 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 muito 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,

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

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.

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 em 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 objetivo 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. A 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, Chris *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 modens 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 California (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*.

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).

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.

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:

- 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*, utilizando *laptop* e GPS.
Fonte: HURLEY, Chris *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 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.

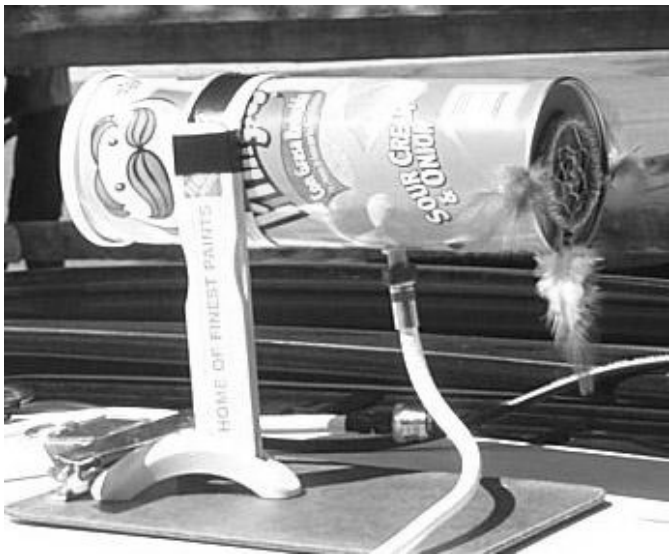

Figura 3.2 - Antena caseira.
Fonte: HURLEY, Chris *et al* (2004, p.58).

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. E 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. Para que haja um resultado satisfatório na utilização do *wardriving*, é imprescindível a utilização de um conjunto de *softwares* de qualidade.

Uma análise aprofundada sobre as técnicas utilizadas para *wardriving*, bem como seus métodos (*softwares*, *hardwares*, etc.), será realizada na segunda parte do presente trabalho (TC2).

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 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.

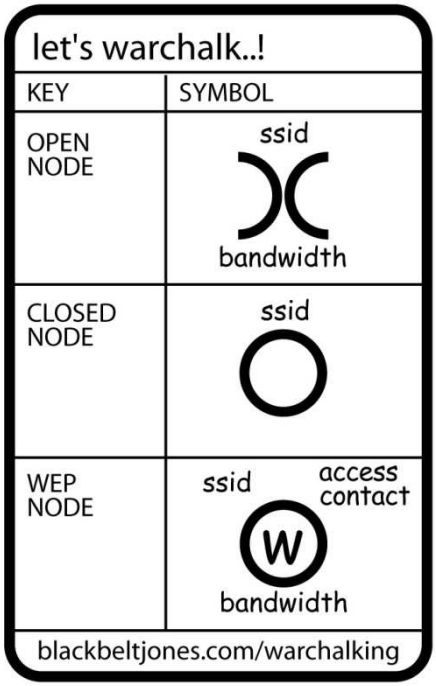

Figura 3.3 - Simbologia utilizada no *Warchalking*.
Fonte: http://www.warchalking.org.

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.

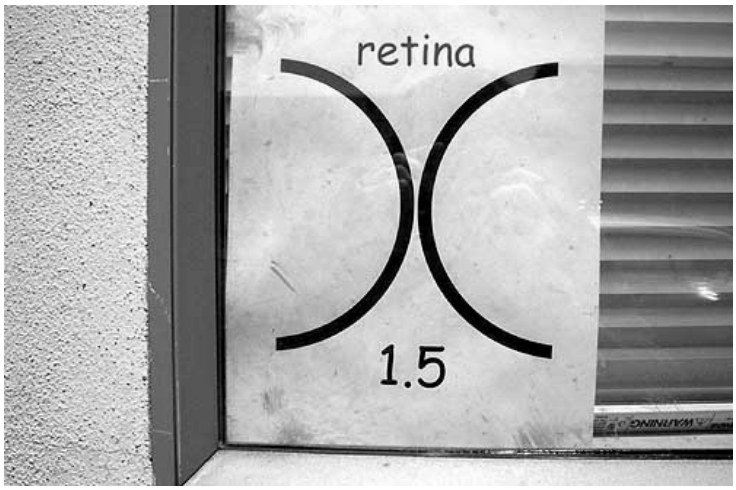

Figura 3.4 - Identificação de rede aberta.
Fonte: http://www.wired.com.

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, 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. 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. O *wardriving* é amplamente utilizado por especialistas em segurança de redes para teste e verificação de vulnerabilidades.

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.

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 à 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. 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. A respeito do padrão WPA2, observa-se uma estrutura de segurança muito mais robusta, incrementando diversas tecnologias que prometem manter a segurança da rede *wi-fi*, 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*).

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.

Na segunda parte deste trabalho, será abordado um estudo acerca dos métodos de *wardriving*, utilizando estes para realizar efetivamente o mapeamento de pontos de acesso. Será desenvolvida uma metodologia específica para esse fim, abordando as questões de segurança reportadas e relacionadas ao *wardriving*, a fim de detectar as principais vulnerabilidades de segurança em redes *wi-fi* (um cenário de *hardware* + *software versus* vulnerabilidades). A busca e o mapeamento de pontos de acesso *wi-fi* ocorrerão na cidade de Farroupilha, no Rio Grande do Sul, em áreas a serem definidas posteriormente.

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.

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.

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.

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

HURLEY, Chris et al. 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.

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.

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.

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.