

GILSON MARQUES DA SILVA

SEGURANÇA EM REDES LOCAIS SEM FIO

Dissertação apresentada ao programa de pós-graduação em ciência da computação da Universidade Federal de Uberlândia, como requisito parcial para a obtenção do título de mestre em ciência da computação.

Orientador: Prof. Dr. João Nunes de Souza, da Universidade Federal de Uberlândia.

UBERLÂNDIA – MG

2005

S586s Silva, Gilson Marques da.
Segurança em redes locais sem fio / Gilson Marques da Silva. -
Uberlândia, 2005.
123f. : il.
Orientador: João Nunes de Souza.
Dissertação (mestrado) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Ciência da Computação.
Inclui bibliografia.
1. Redes de computação - Medidas de segurança - Teses. I. Souza, João Nunes de. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Ciência da Computação. III. Título.

CDU: 681.3-78 (043.3)

Gilson Marques Da Silva

SEGURANÇA EM REDES LOCAIS SEM FIO

Dissertação apresentada ao programa de pós-graduação em ciência da computação da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de mestre em ciência da computação.

Banca examinadora:

Uberlândia, 03 de junho de 2005.

Prof. Dr. João Nunes de Souza – Orientador – UFU

Prof. Dr. Júlio Cesar López Hernández – UNICAMP

Prof. Dr. Luís Fernando Faina – UFU

Prof. Dr. Ilmério Reis da Silva – UFU

AGRADECIMENTOS

À Universidade Federal de Uberlândia, em especial, à Faculdade de Computação, pela oportunidade de realizar este curso.

À CTBC, empresa na qual trabalho, pela permissão que me foi concedida para que eu pudesse me dedicar a todas as atividades do curso.

Ao meu orientador, Prof. Dr. João Nunes de Souza, pela constante orientação, pelo incentivo durante a elaboração desta dissertação e pela confiança e apoio sempre prestados.

Aos demais professores do curso, que também contribuíram para minha formação.

À minha esposa, Andréa, que sempre compreendeu a importância deste curso e sempre me apoiou.

A todas as outras pessoas que, direta ou indiretamente, contribuíram para a realização deste sonho.

"Uma universidade, antes de tudo, é um centro de contestação do mundo à sua volta. Um refúgio onde se cultiva a dúvida. Um oásis onde teorias costumam ser erodidas e mitos, contestados."

(Carlos Chagas - Jornalista)

SUMÁRIO

RESUMO	7
<i>ABSTRACT</i>	8
LISTA DE FIGURAS	9
LISTA DE TABELAS	11
LISTA DE ABREVIATURAS E SIGLAS	12
1 – INTRODUÇÃO	15
2 – REDES LOCAIS SEM FIO	18
2.1 Introdução	18
2.2 Tipos de redes locais sem fio	19
2.3 Visão geral do padrão IEEE 802.11	21
2.4 Os processos de operação da rede local sem fio	24
2.5 Os quadros de rede e formato de mensagens	30
3 – VULNERABILIDADES DAS REDES LOCAIS SEM FIO	44
3.1 Introdução	44
3.2 Mecanismos de segurança do IEEE 802.11 e suas fragilidades	45
3.3 Mecanismos de segurança agregados pelos fabricantes e suas fragilidades	47
3.4 Mecanismos de segurança do IEEE 802.1X e suas fragilidades	49
3.5 Mecanismos de segurança do WPA e suas fragilidades	51
3.6 Administração e gerência dos pontos de acesso e suas fragilidades	55
3.7 Um teste de invasão em uma rede baseada no padrão IEEE 802.11	56
4 – OS PROTOCOLOS RC4 E WEP	68
4.1 Introdução	68
4.2 Cifradores de bloco, cifradores de fluxo e modos de criptografia	68
4.3 Visão geral do protocolo RC4	73
4.4 Visão geral do protocolo WEP	74
4.5 Fragilidades do protocolo WEP	76
5 – PROPOSTA DE MELHORIA DO NÍVEL DE SEGURANÇA DAS REDES LOCAIS SEM FIO	84
5.1 Introdução	84
5.2 Proposta de melhoria do nível de segurança de redes locais sem fio	85
5.3 Redução dos efeitos das fraquezas do protocolo WEP	94
5.4 Revogação de chaves de sessão	95

5.5 Formato e tamanho dos quadros de rede e processos	96
5.6 Avaliação da proposta	106
5.7 Outras medidas para melhorar a segurança das redes locais sem fio	111
CONCLUSÃO	115
REFERÊNCIAS BIBLIOGRÁFICAS	117

RESUMO

Esta dissertação apresenta os principais conceitos e tipos de redes locais sem fio. Os padrões IEEE 802.11, 802.1X e WPA são expostos, e suas fraquezas são apontadas e discutidas. Um estudo com base nos algoritmos criptográficos RC4 e WEP também é apresentado. Com a indicação das principais vulnerabilidades das redes locais sem fio, um teste de invasão em um ambiente de testes é conduzido com sucesso. Finalmente, uma proposta para melhoria do nível de segurança deste ambiente é exibida e avaliada como uma comparação aos atuais padrões.

Palavras chave: segurança, rede, sem fio, criptografia

ABSTRACT

This dissertation presents the main concepts and types of the wireless LAN. The standards IEEE 802.11, 802.1X and WPA are showed, and theirs fragilities are pointed and discussed. A study based on the cryptographic algorithms RC4 and WEP are also presented. Pointing the main vulnerabilities of the wireless LAN, an invasion test is successfully conducted. Finally, a proposal to increase the security level of this environment is exhibited and evaluated as a comparison with the nowadays standards.

Key-words: security, network, wireless, cryptography

LISTA DE FIGURAS

Figura 1 – Rede independente ou sem infra-estrutura (<i>ad-hoc</i>)	20
Figura 2 – Rede com infra-estrutura: (a) isolada e (b) conectada à rede cabeada	21
Figura 3 – Conexão à rede local sem fio, padrão IEEE 802.11	22
Figura 4 – Campo de controle do quadro	30
Figura 5 – Quadros de controle	33
Figura 6 – Quadros de dados	34
Figura 7 – Quadros de gerenciamento	36
Figura 8 – Conexão à rede local sem fio, padrão 802.11 com mecanismos adicionais	48
Figura 9 – Tela de propriedades do <i>driver</i> do Windows para uma interface Orinoco	57
Figura 10 – Tela de abertura do processo de atualização	58
Figura 11 – Tela de confirmação do processo de <i>downgrade</i>	58
Figura 12 – Tela de confirmação da atualização com sucesso	59
Figura 13 – Tela de propriedades do <i>driver</i> alterado	59
Figura 14 – Tela do controlador Orinoco com as versões em uso	60
Figura 15 – Tela do NetStumbler mapeando a rede utilizada no teste de invasão	62
Figura 16 – Tela do AiroPeek exibindo o conteúdo de um pacote capturado	63
Figura 17 – Tela do MAC MakeUp alterando o MAC da interface sem fio	64
Figura 18 – Tela do AirSnort capturando tráfego na rede	64
Figura 19 – Tela do AirSnort ao término do processo de quebra da chave WEP	65
Figura 20 – Telas de configuração do cliente da interface sem fio	65
Figura 21 – Tela do Ethereal exibindo o conteúdo de um pacote capturado	66
Figura 22 – Esquema de um cifrador de fluxo	69
Figura 23 – Esquema de um cifrador de blocos	70
Figura 24 – Esquema de um quadro de rede com os detalhes do vetor de inicialização	71
Figura 25 – Esquema do modo de operação CBC	72
Figura 26 – Esquema do algoritmo RC4	73
Figura 27 – Esquema do protocolo WEP	75
Figura 28 – Ataque por injeção de mensagem	79
Figura 29 – Expansão de uma chave-fluxo	80
Figura 30 – Ataque por alteração de <i>bits</i>	81
Figura 31 – Alteração de <i>bits</i> na mensagem criptografada	82
Figura 32 – Conexão à rede local sem fio, de acordo com esta proposta	85

Figura 33 – Detalhamento da fase de autenticação, de acordo com esta proposta	88
Figura 34 – Exemplo didático de uma autenticação, de acordo com esta proposta	91
Figura 35 – Processo de reautenticação	92
Figura 36 – Processo de desautenticação	93
Figura 37 – Processo de revogação de chaves	95
Figura 38 – Formato do <i>frame body</i>	96
Figura 39 – Gráfico do tráfego da rede em um dia	110

LISTA DE TABELAS

Tabela 1 – Combinações de tipo e subtipo de pacotes	31
Tabela 2 – Campos e conteúdo de endereços	34
Tabela 3 – Conteúdo do pacote <i>beacon</i>	37
Tabela 4 – Conteúdo do pacote de desassociação	37
Tabela 5 – Conteúdo do pacote de pedido de associação	38
Tabela 6 – Conteúdo do pacote de resposta de associação	38
Tabela 7 – Conteúdo do pacote de pedido de reassociação	39
Tabela 8 – Conteúdo do pacote de resposta de reassociação	39
Tabela 9 – Conteúdo do pacote de pedido de sondagem	40
Tabela 10 – Conteúdo do pacote de resposta de sondagem	40
Tabela 11 – Conteúdo do pacote de autenticação	41
Tabela 12 – Aplicabilidade do algoritmo WEP	41
Tabela 13 – Processo de autenticação no padrão	42
Tabela 14 – Conteúdo do pacote de desautenticação	42
Tabela 15 – Processo de desautenticação no padrão	43
Tabela 16 – Processo de autenticação	105
Tabela 17 – Processo de reautenticação	105
Tabela 18 – Processo de desautenticação	105
Tabela 19 – Processo de revogação de chaves	105
Tabela 20 – Tamanho dos processos no padrão e na proposta	106
Tabela 21 – Perfil de autenticação e desautenticação	107

LISTA DE ABREVIATURAS E SIGLAS

AID – Association Identifier
AP – Access Point
ATIM – Announcement Traffic Indication Message
BSSID – Basic Service Set Identifier
CBC – Cipher Block Chaining
CFB – Cipher Feedback
CF-END – Content Free End
CFP – Contention Free Period
CRC32 – Cyclic Redundancy Check
CTBC – Companhia de Telecomunicações do Brasil Central
CTS – Clear To Send
DA – Destination Address
DHCP – Dynamic Host Configuration Protocol
DOS – Denial of Service
DS – Distribution System
DSSS – Direct Sequence Spread Spectrum
EAP – Extensible Authentication Protocol
ECB – Electronic Code Book
ESS – Extended Service Set
FCS – Frame Check Sequence
FH – Frequency Hopping
FHSS – Frequency Hopped Spread Spectrum
HTTP – HyperText Transfer Protocol
HTTPS – Hypertext Transfer Protocol Secure
I2TS – International Information and Telecommunication Technologies
IBSS – Independent Basic Service Set
ICMP – Internet Control Message Protocol
ICV – Integrity Check Value
IDS – Intrusion Detection System
IEEE – Institute of Electrical and Electronics Engineers
IP – Internet Protocol

IPSEC – Internet Protocol Secure
ITA – Instituto Tecnológico de Aeronáutica
IV – Initialization Vector
KSA – Key Scheduling Algorithm
LEAP – Lightweight Extensible Authentication Protocol
MAC – Medium Access Control
MIC – Message Integrity Check
MIT – Massachusetts Institute of Technology
MSDU – MAC Service Data Unit
MTU – Maximum Transmission Unit
OFB – Output Feedback
OSA – Open System Authentication
PCMCIA – Personal Computer Memory Card International Association
PRGA – Pseudo Random Generation Algorithm
PRNG – Pseudo Random Number Generator
PSK – Pre Shared Key
RA – Receiver Address
RADIUS – Remote Authentication Dial-In User Service
RAM – Random Access Memory
RC4 – Ron’s Code #4
RFC – Request For Comments
RTS – Request To Send
SA – Source Address
SBRC – Sociedade Brasileira de Redes de Computadores
SKA – Shared Key Authentication
SNMPv1 – Simple Network Management Protocol version 1
SNMPv3 – Simple Network Management Protocol version 3
SOHO – Small Office Home Office
SRP – Secure Remote Password
SSH – Secure Shell
SSI – Simpósio de Segurança em Informática
SSID – Service Set Identifier
SSL – Secure Sockets Layer
TA – Transmitter Address
TCP – Transmission Control Protocol

TIM – Traffic Indication Message

TKIP – Temporal Key Integrity Protocol

TLS – Transport Layer Security

TTLS – Tunneled Transport Layer Security

UFU – Universidade Federal de Uberlândia

VPN – Virtual Private Network

WEP – Wired Equivalent Privacy

WI-FI – Wireless Fidelity

WPA – Wi-Fi Protected Access

WSEG – Workshop de Segurança

1 INTRODUÇÃO

As redes locais sem fio são uma alternativa às redes cabeadas, com a grande vantagem de prover flexibilidade e mobilidade. Tais redes permitem que diversas estações ou servidores se comuniquem sem a necessidade de cabos. Com isso, essas redes têm se tornado, cada vez mais, uma opção para ambientes corporativos, pois podem ser rapidamente implementadas em ambientes que não possuam infra-estrutura de cabeamento, além de possibilitar a mobilidade que, gradativamente, torna-se um requisito importante no mundo atual.

Por sua vez, outro requisito cada vez mais necessário é a segurança do ambiente ou solução. Logo, no caso das redes locais sem fio, é importante que a solução garanta mecanismos de disponibilidade, integridade e confidencialidade dos dados e autenticidade das partes envolvidas.

Os padrões e soluções atuais não oferecem o nível desejado de segurança, ou seja: não garantem a confidencialidade das informações, com isso, muitos fabricantes agregaram mecanismos de proteção proprietários, que nem sempre resolvem as atuais vulnerabilidades. A maioria das soluções disponíveis no mercado não podem ser consideradas seguras devido às várias vulnerabilidades existentes.

O grande objetivo desta dissertação é avaliar os mecanismos de segurança das redes locais sem fio testando na prática as vulnerabilidades identificadas. Entendidas estas vulnerabilidades o objetivo passa a ser propor um protocolo para acesso às redes locais sem fio com as seguintes premissas: manter o máximo de adesão aos princípios do padrão IEEE 802.11; manter compatibilidade com o hardware atualmente instalado na maioria das empresas; e elevar consideravelmente o nível de segurança deste ambiente, eliminando ou minimizando as principais vulnerabilidades dos atuais esquemas.

Esta dissertação está dividida em seis capítulos, da seguinte forma: o capítulo 1 apenas introduz, de forma simplificada, o assunto e o trabalho realizado. O capítulo 2 introduz os principais conceitos e tipos de redes locais sem fio, o padrão IEEE 802.11, os processos e quadros necessários para a operação da rede. No capítulo 3, as vulnerabilidades das redes locais sem fio são estudadas e apontadas, incluindo os padrões IEEE 802.11, 802.1X e WPA (*Wi-Fi Protected Access*) alguns mecanismos de segurança agregados pelos fabricantes de equipamentos também são analisados. Ainda no capítulo 3, é descrito um teste de invasão bem sucedido, implementado em um ambiente de testes. Já no capítulo 4, um estudo dos protocolos criptográficos RC4 (*Ron's Code #4*) e WEP (*Wired Equivalent Privacy*) é exposto, estes protocolos são amplamente utilizados nas redes locais sem fio. No capítulo 5, é apresentada uma proposta que visa minimizar ou extinguir as atuais vulnerabilidades, elevando o nível de segurança das redes locais sem fio; os processos e esquemas de quadros da nova proposta também são detalhados para que possam auxiliar no processo de avaliação. Ainda no capítulo 5, é realizado um estudo que avalia a proposta em relação aos atuais padrões, ele é baseado em um estudo de caso efetuado em uma rede real; ainda de forma complementar, outras medidas, já conhecidas, que podem auxiliar na proteção de redes locais sem fio são discutidas.

Como fruto de pesquisas e estudos realizados durante este curso, e como base para esta dissertação, três artigos foram produzidos e publicados pelo mestrando em conjunto com seu orientador. Estes artigos são relacionados a seguir, na ordem de publicação.

Uma análise dos mecanismos de segurança das redes locais sem fios e uma proposta de melhoria.

Publicado no **WSEG** (Workshop de Segurança) do **SBRC** em Maio de 2003 em Natal/RN.

Proposta de melhoria dos mecanismos de segurança das redes locais sem fios.

Publicado no Simpósio de Segurança em Informática (SSI) no ITA em Novembro de 2003 em São José dos Campos/SP.

Estudo e melhoria dos mecanismos de segurança em redes locais sem fios.

Publicado no I2TS - International Information and Telecommunication Technologies em Novembro de 2003 em Florianópolis/SC.

Pelo artigo publicado no SSI, ocorrido no ITA, os autores receberam o prêmio Tércio Pacitti como Menção Honrosa oferecido pela SIEMENS.

2 REDES LOCAIS SEM FIO

2.1 Introdução

As redes locais sem fio são uma alternativa às atuais redes cabeadas, com a grande vantagem de prover flexibilidade e mobilidade. Elas permitem que diversas estações ou servidores se comuniquem sem a necessidade de cabos. A comunicação ocorre através de ondas eletromagnéticas. Essas redes podem existir de forma isolada, apenas com o intuito de prover conectividade a um grupo de sistemas, mas também podem existir como uma extensão de uma rede convencional cabeada. Ou seja, parte do ambiente de rede pode ser implementado no formato convencional através de conexões cabeadas e parte dela, a que requer mobilidade, pode ser implementada por meio de conexões sem fio. Logo, uma rede local sem fio pode ser definida como um meio flexível de comunicação de dados, implementado como uma extensão ou uma alternativa de uma rede local cabeada.

Essas redes têm se tornado cada vez mais uma opção para ambientes corporativos, já que podem ser rapidamente implementadas em locais que não possuam infra-estrutura de cabeamento. Além de permitir a mobilidade, que é um requisito importante no mundo atual.

Em 1999, o IEEE (*Institute of Electrical and Electronics Engineers*) publicou o padrão IEEE 802.11 [IEEE 1999], que é o responsável pela especificação das redes locais sem fio. Ele descreve o ambiente e o protocolo em todos seus aspectos, incluindo desde a parte física até os mecanismos de segurança do protocolo.

Outro padrão, relacionado às redes sem fio, descreve mecanismos de autenticação por porta. Originalmente desenvolvido para as redes convencionais, o padrão IEEE 802.1X [IEEE 2001] é bastante utilizado para as implementações de redes sem fio. Esse padrão descreve

mecanismos adicionais de segurança, que visam tornar essas redes locais sem fio mais seguras.

A seção 2.2 exhibe os principais tipos de redes locais sem fio e suas principais características. A seção 2.3 apresenta uma visão geral do padrão IEEE 802.11. A seção 2.4 descreve os principais processos necessários para a operação da rede local sem fio no padrão IEEE 802.11. Finalmente, na seção 2.5, o formato das mensagens e os quadros de rede são detalhados.

2.2 Tipos de redes locais sem fio

Basicamente, existem dois tipos de redes locais sem fio: as rede independentes, ou *ad-hoc*, e as redes com infra-estrutura.

As redes independentes, também chamadas de *ad-hoc*, são as redes sem fio mais básicas e simples. São redes sem topologia determinada, em que não existe qualquer elemento central que estruture a comunicação. Neste caso, as estações se comunicam diretamente entre si. A grande vantagem dessas redes é a facilidade de instalação, que se resume à configuração das interfaces de rede sem fio em cada estação móvel. Como nenhum outro elemento é necessário, os custos também são reduzidos, e nem mesmo um projeto precisa ser elaborado. No entanto, como desvantagens tem-se o fato de uma cobertura pequena e restrita e inconstância na qualidade da comunicação. Há também falhas devido a barreiras físicas que podem interferir na comunicação entre estações, já que elas se comunicam diretamente. Além de deficiências de controle, há também deficiências de segurança, pois a maioria dos

mecanismos de segurança são implementados no elemento que coordena a rede e que, neste caso, não existe. A figura 1 mostra o esquema de comunicação em uma rede independente:

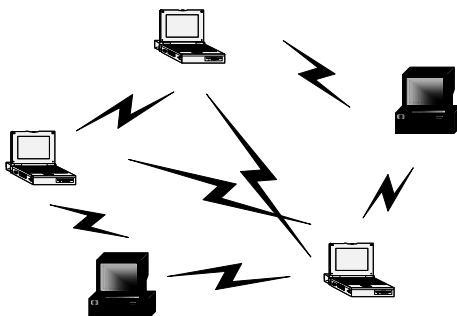


Figura 1 – Rede independente ou sem infra-estrutura (*ad-hoc*)

As redes com infra-estrutura incluem pelo menos um elemento centralizador de área que coordena parte da rede, chamado de ponto de acesso. Toda e qualquer comunicação passa por esse elemento, e a qualidade de serviço pode ser controlada. Além disso, barreiras físicas raramente são problemas, visto que a rede é projetada a fim de prover cobertura em uma certa área. Neste caso, o posicionamento do ponto de acesso é definido de modo a maximizar a qualidade e área de cobertura desejada. Ainda quando a cobertura for insuficiente, outros pontos de acesso podem ser inseridos, resultando em uma expansão da infra-estrutura da rede local sem fio. Desta forma, a comunicação entre duas estações em pontos de acesso diferentes pode ocorrer sem problemas. Outra vantagem é referente aos mecanismos de controle e segurança, pois cada estação cliente deverá associar-se e autenticar-se perante o ponto de acesso, como será detalhado mais adiante. Basicamente, apenas as redes com infra-estrutura são utilizadas em ambientes corporativos e são o tipo mais empregado atualmente. A figura 2 mostra o esquema de comunicação em uma rede com infra-estrutura: (a) de forma isolada e (b) conectada à rede cabeada:

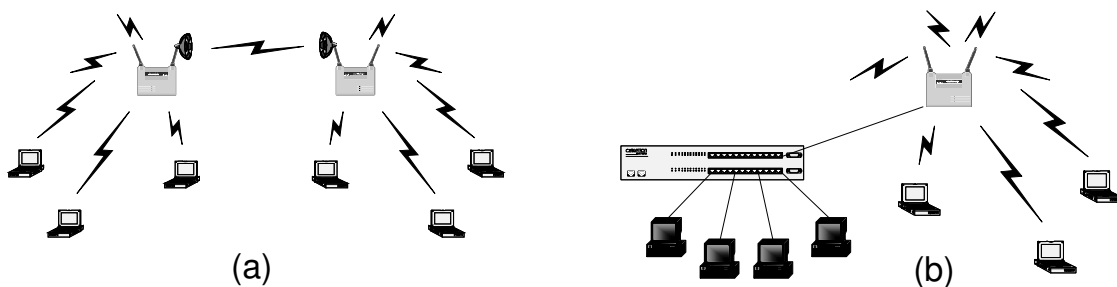


Figura 2 – Rede com infra-estrutura: (a) isolada e (b) conectada à rede cabeada

2.3 Visão geral do padrão IEEE 802.11

O IEEE 802.11 é um padrão aprovado, em 1997, para as redes locais sem fio, definindo a camada física e a camada MAC (*Medium Access Control*) e seus protocolos. Inclui, ainda, mecanismos de controle de acesso, confidencialidade e integridade.

O padrão determina duas tecnologias que podem ser utilizadas na camada física: DSSS (*Direct Sequence Spread Spectrum*) e FHSS (*Frequency Hopped Spread Spectrum*).

O padrão IEEE 802.11 é dividido em alguns sub-grupos como descrito em [Deshpande 2003] e [Lim 2003]:

- no 802.11a, a velocidade pode chegar a 54Mbits/s, no entanto opera em 5GHz, necessitando de autorização para uso de frequência;
- no 802.11b, a velocidade pode chegar a 11Mbits/s operando em 2.4GHz. É a versão atualmente mais utilizada e comum;
- no 802.11g, a velocidade pode chegar a 22Mbits/s, com a vantagem de operar em 2.4GHz;

- o 802.11h é a versão européia do 802.11a, com poucas diferenças e algumas otimizações;
- o 802.11i foca as questões de segurança;
- o 802.11c foca a melhoria de interoperabilidade entre dispositivos;
- o 802.11d foca a melhoria de *roaming*;
- o 802.11e foca a melhoria de qualidade de serviço;
- o 802.11f foca a regularização de *handoff*.

O padrão determina três fases pelas quais qualquer cliente deve passar com sucesso antes de obter acesso à rede sem fio. A figura 3 ilustra essas 3 fases. Ela descreve um esquema de conexão à rede local sem fio, incluindo as fases de sondagem, autenticação e associação. Cada seta para a direita representa a transmissão dos dados nela nomeados do cliente para o ponto de acesso, e cada seta para a esquerda representa uma transmissão dos dados nela nomeados do ponto de acesso para o cliente. No caso do exemplo ilustrado na figura 3, o padrão IEEE 802.11 é utilizado com o algoritmo SKA (*Shared Key Authentication*), que será detalhado em breve.

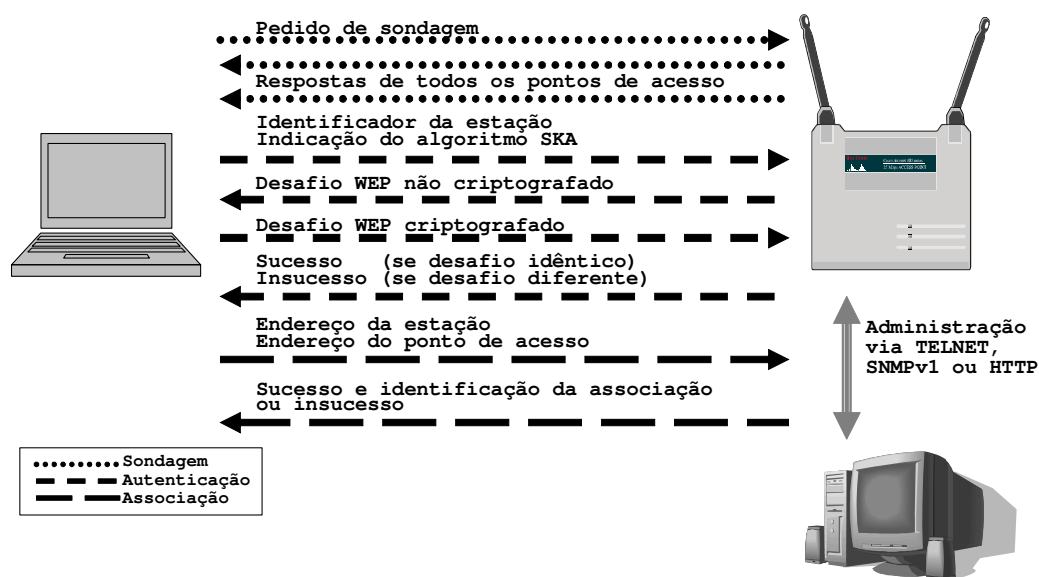


Figura 3 – Conexão à rede local sem fio, padrão IEEE 802.11

As três fases de conexão são:

Fase de sondagem – O cliente envia requisições de acesso pelo ar, como se fosse um *broadcast* em uma rede convencional. Em seguida, todos os pontos de acesso que estiverem na área de cobertura respondem com informações que podem ser utilizadas nas fases de autenticação e associação. A fase de sondagem é indicada na figura 3 pelas três primeiras linhas.

Fase de autenticação – Existem dois tipos de autenticação definidos no padrão: OSA (*Open System Authentication*) e SKA (*Shared Key Authentication*). A configuração do ponto de acesso e a indicação do cliente definem qual esquema é utilizado. A fase de autenticação é indicada na figura 3, entre a quarta e sétima linha. Os dois tipos de autenticação são detalhados a seguir:

OSA – *Open System Authentication*: Neste protocolo, toda a negociação é feita em texto não criptografado e nenhuma condição é imposta, ou seja, todos clientes que solicitam a autenticação são autenticados. Basicamente, é uma autenticação nula e pode ser utilizada em redes de acesso público.

SKA – *Shared Key Authentication*: Neste tipo de autenticação, o ponto de acesso, normalmente denominado por AP (*Access Point*), envia um desafio em texto não criptografado para o cliente. Esta criptografia é feita com uma chave pré-compartilhada anteriormente definida entre o ponto de acesso e o cliente. O cliente deve criptografar o desafio com o protocolo WEP, utilizando uma chave de sessão pré-compartilhada, que, depois, deve ser enviado novamente ao ponto de acesso. O ponto de acesso verifica se a resposta ao seu desafio está

correta. Estes passos são ilustrados na composição da fase de autenticação da figura 3.

Fase de associação – O cliente, já autenticado e de posse das informações recebidas na fase de sondagem, envia um pedido de associação para o ponto de acesso escolhido. O ponto de acesso devolve uma resposta contendo o identificador da associação que pode ser empregado para pedidos de reassociação ou desassociação. Esta fase é indicada na figura 3 pelas duas últimas linhas.

O padrão IEEE 802.11 pode utilizar o protocolo WEP para garantir a confidencialidade dos dados no ar. A integridade é assegurada pelo uso de um algoritmo redundante do tipo CRC32 (*Cyclic Redundancy Check*), denominado ICV (*Integrity Check Value*), conforme mostrado em [Peres e Weber 2003].

O protocolo WEP, por sua vez, é baseado no protocolo *stream cipher* RC4. Ele é considerado vulnerável, pois possui falhas na programação de chaves no algoritmo KSA (*Key Scheduling Algorithm*), que trata a questão de reuso de chave-fluxo (*key-stream*). Estudos sobre as fraquezas do protocolo WEP são apresentados no capítulo 3, 4 e também em [Arbaugh e Shankar 2001] e [Roshan 2002].

2.4 Os processos de operação da rede local sem fio

Para que a rede local sem fio possa operar normalmente, alguns processos são necessários. Estes processos controlam e inspecionam a forma de acesso à rede. Permitem,

também, a mobilidade entre pontos de acesso por intermédio de processos de associação. Garantem a segurança mediante processos de validação e a privacidade por meio de processos de criptografia.

Em seqüência, os principais processos são apresentados, detalhando suas etapas, mensagens e possíveis valores de conteúdo.

2.4.1 Processo de transferência de dados

O processo de transferência de dados é utilizado por uma estação para o envio de dados para outra estação, seja um sistema terminal na rede ou um ponto de acesso.

Este processo opera com mensagens no seguinte formato:

Nome da mensagem	: Mensagem de dados
Tipo da mensagem	: Dados
Subtipo da mensagem	: Dados
Itens de informação	: Endereço de origem Endereço de destino Identificador da rede Dados
Sentido	: De uma estação para outra estação

2.4.2 Processo de associação

O processo de associação é utilizado por uma estação, para que esta possa associar-se à rede após o processo de autenticação.

Este processo opera com mensagens no seguinte formato:

Nome da mensagem	: Pedido de associação
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Pedido de associação
Itens de informação	: Endereço da estação que faz o pedido

	Endereço do ponto de acesso envolvido
	Identificador da rede
Sentido	: De uma estação para o ponto de acesso
Nome da mensagem	: Resposta de associação
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Resposta de associação
Itens de informação	: Resultado do pedido de associação
	No caso de sucesso o identificador da associação é enviado
Sentido	: Do ponto de acesso para uma estação

2.4.3 Processo de reassociação

O processo de reassociação é utilizado por uma estação, para que esta possa associar-se a outro ponto de acesso. O requisito é que a estação já esteja associada a algum ponto de acesso.

Este processo opera com mensagens no seguinte formato:

Nome da mensagem	: Pedido de reassociação
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Pedido de reassociação
Itens de informação	: Endereço da estação que faz o pedido
	Endereço do ponto de acesso associado
	Endereço do novo ponto de acesso
	Identificador da rede
Sentido	: De uma estação para o novo ponto de acesso
Nome da mensagem	: Resposta de reassociação
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Resposta de reassociação
Itens de informação	: Resultado do pedido de associação

No caso de sucesso, o identificador da associação é enviado

Sentido : Do novo ponto de acesso para uma estação

2.4.4 Processo de desassociação

O processo de desassociação é utilizado por uma estação, para que esta deixe de participar da rede local sem fio.

Este processo opera com mensagens no seguinte formato:

Nome da mensagem : Desassociação

Tipo da mensagem : Gerenciamento

Subtipo da mensagem : Desassociação

Itens de informação : Endereço da estação que faz o pedido

Endereço do ponto de acesso envolvido

Sentido : De uma estação para o ponto de acesso ou de um ponto de acesso para uma estação

2.4.5 Processo de privacidade

O processo de privacidade é utilizado por uma estação, para que o protocolo WEP seja ativado protegendo as informações trafegadas quanto à confidencialidade. Nenhuma mensagem específica é necessária, apenas o *bit* do campo WEP dos quadros de controle precisam ser definidos.

2.4.6 Processo de autenticação OSA

O processo de autenticação OSA é um tipo de autenticação nula, pois todos os clientes que solicitam autenticação são aceitos.

Este processo opera com mensagens no seguinte formato:

Nome da mensagem : Autenticação OSA – pacote inicial

Tipo da mensagem : Gerenciamento

Subtipo da mensagem : Autenticação

Itens de informação	: Algoritmo de autenticação = OSA Seqüência de transação da autenticação = 1
Sentido	: De uma estação para o ponto de acesso
Nome da mensagem	: Autenticação OSA – pacote final
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Autenticação
Itens de informação	: Algoritmo de autenticação = OSA Seqüência de transação da autenticação = 2 Resultado = sucesso
Sentido	: Do ponto de acesso para uma estação

2.4.7 Processo de autenticação SKA

O processo de autenticação SKA utiliza o algoritmo WEP para validar a estação que solicita a autenticação.

Este processo opera com mensagens no seguinte formato:

Nome da mensagem	: Autenticação SKA – pacote inicial
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Autenticação
Itens de informação	: Algoritmo de autenticação = SKA Seqüência de transação da autenticação = 1 Identificador da estação
Sentido	: De uma estação para o ponto de acesso
Nome da mensagem	: Autenticação SKA – pacote intermediário
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Autenticação
Itens de informação	: Algoritmo de autenticação = SKA Seqüência de transação da autenticação = 2

	Informações adicionais = texto de desafio
Sentido	: Do ponto de acesso para uma estação
Nome da mensagem	: Autenticação SKA – pacote intermediário
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Autenticação
Itens de informação	: Algoritmo de autenticação = SKA
	Seqüência de transação da autenticação = 3
	Informações adicionais = desafio criptografado
Sentido	: De uma estação para o ponto de acesso
Nome da mensagem	: Autenticação SKA – pacote final
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Autenticação
Itens de informação	: Algoritmo de autenticação = SKA
	Seqüência de transação da autenticação = 4
	Resultado = sucesso ou insucesso
Sentido	: Do ponto de acesso para uma estação

2.4.8 Processo de desautenticação

O processo de desautenticação é utilizado por uma estação, para que esta deixe de participar da rede local sem fio.

Este processo opera com mensagens no seguinte formato:

Nome da mensagem	: Desautenticação
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Desautenticação
Itens de informação	: Endereço da estação que faz o pedido
Sentido	: De uma estação para o ponto de acesso

Esses pacotes ilustram os processos que mantêm o controle e a segurança em uma rede baseada no padrão IEEE 802.11. No capítulo 5, novos processos são definidos e exibidos, de acordo com a proposta deste trabalho.

2.5 Os quadros de rede e formato de mensagens

Os quadros de rede utilizados pelo padrão IEEE 802.11 são denominados quadros MAC. Cada estação deve estar habilitada a criar, enviar e receber este tipo de quadro, pois neles trafegam todas as mensagens de controle, dados e gerenciamento de uma rede local sem fio.

Existe um campo de controle do quadro, denominado *frame control*, que compõe tanto os quadros de controle, como dados e gerenciamento. Este campo é composto por 11 subcampos, totalizando 2 bytes. A figura 4 exibe a estrutura deste campo.

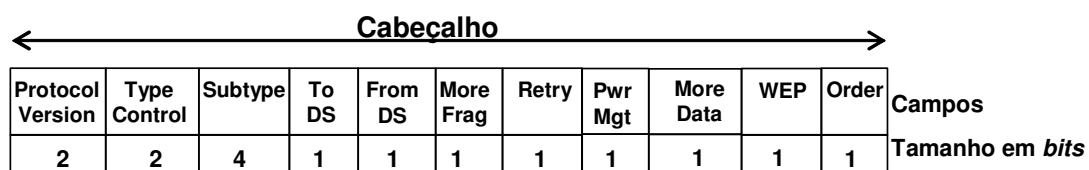


Figura 4 – Campo de controle do quadro

O campo “versão do protocolo”, *protocol version*, tem o tamanho fixo de 2 bits. O valor para o padrão atual é 0, e qualquer outro valor é reservado para versões futuras do protocolo.

O campo “controle de tipo”, *type control*, também tem tamanho fixo de 2 bits, e opera em conjunto com o campo de subtipo, que tem o tamanho fixo de 4 bits. O campo de tipo

determina se o quadro é de controle, dados ou gerenciamento, e o campo de subtipo possui os detalhes de cada tipo de quadro. A tabela 1 indica as possíveis combinações.

Tabela 1 – Combinações de tipo e subtipo de pacotes

Valor do Tipo	Descrição do Tipo	Valor do subtipo	Descrição do subtipo
00	Gerenciamento	0000	Pedido de associação
00	Gerenciamento	0001	Resposta de associação
00	Gerenciamento	0010	Pedido de reassociação
00	Gerenciamento	0011	Resposta de reassociação
00	Gerenciamento	0100	Pedido de sondagem
00	Gerenciamento	0101	Resposta de sondagem
00	Gerenciamento	0110-0111	Reservado
00	Gerenciamento	1000	Beacon
00	Gerenciamento	1001	ATIM
00	Gerenciamento	1010	Desassociação
00	Gerenciamento	1011	Autenticação
00	Gerenciamento	1100	Desautenticação
00	Gerenciamento	1101-1111	Reservado
01	Controle	0000-1001	Reservado
01	Controle	1010	PS-Poll
01	Controle	1011	RTS
01	Controle	1100	CTS
01	Controle	1101	ACK
01	Controle	1110	CF-End
01	Controle	1111	CF-End+CF-Ack
10	Dados	0000	Dados
10	Dados	0001	Dados+CF-Ack
10	Dados	0010	Dados+CF-Poll
10	Dados	0011	Dados+CF-Ack+CF-Poll
10	Dados	0100	Função nula
10	Dados	0101	CF-Ack (sem dados)
10	Dados	0110	CF-Poll (sem dados)
10	Dados	0111	CF-Ack+CF-Poll (sem dados)
10	Dados	1000-1111	Reservado
11	Reservado	0000-1111	Reservado

Os campos “para” e “do sistema de distribuição”, *to DS e from DS (Distribution System)*, indicam o sentido do pacote. Ambos os campos possuem tamanho fixo de 1 bit. O campo “para” o DS é definido com valor 1 nos casos em que o pacote de dados foi gerado por

uma estação associada e com destino ao sistema de distribuição, nos demais casos, o valor do campo é 0. O mesmo ocorre com o campo “do” DS, porém no sentido contrário.

O campo “mais fragmentos”, *more frag*, também tem o tamanho fixo de 1 bit e é definido com o valor 1 em qualquer campo de dados ou gerenciamento que possuam outros fragmentos, nos demais casos, o valor do campo é definido em 0.

O campo de “retentativa”, *retry*, possui um único *bit*, que é definido como 1 nos campos de dados e gerenciamento que estão sendo retransmitidos. A estação que recebe o pacote utiliza esta informação para evitar o processamento de pacotes duplicados, nos demais casos, o valor do campo é 0.

O campo de “gerenciamento de energia”, *power managment*, tem 1 bit de tamanho fixo, e seu valor é definido em 1, quando a estação irá entrar no modo de economia de energia, e novamente definido em 0, quando sair deste modo. Um ponto de acesso sempre transmite seus pacotes com este campo definido em 0.

O campo “mais dados”, *more data*, também tem o tamanho fixo de 1 bit, e este tem o valor 1, quando o ponto de acesso possui pelo menos um pacote, em fila, destinado a uma estação que está no modo de economia de energia. Este campo é definido em 1 somente neste sentido e tem o valor 0 em todos os outros casos. Este pacote pode ser utilizado pela estação a fim de que saia do modo de economia de energia, se assim foi configurada.

O campo “WEP” tem 1 bit de tamanho fixo e é definido em 1 quando determina que parte do controle do quadro foi processado com este algoritmo. Nos demais casos, o valor é definido em 0.

O campo de “ordem”, *order*, também tem o tamanho fixo de 1 *bit* e é definido com valor 1 nos casos nos quais existem fragmentos de pacotes de dados operando na classe em que não devem ser recebidos em ordem diferente da gerada.

2.5.1 Quadros de controle

Os quadros de controle são responsáveis por controlar o fluxo de pacotes na rede. Logo, tarefas como autorização para transmissão, controle de reconhecimento de pacotes recebidos e outras, são inerentes aos quadros de controle.

A figura 5 apresenta os esquemas dos quadros dos diversos tipos de controles aplicados às redes locais sem fio.

RTS	Frame Control	Duration	RA	TA	FCS	Campos
	2	2	6	6	4	Tamanho em bytes

CTS	Frame Control	Duration	RA	FCS	Campos
	2	2	6	4	Tamanho em bytes

ACK	Frame Control	Duration	RA	FCS	Campos
	2	2	6	4	Tamanho em bytes

PS-Poll	Frame Control	AID	BSSID	TA	FCS	Campos
	2	2	6	6	4	Tamanho em bytes

CF-End	Frame Control	Duration	RA	BSSID	FCS	Campos
	2	2	6	6	4	Tamanho em bytes

CF-End+CF-Ack	Frame Control	Duration	RA	BSSID	FCS	Campos
	2	2	6	6	4	Tamanho em bytes

Figura 5 – Quadros de controle

Cada um desses 6 tipos de quadros de controle tem um objetivo específico, relacionados à garantia de entrega dos pacotes, autorização para transmissão, reconhecimento de pacotes e outros. Assim, esses quadros não são detalhados neste trabalho por não estarem diretamente relacionados com o seu objetivo.

2.5.2 Quadros de dados

Os quadros de dados são responsáveis pela transmissão das mensagens de dados da rede, ou seja, executam a atividade fim da rede que é transmitir os dados do usuário. Esses quadros são controlados pelos quadros de controle, acompanhados e autorizados pelos quadros de gerenciamento. A figura 6 mostra a estrutura dos quadros de dados.

Cabeçalho								
Frame Control	Duration ID	Address 1	Address2	Address3	Sequence Control	Address4	Frame Body	FCS
2	2	6	6	6	2	6	0-2312	4

Campos
Tamanho em bytes

Figura 6 – Quadros de dados

O quadro de dados é formado por 9 campos. O campo de controle do quadro já foi discutido. O campo “duração”, *duration id*, tem o tamanho de 2 bytes e indica um valor baseado no tipo do quadro, conforme determinado em [IEEE 1999].

Os 4 campos de endereços têm uso variável, dependendo da origem e do destino da comunicação. A tabela 2 mostra informações sobre o sentido da comunicação, e em função deste, os valores de conteúdo dos quatro campos de endereços.

Tabela 2 – Campos e conteúdo de endereços

Para o DS	Do DS	Endereço 1	Endereço 2	Endereço 3	Endereço 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Dependendo da combinação dos campos *To* e *From* DS, os campos de endereços têm conteúdos diferenciados. Considera-se, por exemplo, a terceira linha de dados da tabela 2, em que um pacote tem o destino para o DS e contém o valor BSSID (*Basic Service Set Identifier*) no primeiro campo de endereços e o endereço SA (*Source Address*) da estação de origem no segundo campo de endereço. No terceiro campo de endereço, tem-se o endereço DA (*Destination Address*) de destino, e o último campo de endereços não é utilizado neste caso. Embora os termos TA e RA não sejam utilizados na referida linha, sabe-se que TA (*Transmitter Address*) é o endereço do transmissor, e RA (*Receiver Address*) é o endereço do receptor.

O campo de “controle de sequência”, *sequence control*, é dividido em 2 sub-campos: o “número do fragmento”, *fragment number*, que tem o tamanho fixo de 4 *bits*, e o “número de sequência”, *sequence number*, que tem tamanho fixo de 12 *bits*. Ambos fazem o controle de sequência de pacotes e fragmentos.

O campo “corpo do quadro”, *frame body*, tem tamanho variável, o tamanho mínimo é 0 *bytes*, e o máximo depende do tamanho do MTU (*Maximum Transmission Unit*). Este campo, efetivamente, transporta os dados da rede.

Finalmente, o campo FCS (*Frame Check Sequence*) tem um tamanho fixo de 32 *bits*. Este campo tem seu valor calculado utilizando uma função do tipo CRC32, autenticando todo o restante do pacote, incluindo cabeçalho e a parte dos dados.

2.5.3 Quadros de gerenciamento

O esquema dos quadros de gerenciamento é independente dos campos tipo e sub-tipo como aqueles definidos na tabela 1. Além disso, os campos de endereços também não variam a cada tipo de mensagem. Os quadros de gerenciamento controlam os processos de sondagem,

autenticação e associação. Assim, a estrutura de um quadro de gerenciamento é mostrada na figura 7.

← Cabeçalho →								Campos Tamanho em <i>bytes</i>
Frame Control	Duration	DA	SA	BSSID	Sequence Control	Frame Body	FCS	
2	2	6	6	6	2	6-2312	4	

Figura 7 – Quadros de gerenciamento

Alguns campos componentes deste quadro já foram discutidos. Entretanto, deve-se observar que, no caso dos quadros de gerenciamento, o campo “duração”, *duration*, é definido com o valor 32768 para todos os pacotes durante o CFP (*Contention Free Period*), no entanto, durante o período de contenção, o campo é utilizado para auxiliar no controle da rede, seguindo as regras definidas em [IEEE 1999]. O campo BSSID tem como valor o identificador da rede, ou, no caso de um pacote *beacon*, é o identificador da rede sobre a qual se desejam informações.

As mensagens para cada tipo de quadro de gerenciamento são exibidas a seguir. Muitas delas são associadas à operação da rede independentemente do foco em segurança e não são aqui detalhadas. Os processos de autenticação e associação são os mais importantes para o escopo deste trabalho.

2.5.3.1 Beacon

O campo de dados de um pacote *beacon* contém a informação mostrada na tabela 3. É utilizado para troca de informações e capacidades da rede entre estações e pontos de acesso.

Tabela 3 – Conteúdo do pacote *beacon*

Ordem	Informação
1	Timestamp
2	Beacon Interval
3	Capability Information
4	SSID
5	Supported Rates
6	FH Parameter Set
7	DS Parameter Set
8	CF Parameter Set
9	IBSS Parameter Set
10	TIM

2.5.3.2 IBSS ATIM (*Independent Basic Service Set Announcement Traffic Indication Message*)

O campo de dados de um pacote ATIM é nulo. É utilizado para a indicação de tráfego na rede.

2.5.3.3 Desassociação

O campo de dados de um pacote de desassociação contém a informação mostrada na tabela 4. É utilizado para solicitar a desassociação de uma estação. O motivo da operação é o conteúdo do pacote.

Tabela 4 – Conteúdo do pacote desassociação

Ordem	Informação
1	Reason Code

2.5.3.4 Pedido de associação

O campo de dados de um pacote de pedido de associação contém a informação mostrada na tabela 5. É utilizado por uma estação que deseja iniciar o processo para acesso à rede sem fio.

Tabela 5 – Conteúdo do pacote de pedido de associação

Ordem	Informação
1	Capability Information
2	Listen Interval
3	SSID
4	Supported Rates

2.5.3.5 Resposta de associação

O campo de dados de um pacote de resposta de associação contém a informação mostrada na tabela 6. É utilizado por um ponto de acesso em resposta a um pedido de associação.

Tabela 6 – Conteúdo do pacote de resposta de associação

Ordem	Informação
1	Capability Information
2	Status Code
3	Association ID (AID)
4	Supported Rates

2.5.3.6 Pedido de reassociação

O campo de dados de um pacote de pedido de reassociação contém a informação mostrada na tabela 7. É utilizado por uma estação que já está associada a um ponto de acesso.

Tabela 7 – Conteúdo do pacote de pedido de reassociação

Ordem	Informação
1	Capability Information
2	Listen Interval
3	Current AP Address
4	SSID
5	Supported Rates

2.5.3.7 Resposta de reassociação

O campo de dados de um pacote de resposta de reassociação contém a informação mostrada na tabela 8. É utilizado por um ponto de acesso em resposta a um pedido de reassociação.

Tabela 8 – Conteúdo do pacote de resposta de reassociação

Ordem	Informação
1	Capability Information
2	Status Code
3	Association ID (AID)
4	Supported Rates

2.5.3.8 Pedido de sondagem

O campo de dados de um pacote pedido de sondagem contém a informação mostrada na tabela 9. É utilizado por uma estação que deseja iniciar o processo de acesso a rede sem fio.

Tabela 9 – Conteúdo do pacote de pedido de sondagem

Ordem	Informação
1	SSID
2	Supported Rates

2.5.3.9 Resposta de sondagem

O campo de dados de um pacote de resposta de sondagem contém a informação mostrada na tabela 10. É utilizado por um ponto de acesso em resposta a um pedido de sondagem.

Tabela 10 – Conteúdo do pacote de resposta de sondagem

Ordem	Informação
1	Timestamp
2	Beacon Interval
3	Capability Information
4	SSID
5	Supported Rates
6	FH Parameter Set
7	DS Parameter Set
8	CF Parameter Set
9	IBSS Parameter Set

2.5.3.10 Autenticação

O campo de dados de um pacote de autenticação contém a informação mostrada na tabela 11. É utilizado no processo de autenticação.

Tabela 11 – Conteúdo do pacote de autenticação

Ordem	Informação
1	Authentication Algorithm Number
2	Authentication Transaction Sequence Number
3	Status Code
4	Challenge Text

A tabela 12 apresenta os pacotes que levam o desafio WEP em seu conteúdo, dependendo do algoritmo de validação utilizado e da sequência dos pacotes.

Tabela 12 – Aplicabilidade do algoritmo WEP

Algoritmo de autenticação	Número de sequência de autenticação	Texto de desafio ou resposta
OSA	1	Não presente
OSA	2	Não presente
SKA	1	Não presente
SKA	2	Presente
SKA	3	Presente
SKA	4	Não presente

A tabela 13 descreve o tamanho dos campos utilizados no processo de autenticação segundo o padrão IEEE 802.11. O número da terceira coluna é o tamanho do campo de texto que varia a cada sequência, representado em *bits*. Na quarta coluna, este tamanho, já representado em *bytes* é acrescido ao número 34, que indica o tamanho dos cabeçalhos utilizados para o transporte desses dados, sendo 28 *bytes* do cabeçalho do pacote de gerenciamento e mais 6 *bytes* do *frame body*, conforme as figuras 7 e 38. Assim, o tamanho

total de um processo de autenticação no padrão IEEE 802.11 é de 206 *bytes*. Estes valores são amplamente utilizados na seção 5.6 em comparação a proposta deste trabalho.

Tabela 13 – Processo de autenticação no padrão

Seqüência	Texto	Tam. bits	Total Bytes
1	Id estação	48	6+34= 40
2	Desafio WEP	256	32+34= 66
3	Resposta WEP	256	32+34= 66
3	Resultado	0	0+34= 34

2.5.3.11 Desautenticação

O campo de dados de um pacote de desautenticação contém a informação mostrada na tabela 14. É utilizado para que uma referida estação deixe de fazer parte da rede em conjunto com o processo de desassociação.

Tabela 14 – Conteúdo do pacote de desautenticação

Ordem	Informação
1	Reason Code

A tabela 15 apresenta o tamanho dos campos utilizados no processo de desautenticação segundo o padrão IEEE 802.11. De forma análoga à interpretação da tabela 13, o tamanho total de um processo de desautenticação no padrão é de 40 *bytes*.

Tabela 15 – Processo de desautenticação no padrão

Seqüência	Texto	Tam. bits	Total bytes
1	Id estação	48	6+34= 40

3 VULNERABILIDADES DAS REDES LOCAIS SEM FIO

3.1 Introdução

A insegurança das redes locais sem fio é conhecida na comunidade de ciência da computação, sendo considerada de total insegurança. Os padrões IEEE 802.11 e 802.1X bem como os mecanismos de segurança agregados pelos fabricantes elevam o nível de segurança desses ambientes, porém ainda os mantêm vulneráveis a uma série de ataques descritos a seguir.

Existe um grupo de trabalho do IEEE que desenvolve o IEEE 802.11i. No entanto, os resultados deste grupo eram esperados com grande ansiedade pelo mercado, como o 802.11i somente foi publicado no segundo semestre de 2004, os fornecedores, mais uma vez, anteciparam-se ao padrão trabalhando no conjunto WPA (*Wi-Fi Protected Access*). O WPA emprega novos mecanismos de segurança, no entanto, já existem estudos que evidenciam algumas falhas nessa nova implementação, como os mostrados na seção 3.5 e em [Wong 2003].

Na seção 3.2, as vulnerabilidades do padrão IEEE 802.11 são discutidas. De forma análoga, as vulnerabilidades dos mecanismos de segurança agregados pelos fabricantes são discutidas na seção 3.3. Na seção 3.4, as vulnerabilidades do padrão IEEE 802.1X também são discutidas. As fragilidades do WPA são apontadas na seção 3.5. As fragilidades associadas aos mecanismos de administração e gerência dos pontos de acesso são descritas na seção 3.6. Finalmente, na seção 3.7, é exibido o roteiro elaborado para a implementação de

uma invasão contra uma rede local sem fio, concretizada com poucos recursos de *hardware* e *software*.

3.2 Mecanismos de segurança do IEEE 802.11 e suas fragilidades

Sobre o aspecto de segurança, o padrão IEEE 802.11 considera o controle de acesso à rede, a confidencialidade e a integridade dos dados. Ele propõe um modelo de acesso baseado nas três fases: sondagem, autenticação e associação, apresentadas no capítulo anterior. As fases de sondagem e associação estão mais relacionadas à operação do protocolo do que à segurança propriamente dita, que é considerada na fase de autenticação.

A fase de autenticação, quando indica uma validação no modelo OSA, também não agrega segurança ao ambiente. A validação no modelo OSA é uma autenticação nula, permitindo o acesso à rede a qualquer cliente que o solicite. No entanto, quando o modelo SKA é utilizado, é necessário que a estação conheça uma chave pré-compartilhada. O ponto de acesso com o objetivo de validar a estação emite um desafio em texto não criptografado. A estação deve, ao receber esse desafio, criptografá-lo com a chave pré-compartilhada e devolvê-lo ao ponto de acesso, que verifica a validade da chave conhecida pela estação. No caso de sucesso, o acesso desta estação à rede é autorizado. Uma deficiência neste processo de autenticação é que apenas o cliente é autenticado, não existe a autenticação do ponto de acesso perante o cliente.

O padrão IEEE 802.11 utiliza o atributo SSID (*Service Set Identifier*) como um identificador para a rede. Ele é transmitido periodicamente por *broadcast*, e de forma não criptografada. Isto permite que qualquer cliente o capture, mediante a escuta em modo

simples na rede sem fio, e o use quando oportuno. Assim sendo, o SSID não é considerado um mecanismo eficaz de segurança quando implementado desta forma.

Nesse contexto, existe a possibilidade de mapeamento da rede. Tal mapeamento possibilita que os *war drivers* tenham sucesso ao identificar e conseguir informações sobre as redes sem fio. Isto pode ser feito, por exemplo, com um receptor e algum *software* instalado em um *notebook*, fora das instalações onde a rede sem fio está fisicamente instalada.

Como na fase de sondagem os pontos de acesso respondem a qualquer solicitação de informação, a tarefa de mapear a rede é simples e direta, pois qualquer cliente pode obter informações a partir da solicitação direta aos pontos de acesso. Além disso, como o SSID é enviado em texto não criptografado e por *broadcast*, sua leitura também torna-se direta.

O padrão IEEE 802.11 define o protocolo WEP, porém seu uso é opcional e deve ser configurado no ponto de acesso e nas estações. Caso esteja em uso, a mesma chave pré-compartilhada utilizada no processo de desafio/resposta, na fase de autenticação, é utilizada para criptografar os dados em trânsito.

São apresentadas, a seguir, algumas conclusões sobre a efetividade dos mecanismos de segurança identificados até o momento.

No algoritmo OSA, não existe qualquer tipo de controle de acesso. Logo, considerar as fragilidades deste esquema não faz sentido. Nesse cenário, a rede é considerada como pública, pois oferece acesso a qualquer cliente que esteja em sua área de cobertura.

Por outro lado, quando o algoritmo SKA é utilizado, existe uma validação por desafio/resposta utilizando o protocolo WEP. Neste caso, o desafio é enviado em texto não criptografado e pode ser capturado por qualquer cliente que esteja coletando os pacotes na rede de forma promíscua. A resposta ao desafio, embora criptografada, também pode ser capturada. Assim, de posse do texto não criptografado e do texto criptografado, por meio de

operações de ou-exclusivo, tem-se acesso à chave-fluxo. Este é o primeiro passo para a leitura de dados confidenciais e para a quebra da chave WEP, conforme descrito em [Roshan 2002].

Outro problema, já mencionado, é a falta de autenticação do ponto de acesso. É totalmente viável que o invasor insira um ponto de acesso para que este passe por um dos pontos de acesso legítimos da rede. Neste caso, o único objetivo desse falso ponto de acesso é capturar credenciais e informações que deveriam ser confidenciais. Um ponto de acesso pode ser montado em um computador equipado com uma interface sem fio rodando o sistema Linux [Seebach 2003].

A questão dos dados serem protegidos mediante processo de criptografia dos dados, com a mesma e única chave pré-compartilhada, também é um sério risco, pois, devido a falhas no controle de reuso dos vetores de inicialização do protocolo WEP, uma atacante pode, ao capturar um razoável volume de dados, conseguir derivar a chave-fluxo utilizada na comunicação [Silva e Souza 2003].

Esse esquema de comunicação não impede ataques criptográficos do tipo homem-do-meio (*man-in-the-middle*) [Stallings 1998]. Um intruso pode capturar as credenciais de um cliente e se passar por ele. Da mesma forma, o intruso pode se passar por um ponto de acesso.

Várias ferramentas de auditoria e ataques existem. A grande maioria tem distribuição *freeware* e está disponível na Internet juntamente com receitas de como proceder em ataques a esses ambientes. Muitas dessas ferramentas são descritas em [Peikari e Fogie 2003].

3.3 Mecanismos de segurança agregados pelos fabricantes e suas fragilidades

Os principais fabricantes de equipamentos para redes locais sem fio, face às necessidades de segurança do mercado, estão antecipando-se aos padrões e agregando novos

mecanismos de segurança aos seus equipamentos. Entretanto, nem sempre, tais mecanismos são eficazes.

A figura 8, de forma análoga à figura 3, representa as etapas para o acesso à rede local sem fio, porém, com a agregação de dois mecanismos adicionados pelos fabricantes: o uso da “rede fechada” e a filtragem MAC.

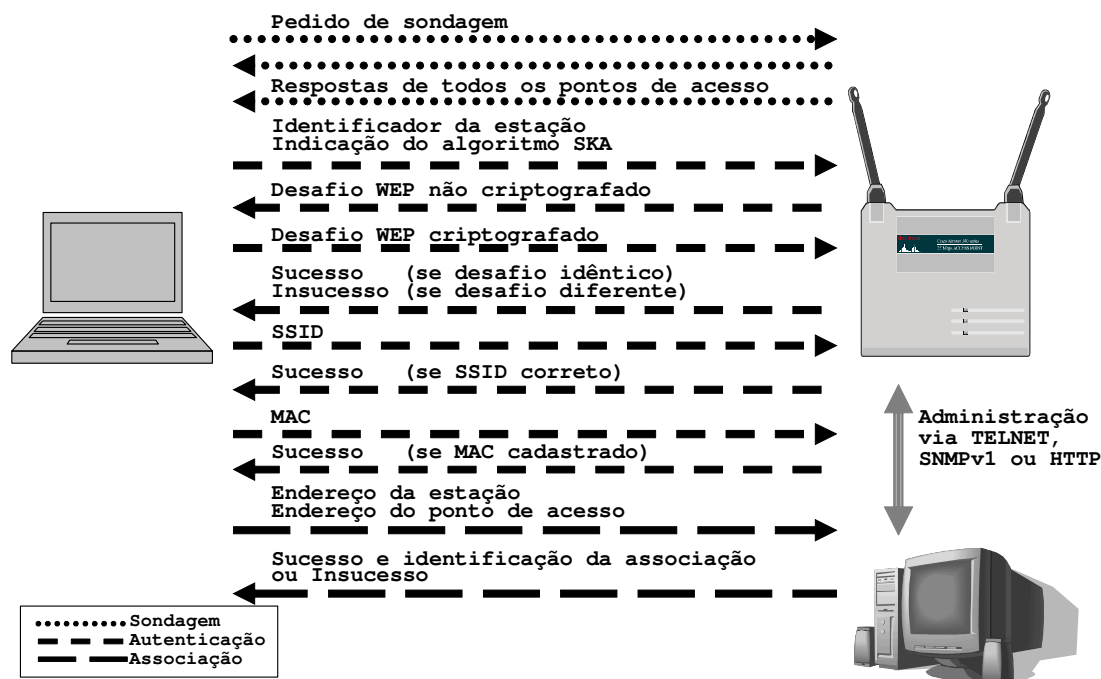


Figura 8 – Conexão à rede local sem fio, padrão 802.11 com mecanismos adicionais

Um dos mecanismos mais utilizados é denominado “rede fechada”, em que não se transmite o SSID por *broadcast*. O SSID é utilizado como uma senha simples, necessária no processo de autenticação. Neste caso, o cliente é solicitado a informar o SSID correto como uma das etapas do processo de autenticação.

Quando um cliente legítimo percorre o processo de autenticação, de acordo com a figura 8, ele deve enviar o SSID de forma não criptografada, conforme a oitava linha da figura

8, o que possibilita sua captura e posterior utilização. Desta maneira, o SSID não resolve o problema do nível de segurança do sistema.

Outro mecanismo considerado é a filtragem de endereços MAC. Como mais uma etapa no processo de autenticação, o endereço MAC do cliente é verificado contra uma base de endereços MAC autorizados. Esta base pode ser armazenada em cada ponto de acesso ou de forma centralizada, em um servidor RADIUS (*Remote Authentication Dial-In User Service*).

Embora pareça, a filtragem MAC não é a solução para os problemas de acesso indevido às redes locais sem fio. Como os endereços MAC podem ser falsificados e alterados com facilidade um invasor pode capturar um endereço MAC cadastrado por meio da captura de pacotes na rede. Em seguida, ele pode alterar o endereço MAC de sua interface de rede sem fio para o endereço MAC capturado, burlando, assim, este mecanismo no acesso à rede [Huey 2003] e [Etter 2002].

Existem outros mecanismos, no entanto a maioria deles são baseados nesses princípios. Os fabricantes atualizam e criam novos mecanismos com muita dinamicidade, entretanto, a maioria deles, embora agreguem um pouco em termos de segurança dificultando ataques, não resolvem os problemas existentes.

3.4 Mecanismos de segurança do IEEE 802.1X e suas fragilidades

O padrão IEEE 802.1X prevê o controle de acesso por porta a toda a família IEEE 802 e também pode ser utilizado para as redes locais sem fio. Porém existe uma grande diferença entre as redes locais sem fio e as demais redes cabeadas da família 802. Nas redes

cabeadas, a ligação entre o cliente e sua porta de acesso é definida por um cabo fisicamente conectado às duas partes e, no caso das redes locais sem fio, esta ligação não existe de forma física. Assim sendo, o padrão falha justamente em não definir os aspectos de segurança nesse tipo de conexão, sendo possível a captura, adulteração e repetição de pacotes de validação. A segurança dos dados, quando em trânsito entre o cliente e o ponto de acesso, fica a cargo das implementações dos fabricantes, já que não é prevista no padrão. Em [Mishra e Arbaugh 2002], é feita uma análise dos aspectos de segurança do 802.1X, na qual são exibidas algumas possibilidades de ataques contra o padrão.

O padrão IEEE 802.1X considera um servidor de autenticação, muitas vezes denominado por *backend server*. O ponto de acesso pode tornar-se um repassador de pacotes de autenticação dado que toda a base é armazenada no servidor de autenticação. Geralmente, o papel de autenticador é definido em servidores especializados, como, por exemplo, servidores RADIUS. O ponto de acesso traduz os pacotes que recebe do cliente no formato definido para pacotes no protocolo de validação, por exemplo, RADIUS, e no sentido inverso também.

A validação de usuário e senha por intermédio do protocolo RADIUS pode ser realizada de várias maneiras, como mostrado em [ORINOCO 2003]. Quando utilizada sem mecanismos adicionais de criptografia, as credenciais do usuário trafegam entre o cliente e o ponto de acesso de forma não criptografada, pois o protocolo RADIUS é implementado somente entre o ponto de acesso e o autenticador. Neste último trecho, as credenciais estão criptografadas pela chave do próprio RADIUS.

Quando as credenciais trafegam de forma não criptografada pela rede, elas podem ser facilmente capturadas e oportunamente utilizadas, ataques do tipo seqüestro de sessão ou homem-do-meio também são viáveis. Contudo, mesmo quando recursos adicionais protegem essas credenciais, ainda existem problemas. Isto ocorre porque ainda é possível capturar tais

credenciais e, mesmo sem poder interpretá-las, o invasor pode utilizá-las oportunamente, caracterizando um ataque por repetição.

Embora o padrão IEEE 802.1X não contemple a distribuição automática de chaves de sessão, alguns fornecedores agregaram, de forma proprietária, essa distribuição com o intuito de minimizar os impactos do uso das chaves pré-compartilhadas. A distribuição periódica de chaves de sessão, praticamente, elimina os riscos associados ao uso de chave pré-compartilhada e diminui os perigos advindos das fragilidades do protocolo WEP. Entretanto, para ser eficaz, o mecanismo de troca de chave de sessão deve estar associado a processos de reautenticação, com geração e distribuição de novas chaves de forma periódica. No entanto, a maioria dos produtos comerciais, não implementam essa funcionalidade de forma automática.

Certamente, o uso do 802.1X eleva o nível de segurança da rede, no entanto, seu maior dificultador é o fato da necessidade de um servidor de autenticação, muitas vezes, não disponível em ambientes menores, e com isso, o 802.1X não é implementado.

3.5 Mecanismos de segurança do WPA e suas fragilidades

O WPA é um padrão de mercado, fruto do trabalho da *Wi-Fi Alliance*, uma organização sem fins lucrativos, fundada em 1999, que atesta os produtos *wireless* de acordo com o padrão WPA. Mais de 600 produtos estão certificados pela *Wi-Fi Alliance* [Wong 2003]. O objetivo do WPA é sanar as vulnerabilidades conhecidas do protocolo WEP, agregando maior segurança e possibilitando a utilização do mesmo *hardware* atualmente utilizado. O WPA pode ser considerado como um sub-conjunto do IEEE 802.11i, que objetiva melhorar ainda mais o nível de segurança.

O WPA aproveita o baixo consumo de recursos computacionais e o bom desempenho do WEP, porém propõe mecanismos diferenciados, a fim de sanar as falhas do WEP. Neste caso, apenas a atualização de *firmware* e *software* é suficiente, sem a necessidade de atualização de *hardware*.

São três as principais funcionalidades do padrão WPA:

3.5.1 Reforço no controle de acesso

Com o 802.1X EAP (*Extensible Authentication Protocol*), previsto no IEEE 802.1X, o sistema abstrai o mecanismo de autenticação. Desta forma, o ponto de acesso não precisa conhecer os detalhes do processo de autenticação, podendo apenas repassar os pacotes de autenticação entre a estação e o servidor de validação, que devem trabalhar com o mesmo mecanismo de autenticação.

Existem alguns tipos de EAP utilizados atualmente: LEAP, desenvolvido pela Cisco, o TLS, descrito na RFC 2716, o TTLS, desenvolvido pela Funk *Software* e outros.

O WPA prevê, para ambientes SOHO (*Small Office Home Office*), a não utilização do protocolo 802.1X, pois em ambientes pequenos a dedicação de um servidor de autenticação poderia ser inviável. Para estes casos, o WPA prevê a utilização de chave pré-compartilhada, PSK (*Pre Shared Key*) entre os clientes e pontos de acesso.

3.5.2 Reforço na garantia da confidencialidade

O TKIP (*Temporal Key Integrity Protocol*) é a opção encontrada para prover um bom nível de segurança, mantendo a compatibilidade de *hardware*. O TKIP é também baseado no RC4 e é formado por: uma chave pré-compartilhada, de 128 *bits*, entre os clientes e pontos de acesso, o endereço MAC da estação e um vetor de inicialização de 48 *bits*. A chave temporal

é trocada a cada 10.000 pacotes; o mecanismo de troca da chave temporal ainda não é padronizado, criando a possibilidade de brechas em implementações específicas.

3.5.3 Reforço na garantia da integridade

O WPA padroniza o uso do Michael MIC (*Message Integrity Check*), em substituição ao CRC32, melhorando a garantia da integridade dos dados em trânsito, o Michael é uma função *hash* com saída de 64 *bits*.

O WPA não deve ser definido como a solução final para as redes locais sem fio, mas, sim, como um adiantamento ao padrão 802.11i, que eleva o nível de segurança, todavia nem todos os equipamentos são compatíveis.

Mesmo sendo o padrão mais recente, o WPA ainda revela algumas vulnerabilidades, menos sérias do que as vulnerabilidades do WEP. Elas também podem ser exploradas no sentido de quebrar a segurança do ambiente ou, então, com o objetivo de negação de serviço.

Uma das vulnerabilidades está no algoritmo utilizado para a garantia da integridade [Stone 2003] e [Deshpande 2003]. O algoritmo Michael possui um mecanismo de proteção que, ao receber mais de um pedido de mesma origem repetidamente, desativa temporariamente sua operação. Esse mecanismo foi desenvolvido para eliminar a possibilidade de mapeamento e força bruta. Entretanto ele pode facilmente ser utilizado para provocar um ataque de negação de serviço. Para isto, basta que o invasor transmita dois pacotes a cada minuto, assim, o sistema fica permanentemente desativado, e a detecção e a identificação do invasor são difíceis, pois o volume de pacotes é pequeno, ao contrário da maioria dos ataques de negação de serviço [Moskowitz 2003].

Sob alguns pontos de vista, essa não é uma vulnerabilidade séria, posto que qualquer rede sem fio é vulnerável a ataques de negação de serviço, com interferência física no sinal. No entanto, quando se analisa a viabilidade e a facilidade do ataque percebe-se que é mais

fácil e direta a implementação do ataque ao algoritmo Michael, pois, para o ataque de interferência, é necessário um potente transmissor, e a identificação do agressor é mais simples.

Outra vulnerabilidade tem relação com o uso das chaves compartilhadas, em especial, em ambientes SOHO que não dispõem de um servidor de autenticação, conseqüentemente, não fazendo uso do protocolo 802.1X EAP.

A vulnerabilidade não está associada diretamente ao protocolo TKIP do WPA, mas à interface, que permite a inserção da frase secreta. Com o uso de uma frase secreta com menos de 20 caracteres baseados em dicionário, é possível efetuar a quebra de forma passiva. Um invasor pode capturar uma sessão de autenticação legítima na rede e para que o invasor não tenha que esperar um cliente legítimo da rede solicitar acesso, ele pode forjar um pedido de desassociação para uma estação qualquer que, em seguida, se associará novamente. Para isto, basta que o invasor esteja no raio de cobertura da rede por alguns minutos.

Desta forma, como as interfaces de manipulação da frase secreta não verificam a sua qualidade, a possibilidade de uso de senhas inadequadas existe e é agravada pelo fato de que esta frase terá que ser inserida em cada estação participante da rede e, com isso, muitas vezes, utilizam-se chaves mais simples em favor da facilidade e em detrimento da segurança. Neste caso, a quebra da confidencialidade do sistema pode ser conseguida mais facilmente do que em uma rede WEP, contudo, em uma rede WEP, a quebra pode ser feita independente da qualidade das chaves utilizadas, o que é ainda mais grave.

Embora se espere que apenas ambientes SOHO não utilizem o 802.1X EAP, certamente, existem vários ambientes corporativos que utilizam o WPA sem a implementação deste mecanismo, o que eleva a criticidade dessa vulnerabilidade.

3.6 Administração e gerência dos pontos de acesso e suas fragilidades

O padrão IEEE 802.11 é omissivo quanto à forma de administração dos pontos de acesso. Neste caso, cada fabricante determina um tipo de acesso e interface em seu equipamento para que este possa ser administrado e gerenciado.

A maioria dos equipamentos disponíveis no mercado são administrados remotamente via rede. Tais equipamentos podem ser configurados para permitir sua administração via interfaces sem fio ou por aquelas conectadas à rede cabeada, quando existentes. Uma deficiência de tais esquemas é que, freqüentemente, são utilizados protocolos sem funcionalidades de garantia de confidencialidade. Exemplos incluem o TELNET, SNMPv1 (*Simple Network Management Protocol version 1*) e HTTP (*HyperText Transfer Protocol*). Nenhum destes protocolos provê a criptografia dos dados. Logo, propiciam a um invasor a captura do tráfego de administração. A partir deste tráfego, pode-se extrair chaves definidas no equipamento, credenciais para administração e gerência dos equipamentos, além de outros detalhes da rede.

Alguns fornecedores já adotam protocolos alternativos, que provêem a proteção da confidencialidade e integridade dos dados no ar. Exemplos incluem o SSH (*Secure Shell*), SNMPv3 (*Simple Network Management Protocol version 3*) e HTTPS (*Hypertext Transfer Protocol Secure*).

3.7 Um teste de invasão em uma rede baseada no padrão IEEE 802.11

Esta seção exibe e discute um roteiro que pode ser utilizado para invadir uma rede no padrão IEEE 802.11 com alguns mecanismos adicionais de segurança. Este roteiro permite o acesso de um invasor à rede sem fio e, caso exista, à rede cabeada conectada à rede sem fio.

Basicamente o teste de invasão consiste em alterar o *driver* da interface de rede sem fio e fazer um processo de *downgrade* no *firmware* da interface para que seja possível a escuta em modo promíscuo e a alteração do endereço MAC. Após esta preparação o primeiro passo é procurar e identificar uma rede sem fio. Uma vez que a rede tenha sido mapeada, um endereço MAC precisa ser capturado e com isso pode-se coletar a quantidade necessária de tráfego para que em seguida o processo de quebra da chave pré-compartilhada possa ser executado. De posse das informações da rede, do endereço MAC e da chave, basta configurar a interface de rede como um cliente legítimo, identificar um endereço IP e máscara para serem usados e o ataque está concluindo fornecendo acesso e conectividade total na rede local sem fio.

O roteiro descrito nesta seção tem como base os trabalhos [Huey 2003] e [Etter 2002], e foi implementado em ambiente de testes para a elaboração desta seção.

3.7.1 Preparando-se para o teste de invasão:

A preparação para o teste de invasão não é complexa e requer poucos recursos em termos de *hardware*, apenas um *notebook* equipado com uma interface sem fio é suficiente.

A ação realizada em ambiente de laboratório, cujos resultados são apresentados a seguir, utilizou os seguintes equipamentos:

Notebook Toshiba P4 2.2Ghz com 512M de memória RAM

Interface de rede sem fio Lucent Orinoco Gold 11Mbps

Sistema Operacional Microsoft Windows 2000 Professional e Linux RedHat 7.3.

A preparação do equipamento e sistema consiste em dois passos: instalação customizada da interface sem fio e instalação de *software* necessário, como descrito a seguir:

3.7.1.1 Instalação customizada da interface sem fio

A instalação da interface de rede sem fio é muito importante e não segue os roteiros normais de instalação, geralmente, publicados nos manuais e *sites* de fabricantes. Se instalada da forma padrão, a interface não será capaz de efetuar duas funções essenciais ao teste de invasão: captura de pacotes em modo promíscuo e habilidade de alterar o endereço MAC.

Ao instalar a interface fisicamente no *slot* PCMCIA (*Personal Computer Memory Card International Association*), o Windows 2000 irá detectar e instalar o *driver* do sistema.

Embora os *drivers* nativos do Windows 2000 sejam adequados para a correta operação da interface em rede, são inadequados às ações deste teste de invasão. A tela de propriedade do *driver* embutido do Windows 2000 é exibida na figura 9.



Figura 9 – Tela de propriedades do *driver* do Windows para uma interface Orinoco

Para que as funções antes descritas sejam habilitadas, é necessário que o *firmware* da interface seja alterado em um processo de *downgrade*, e o *driver* da interface de rede sem fio do Windows 2000 deve ser substituído por uma versão adulterada.

O *firmware* e *software* recomendado para essa interface é a versão distribuída no inverno de 2001, empacotada como R64.winter2001 [Orinoco 2002]. O processo de atualização do *firmware* da interface de rede é exibido nas figuras 10, 11 e 12.

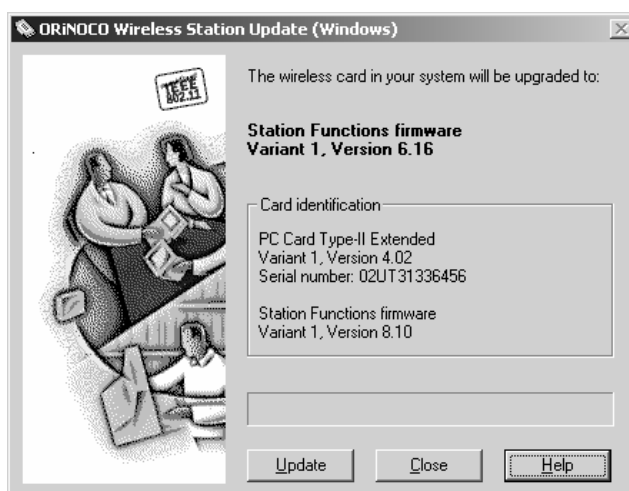


Figura 10 – Tela de abertura do processo de atualização



Figura 11 – Tela de confirmação do processo de *downgrade*



Figura 12 – Tela de confirmação da atualização com sucesso

Após o *firmware* ter sido atualizado, ainda é necessária a aplicação de um *patch*, que adultera o *driver* original do Windows 2000. O *patch* WildPackets AiroPeek [Agere 2002] deve ser instalado, tornando a interface de rede totalmente capacitada às ações do teste de invasão. A tela de propriedades do novo *driver* é exibida na figura 13.



Figura 13 – Tela de propriedades do *driver* alterado

Após o processo de atualização e instalação do *driver* adulterado, as versões em operação devem ser idênticas às exibidas na figura 14.

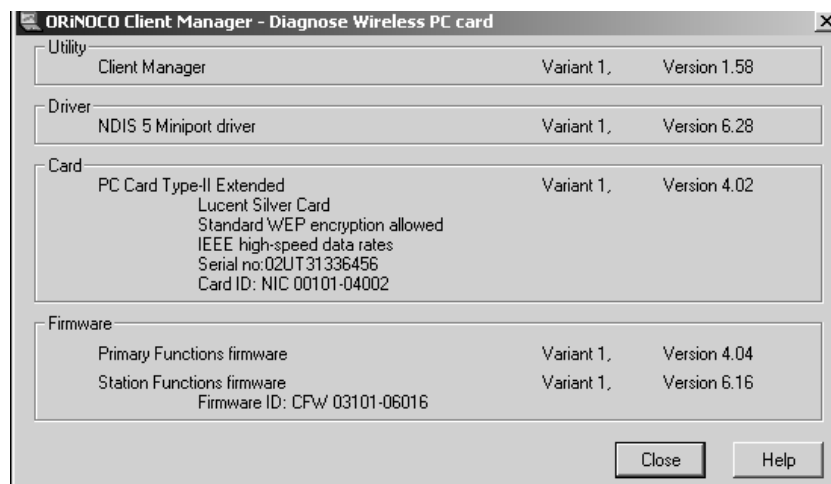


Figura 14 – Tela do controlador Orinoco com as versões em uso

A configuração da interface sem fio no sistema Linux pode seguir as orientações do fabricante da interface, pois nenhum procedimento adicional é necessário.

3.7.1.2 Instalação de *software sniffer* 802.11

Existem vários *sniffers* para redes IEEE 802.11, sendo que muitos são produtos comerciais e de alto custo, no entanto existem ferramentas *freeware* que podem ser utilizadas para esta finalidade e que foram empregadas nesse teste de invasão.

As ferramentas Windump [Lawrence 2004] e Ethereal [Combs 2004] foram, originalmente, desenvolvidas para sistemas UNIX, baseados na biblioteca libcap [Lawrence 2002], mas, com o desenvolvimento da biblioteca winpcap [Lawrence 2002], surgiram versões dessas ferramentas para o ambiente Windows. Desta forma, antes de instalar o Windump ou Ethereal, é necessária a instalação do winpcap, todos *freeware*, mesmo para Windows.

Ainda existe uma outra necessidade, pois o Windump ou Ethereal somente operam após a associação do cliente na rede. Assim, se a rede implementar mecanismos como criptografia WEP, eles não poderão ser utilizados para sua quebra.

No entanto, existem outros *sniffers* capazes de promover a quebra da chave WEP, por exemplo, o AirSnort [Shmoo 2002] e o WepCrack [Rager 2002], que rodam em sistemas UNIX.

O sistema operacional Linux RedHat 7.3 também está instalado no mesmo *notebook* e, com os *drivers* da interface de rede configurados, pode rodar o AirSnort. Isto foi feito nesse roteiro de invasão, para a coleta de tráfego e conseqüente quebra da chave WEP.

O AirSnort precisa capturar de 500Mbits a 1Gbits de tráfego para a quebra da chave WEP, e o tempo necessário para esta coleta depende da carga de tráfego na rede. A quantidade de tráfego e tempo de quebra independe se as chaves utilizadas têm 64 ou 128 *bits*, posto que o tamanho do vetor de inicialização é idêntico nos dois casos: 24 *bits*, e a falha explorada está justamente na formação e uso do vetor de inicialização, conforme descrito no capítulo 4.

3.7.1.3 Instalação de um localizador de pontos de acesso

Se a topologia da rede já é conhecida, não é necessária a instalação de um localizador de pontos de acesso.

Caso não se conheça a topologia da rede, a ferramenta NetStumbler [Milner 2002] pode ser utilizada para a localização dos pontos de acesso.

3.7.2 Iniciando o teste de invasão

Com todo o equipamento em mãos e todo o *software* instalado e configurado, o teste pode ser iniciado.

Primeiramente, deve-se procurar por uma rede ou pontos de acesso, para isso, deve-se iniciar o NetStumbler, que faz requisições de *broadcast* no ar. Ele exhibe as respostas, indicando os pontos de acesso, seus endereços MAC, a relação sinal/ruído, o SSID, o

fabricante e se o protocolo WEP está em uso ou não. A figura 15 mostra o resultado da execução do NetStumbler.

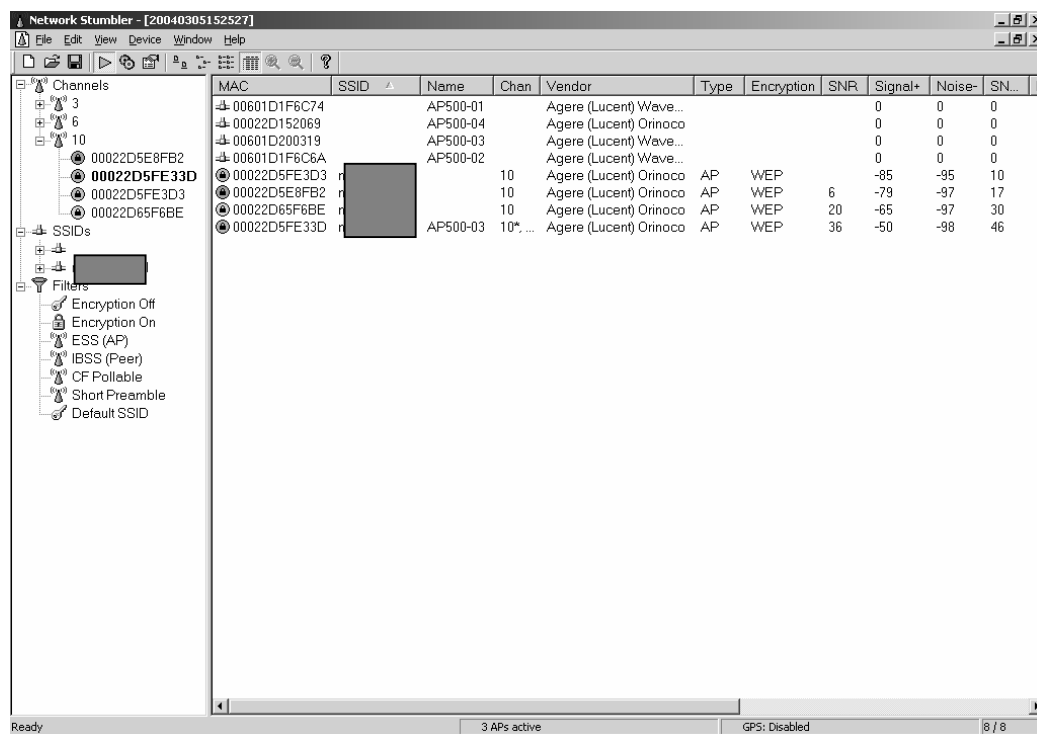


Figura 15 – Tela do NetStumbler mapeando a rede utilizada no teste de invasão

Caso a rede esteja configurada de modo a não responder a requisições de *broadcast*, outro *software* pode ser utilizado: o Kismet [Kershaw 2003]. A diferença deste *software* é que ele não envia requisições. Ele é passivo e somente captura os pedidos e respostas de clientes legítimos da rede e exibe os mesmos detalhes. Por ser passivo, ele é mais lento do que ferramentas ativas, como o NetStumbler.

Na rede utilizada como alvo para esse teste de invasão, existe um mecanismo adicional de segurança, a filtragem MAC. Assim, este mecanismo também foi considerado neste roteiro. Logo, é hora de capturar um endereço MAC válido, de preferência em um processo de desassociação, pois, por estar neste processo, o MAC capturado não mais estará em uso na rede naquele momento, evitando conflitos e facilitando a ação do invasor.

A captura do endereço MAC é feita com o *software* Airopeek, que coleta tráfego na rede, em modo espião, mesmo antes do processo de associação da rede sem fio. A figura 16 mostra o conteúdo de um pacote capturado com o AiroPeek.

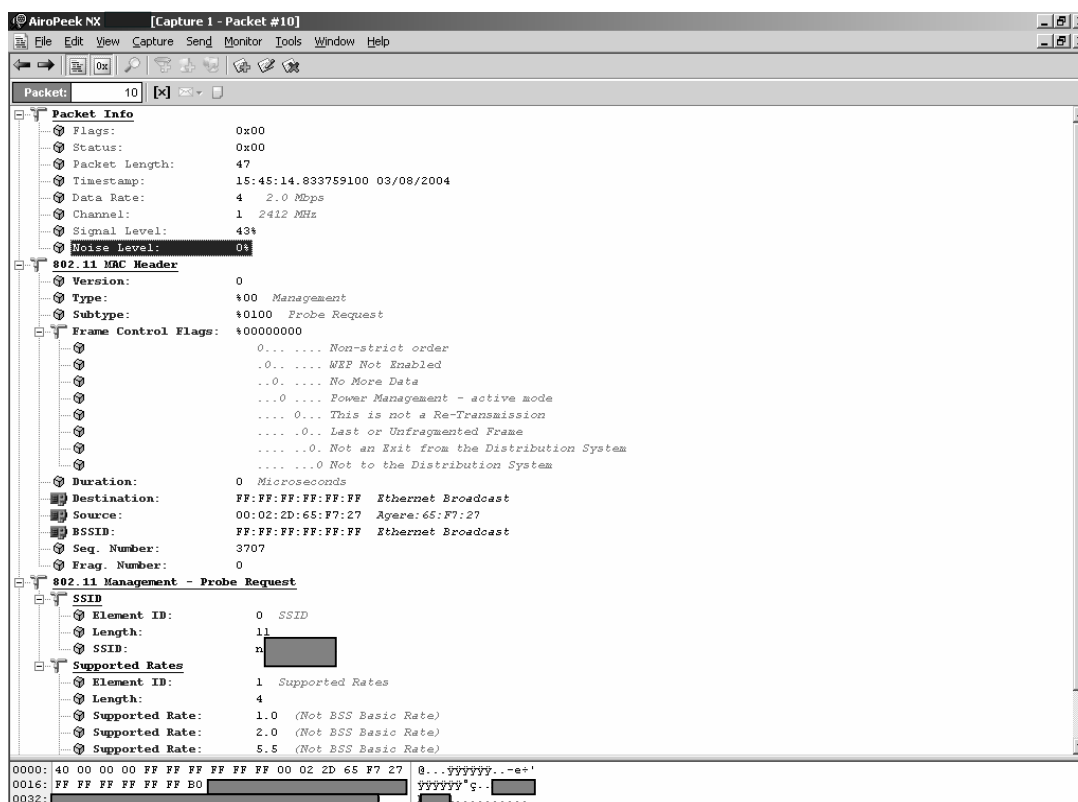


Figura 16 – Tela do AiroPeek exibindo o conteúdo de um pacote capturado

De posse deste MAC, deve-se configurá-lo na interface sem fio. Esta alteração é possível devido ao *driver* adulterado, instalado na fase de preparação e ao uso do programa adequado. A figura 17 exibe a tela do *software* MAC MakeUp [Gorlani 2003], que foi utilizado para a troca do endereço MAC.

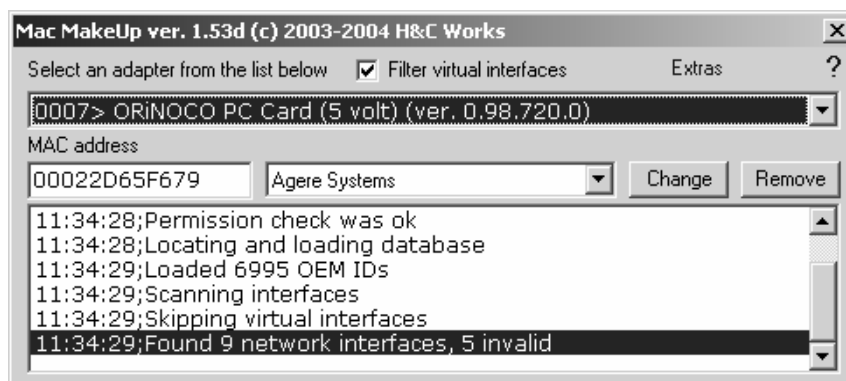


Figura 17 – Tela do MAC MakeUp alterando o MAC da interface sem fio

Resolvida a barreira da filtragem MAC e supondo que a rede esteja utilizando o protocolo WEP, é hora de coletar o tráfego necessário para a quebra da chave WEP. Para isso, basta sair do Windows e iniciar o *notebook* no sistema operacional Linux e iniciar o aplicativo AirSnort, que fará a coleta e quebra da chave WEP conforme a figura 18.

A versão do AirSnort utilizada neste teste é a versão 0.0.9 em modo texto. Esta versão é composta por 2 aplicativos: o *capture*, que coleta tráfego na rede sem fio, e o *crack*, que faz a análise e quebra do tráfego coletado conforme a figura 19.

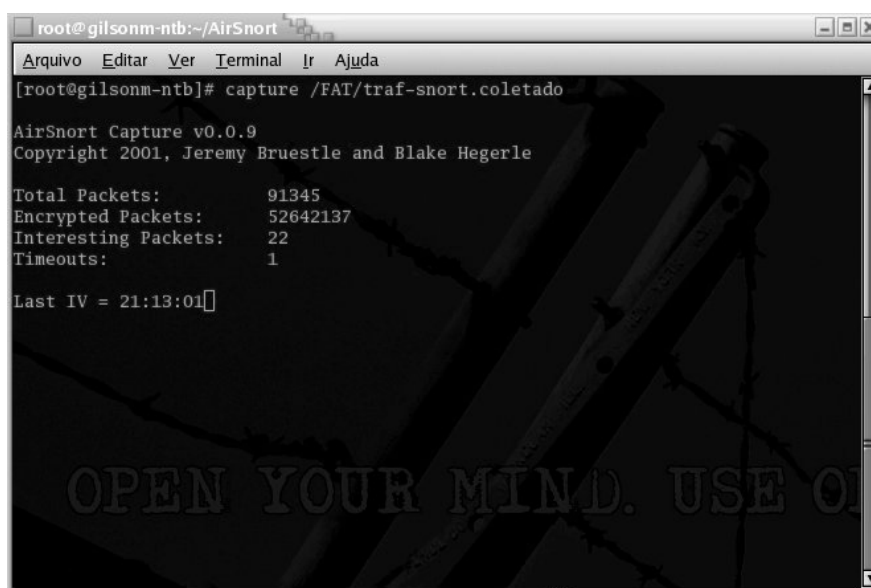


Figura 18 – Tela do AirSnort capturando tráfego na rede

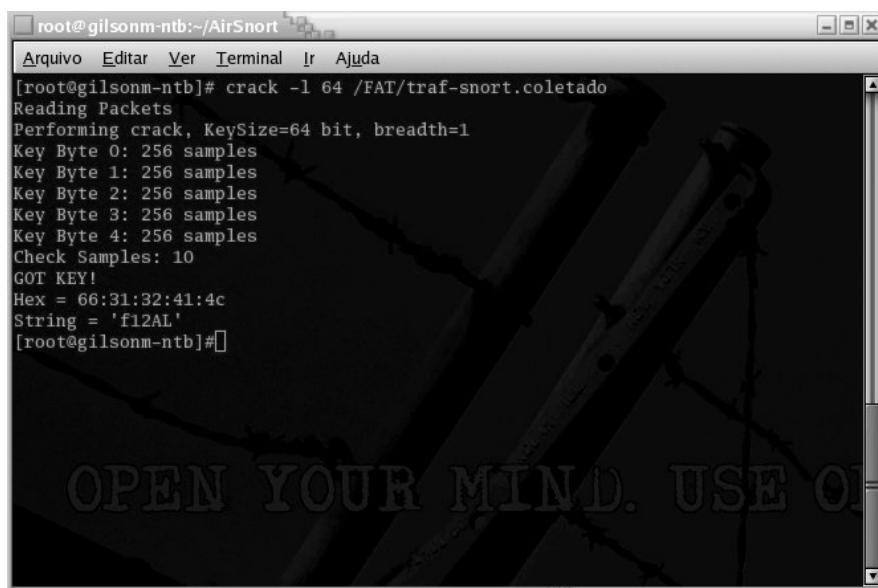


Figura 19 – Tela do AirSnort ao término do processo de quebra da chave WEP

Com a chave em mãos, é hora de configurar o *notebook*, como um cliente normal, conforme a figura 20, pois já se têm as informações necessárias, incluindo SSID e chave WEP, além de um endereço MAC válido.

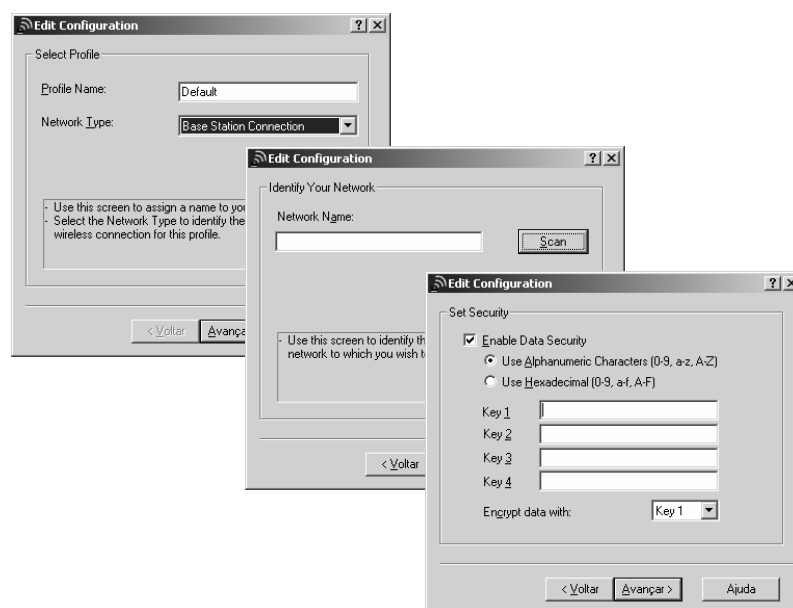


Figura 20 – Telas de configuração do cliente da interface sem fio

A interface sem fio pode ser configurada de modo a obter um endereço IP automaticamente através da rede sem fio. Logo, se a rede estiver configurada para o uso do protocolo DHCP (*Dynamic Host Configuration Protocol*), a interface sem fio, ao receber um IP, já está apta a se comunicar na rede, obtendo conectividade no nível IP.

No entanto, esse roteiro supõe o caso mais complexo, em que não existe a distribuição de endereços IP através de um servidor DHCP. Neste caso, a interface do *notebook*, mesmo se associando à rede sem fio, não tem conectividade no nível IP. Para isto, é necessário que um endereço, máscara e *gateway* sejam configurados na interface sem fio.

Para a descoberta do esquema de endereçamento da rede, utiliza-se um dos *sniffers* anteriormente citados: Wireshark ou Ethereal, ambos podem coletar tráfego na rede, revelando as faixas de endereços utilizadas, bem como possíveis roteadores. Neste teste, foi utilizado o Ethereal conforme a figura 21.

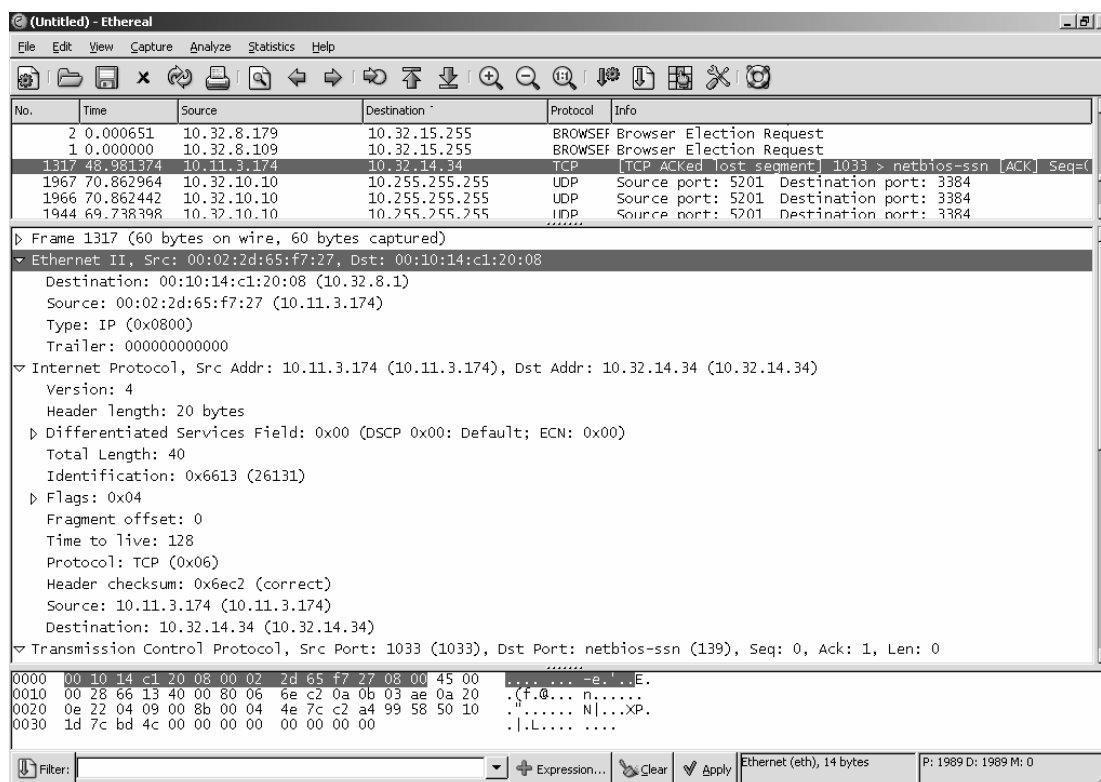


Figura 21 – Tela do Ethereal exibindo o conteúdo de uma pacote capturado

De posse dessas informações e com um razoável conhecimento da pilha de protocolos TCP/IP, pode-se analisar os pacotes coletados, obtendo-se os detalhes necessários. Assim, basta que um endereço IP e máscara sejam configurados e o *notebook* já tem conectividade no nível IP. A partir daí, praticamente, qualquer ataque conhecido é viável, desde um DoS (*Denial of Service*) do tipo *Syn Flood* a uma exploração de uma vulnerabilidade em um servidor. Os impactos das próximas ações nem mesmo podem ser determinados, pois dependem da existência e qualidade de outros mecanismos de proteção e monitoração implementados no ambiente e do conhecimento e determinação do invasor.

4 OS PROTOCOLOS RC4 E WEP

4.1 Introdução

Este capítulo mostra as principais características dos protocolos de criptografia simétrica RC4 e WEP, bem como as fraquezas do protocolo WEP. O protocolo WEP é baseado no RC4 e é utilizado no padrão IEEE 802.11.

A seção 4.2 expõe os conceitos e aplicabilidades dos cifradores de bloco e de fluxos e ainda trata os modos de operação destes cifradores. A seção 4.3 dá uma visão geral do protocolo RC4, enquanto a seção 4.4 exhibe uma visão geral do protocolo WEP. Finalmente, a seção 4.5 indica as vulnerabilidades e fraquezas do protocolo WEP.

4.2 Cifradores de bloco, cifradores de fluxo e modos de criptografia

Existem duas formas de transformar textos não criptografados em textos criptografados: por intermédio de blocos ou através de um fluxo contínuo. A forma mais adequada depende do tipo do dado a ser tratado, por exemplo: um arquivo texto ou mensagem de e-mail podem ser tratados em blocos, pois o computador assim já os trata. No entanto, uma mensagem de voz deve ser tratada na forma de um fluxo contínuo ao contrário de ser separada em blocos de tamanhos fixos. Assim, existem os cifradores de bloco e os cifradores de fluxo, que, embora tenham o mesmo propósito, possuem algumas diferenças em suas estruturas.

4.2.1 Cifradores de fluxo

Os cifradores de fluxo criptografam os dados, gerando a chave-fluxo com base na chave e efetuando um ou-exclusivo entre o texto não criptografado e esta chave-fluxo. Assim, o tamanho da chave-fluxo deve ser variável e sempre igual ao tamanho do dado a ser transformado.

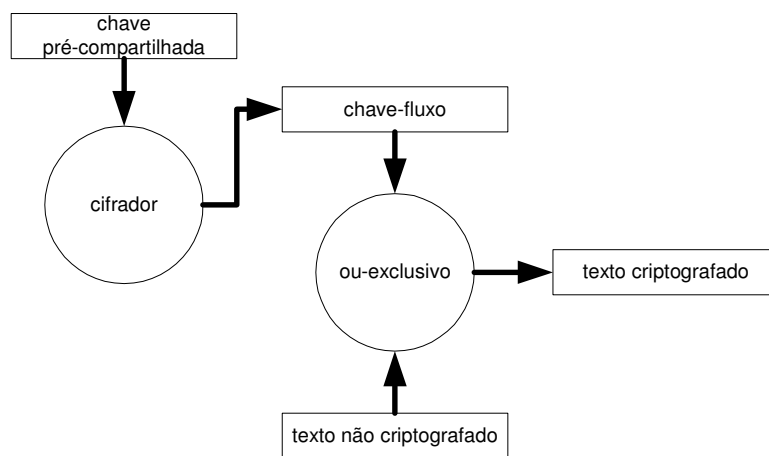


Figura 22 – Esquema de um cifrador de fluxo

A figura 22 descreve o esquema de um cifrador de fluxo. Uma função de criptografia é aplicada à chave pré-compartilhada que gera a chave-fluxo. Em seguida, a chave-fluxo é utilizada na função ou-exclusivo com o texto não criptografado, resultando no texto criptografado.

4.2.2 Cifradores de bloco

Os cifradores de bloco tratam as informações em blocos, ao contrário de quadros de tamanhos variáveis. Esses cifradores dividem os dados em blocos de tamanho fixo e, se necessário, executam o preenchimento do último bloco, a fim de transformá-lo em um bloco do mesmo tamanho dos demais.

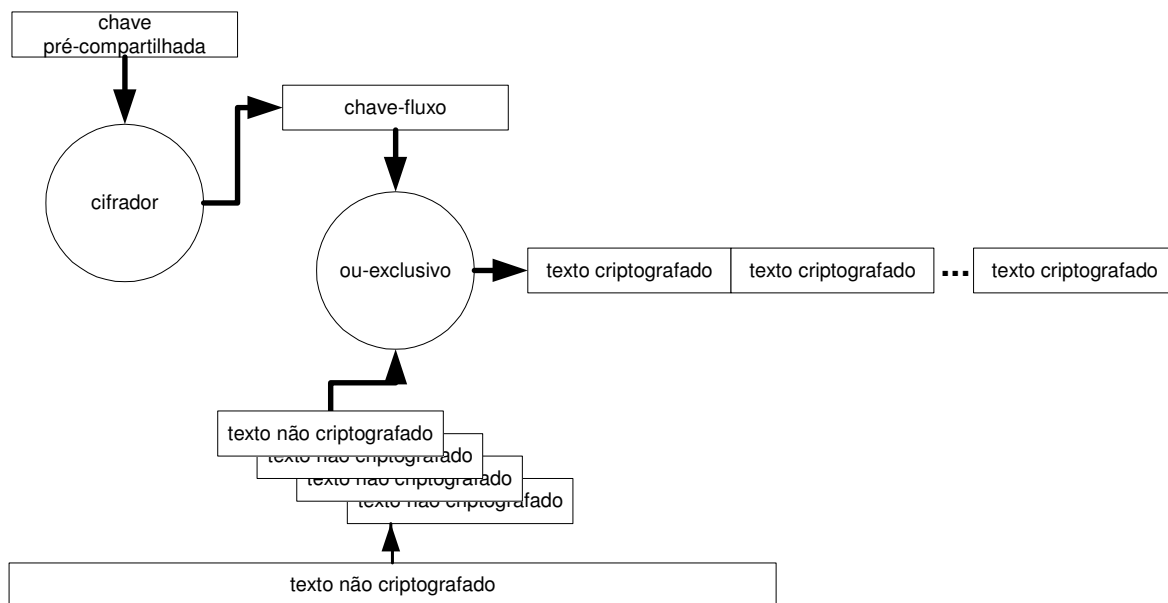


Figura 23 – Esquema de um cifrador de blocos

A figura 23 exibe a estrutura de um cifrador de bloco, em que a chave pré-compartilhada também é submetida a uma função de criptografia, que gera uma chave-fluxo do tamanho de cada bloco. Cada bloco é submetido, em separado, ao ou-exclusivo com a chave-fluxo, resultando em uma sequência de blocos criptografados.

4.2.3 Modos de operação

O modo de operação das estruturas exibidas, tanto para os cifradores de fluxo quanto para os cifradores de bloco é chamada de ECB (*Electronic Code Book*) [Stallings 1998]. Utilizando o ECB, o mesmo texto não criptografado sempre gera o mesmo texto criptografado. Este é um fato que pode ser explorado por criptoanalistas, que podem avaliar padrões de tráfego na rede e iniciar um processo de tentativa de adivinhações. Para sanar esta potencial vulnerabilidade, existem outras duas opções ao ECB: os vetores de inicialização e os modos com retroalimentação, que são detalhados a seguir.

4.2.3.1 Vetores de Inicialização

O vetor de inicialização, geralmente referenciado por IV (*Initialization Vector*), é utilizado para alterar a chave-fluxo. Ele é um valor numérico que é concatenado à chave antes da chave-fluxo ser gerada. Os esquemas com vetores de inicialização são, geralmente, utilizados com cifradores de fluxo. O IV é alterado a cada momento, portanto, a chave-fluxo é sempre diferente, o que resultará em textos criptografados diferentes, mesmo para textos não criptografados idênticos.

O padrão IEEE 802.11 usa vetores de inicialização no protocolo WEP e recomenda, mas não obriga, que o IV seja alterado a cada pacote. Assim, se um mesmo quadro de rede for transmitido duas ou mais vezes, o texto criptografado que trafega pela rede será diferente. O padrão ainda define o IV com tamanho de 24 *bits*, independente do tamanho de chave utilizada, e define ainda que o IV deve trafegar no cabeçalho do quadro de rede de forma não criptografada. Isto ocorre para que o receptor possa identificar o IV utilizado no processo de criptografia para que a correta decriptografia ocorra.

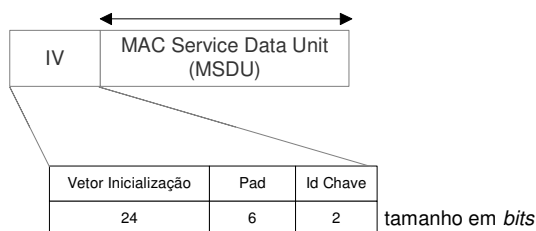


Figura 24 – Esquema de um quadro de rede com os detalhes do vetor de inicialização

A figura 24 exibe o esquema de um quadro de rede no padrão IEEE 802.11 e abre o campo do vetor de inicialização em mais detalhes, onde são exibidos os 24 *bits* do vetor de inicialização, 6 *bits* de preenchimento e o identificador da chave utilizada.

4.2.3.2 Modos com retroalimentação

Assim como os vetores de inicialização, os modos com retroalimentação têm o propósito de evitar que textos não criptografados iguais gerem o mesmo texto criptografado. Geralmente, são utilizados em cifradores de bloco. Existem 3 modos diferentes de operação com retroalimentação [Ferguson 2003]: CBC (*Cipher Block Chaining*), CFB (*Cipher Feedback*) e OFB (*Output Feedback*). O modo mais comum é o CBC.

A filosofia do CBC é descrita na figura 25 e consiste em efetuar o ou-exclusivo entre um bloco de texto não criptografado com a saída de texto criptografado do bloco anterior. Como esta filosofia não se aplica ao primeiro bloco, é utilizado um vetor de inicialização para o primeiro bloco, objetivando alterar o texto criptografado relativo ao primeiro bloco de texto não criptografado.

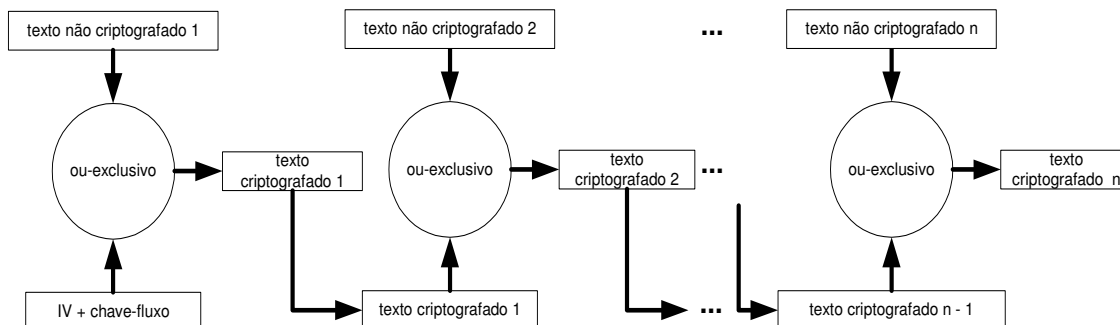


Figura 25 – Esquema do modo de operação CBC

Os outros modos são semelhantes ao CBC, mas têm particularidades que auxiliam na escolha do modo de operação com base no tipo de dado a ser tratado.

4.3 Visão geral do protocolo RC4

O protocolo RC4 é um criptador de fluxo que utiliza criptografia simétrica. Foi desenvolvido, em 1987, por Ron Rivest no MIT (*Massachusetts Institute of Technology*) para a RSA Security. O algoritmo do RC4 foi mantido secreto por praticamente 7 anos, quando foi publicado anonimamente na Internet conforme [Fluhrer 2001].

Mesmo sendo atualmente de conhecimento público, o RC4 ainda é considerado um algoritmo forte, pois ele é resistente à criptoanálise linear e diferencial. Ele é não-linear e não tem ciclos curtos [Fluhrer 2001]. É um dos algoritmos de criptografia de fluxo mais utilizados. O algoritmo do RC4 é muito simples, e pode ser implementado em *software* com performance adequada. O RC4 pode trabalhar com chaves de diferentes tamanhos, que podem chegar a 2048 *bits*. Contudo, as aplicações práticas têm trabalhado com chaves entre 40 e 256 *bits*. O algoritmo RC4 é dividido em duas partes: o KSA (*Key Scheduling Algorithm*), que transforma uma chave aleatória em uma permutação inicial representada pelo vetor *S*; e o PRGA (*Pseudo Random Generation Algorithm*), que utiliza a permutação *S* para gerar uma sequência de saída pseudo aleatória.

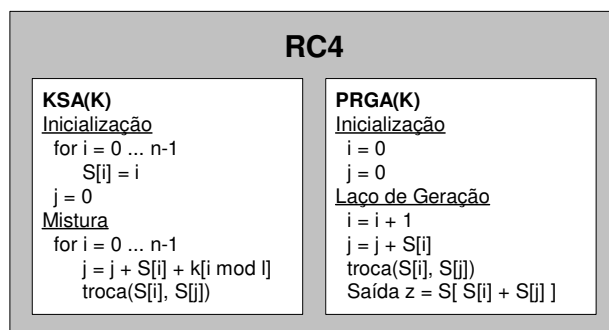


Figura 26 – Esquema do algoritmo RC4

A figura 26 [Fluhrer 2001] exibe as duas partes do algoritmo RC4. O KSA usa a chave para iniciar o gerador de número pseudo-aleatórios. Assim é gerada uma tabela de estado aleatória baseada na chave. Esta iniciação consiste em um laço de repetição, que é executado n vezes, onde n é a quantidade de *bits* da chave utilizada. O KSA inicializa S como uma permutação identidade e j com o valor 0. Em um novo laço de repetição o KSA varia os valores de i em S e atualiza j somando o mesmo a $S[i]$ com a próxima parte da chave de forma cíclica, o tamanho das chaves é definido pela letra l .

Assim que o gerador estiver iniciado o PRGA inicializa 2 índices i e j com o valor 0. Em seguida, executa um laço de repetição com 4 operações simples: incrementa i como um contador, atualiza j de forma pseudo aleatória, troca os valores de S apontados por i e j e calcula o valor de saída. A saída de cada iteração é representada por z e é o valor de S indicado por $S[i] + S[j]$. Esta saída é o valor necessário para os processos que criptografam e decriptografam os dados.

O RC4 pode se apresentar com implementações vulneráveis do KSA. Neste caso o KSA não gera uma distribuição perfeitamente aleatória. Assim é recomendável que algumas saídas do PRGA sejam descartadas, para que a tabela de estado esteja em uma distribuição mais adequada, antes que as informações sejam processadas.

4.4 Visão geral do protocolo WEP

O protocolo WEP utiliza criptografia simétrica e opera com chaves pré-compartilhadas. O WEP é baseado no protocolo RC4 e possui duas opções de tamanho de chaves: 64 e 128 *bits*. No entanto, como o WEP utiliza o esquema baseado em vetores de

inicialização de 24 *bits* nas duas opções, é comum que as chaves sejam indicadas como chaves de 40 e 104 *bits*, uma vez que o vetor de inicialização é utilizado para formar a chave e é transmitido de forma não criptografada pela rede [Walker 2000]. O WEP agrega também um mecanismo que objetiva garantir a integridade dos pacotes. Este mecanismo é um ICV do tipo CRC de 32 *bits*, que gera uma checagem do quadro e é inserido no final de cada pacote.

A figura 27 [Ow 2001] mostra a estrutura do protocolo WEP de uma maneira esquemática. Para criptografar um quadro de rede, o texto não criptografado passa pelo gerador do CRC32, que produz o ICV e o concatena com o texto não criptografado. Por outro lado, a chave pré-compartilhada é concatenada ao vetor de inicialização, que gera uma semente que passa por um PRNG (*Pseudo Random Number Generator*) que produz uma chave-fluxo. Essa chave-fluxo tem o mesmo tamanho do quadro que contém o texto não criptografado concatenado ao ICV. Essas duas entradas passam por um ou-exclusivo, que é o texto criptografado produzido.

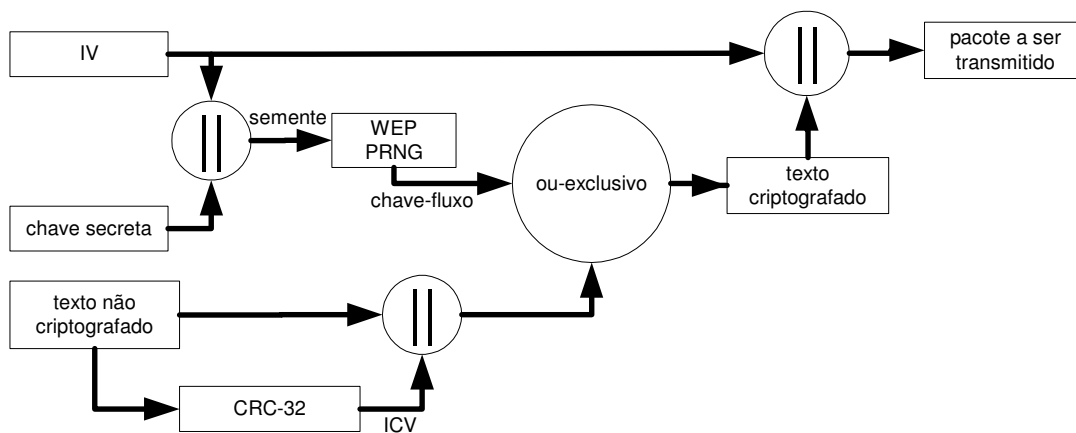


Figura 27 – Esquema do protocolo WEP

O receptor, além do texto criptografado, receberá o vetor de inicialização, que trafega de forma não criptografada pela rede, desta forma, é só fazer o processo inverso para a decriptografia e verificação dos dados recebidos.

4.5 Fragilidades do protocolo WEP

Não há nada errado com o RC4, ele pode ser considerado seguro, ou seja: ainda não foi quebrado de forma viável. Entretanto a implementação do RC4 utilizada pelo WEP insere algumas fraquezas, o ponto principal é que o WEP não descarta nenhuma saída do PRGA, além disso, o WEP reinicia o estado do RC4 a cada pacote. Algumas possibilidades de ataques são descritas a seguir:

4.5.1 Derivação estatística de chave – Ataque passivo

Em agosto de 2001, os criptoanalistas Fluhrer, Martin e Shamir [Fluhrer 2001] determinaram que uma chave WEP poderia ser passivamente derivada a partir da coleta de tráfego na rede sem fio. Isso somente é possível devido a uma vulnerabilidade do protocolo WEP na implementação do algoritmo KSA do cifrador de fluxo RC4.

Os criptoanalistas descobriram que, utilizando apenas os dois primeiros *bytes* da chave-fluxo, poderiam revelar a chave secreta. Desta forma, conseguiram descobrir partes da chave que compostas revelaram a chave secreta.

De forma simplificada, é feita uma pesquisa no tráfego coletado em busca dos vetores de inicialização denominados *fracos*, que podem revelar informação sobre 1 *byte* da chave. Este *byte* deve ser adivinhado, e a probabilidade de acerto cresce com o número de vetores de

inicialização que revelam informações sobre este *byte*. Outros pacotes revelam informações sobre outros *bytes*, e, assim, consegue-se a derivação da chave de modo totalmente passivo. Este processo é detalhado em [Ow 2001].

Pouco tempo depois, pesquisadores da AT&T e Rice University, juntamente com os desenvolvedores do AirSnort implementaram o algoritmo que explora essa vulnerabilidade e consegue derivar a chave após a coleta de cerca de 16 milhões de pacotes. Assim, surgiu o AirSnort. Baseada no mesmo algoritmo, tempos depois, foi desenvolvida outra ferramenta com o mesmo objetivo: o WepCrack.

4.5.2 A questão do reuso da chave-fluxo

Conforme discutido anteriormente, para que um cifrador de fluxo seja considerado seguro, no mínimo, uma propriedade deve ser satisfeita: ao criptografar dois textos não criptografados idênticos os textos criptografados devem ser diferentes [Borisov 2001].

Para que o RC4 se tornasse resistente a esse problema, foi criado o vetor de inicialização, com o objetivo de alterar a chave-fluxo. No entanto existe um problema quando o vetor de inicialização é repetido. O exemplo a seguir considera a utilização da mesma chave e do mesmo IV:

Supondo dois textos não criptografados P_1 e P_2 , e dois textos criptografados C_1 e C_2 , com o mesmo vetor de inicialização, calculados da seguinte forma:

$$C_1 = P_1 \text{ xor } RC4(IV, K) \quad \text{e} \quad C_2 = P_2 \text{ xor } RC4(IV, K), \quad \text{então,}$$

$$C_1 \text{ xor } C_2 = (P_1 \text{ xor } RC4(IV, K)) \text{ xor } (P_2 \text{ xor } RC4(IV, K)), \quad \text{logo,}$$

$$C_1 \text{ xor } C_2 = P_1 \text{ xor } P_2$$

Ou seja o ou-exclusivo de dois textos criptografados é igual ao ou-exclusivo dos dois textos não criptografados. Assim, se o texto não criptografado de uma mensagem é conhecido, o conteúdo da outra mensagem é revelado.

Para que um ataque consiga explorar essa vulnerabilidade, o atacante precisa ter meios para conseguir capturar o tráfego na rede sem fio. Ele também deve ser capaz de injetar uma mensagem de conteúdo conhecido na rede sem fio e encontrar uma mensagem com vetor de inicialização igual ao da mensagem gerada.

Tarefas como capturar tráfego na rede sem fio ou inserir mensagens nela são tarefas relativamente fáceis, conforme exibido na seção 3.7.

Encontrar uma mensagem que tenha o mesmo vetor de inicialização do utilizado na mensagem introduzida é uma questão de tempo, conforme a seção 5.6. O reuso dos vetores de inicialização vai depender da maneira que são inicializados e reutilizados. A relação de tempo e quantidade de tráfego coletado são discutidos nas seções 3.7 e 5.6.

4.5.3 Ataques ativos

Os ataques ativos interagem com a rede sem fio diretamente por meio da inserção ou adulteração de mensagens. Esta estratégia é diferente dos ataques passivos, nos quais somente ocorre a coleta e análise de tráfego da rede.

Os dois ataques ativos mais conhecidos em redes locais em fio são detalhados a seguir. Esses ataques são ataques de texto escolhido (*chosen plaintext*) [Stallings 1998].

4.5.3.1 Ataque por injeção de mensagem

O ataque por injeção de mensagem segue os seguintes passos ilustrados na figura 28:

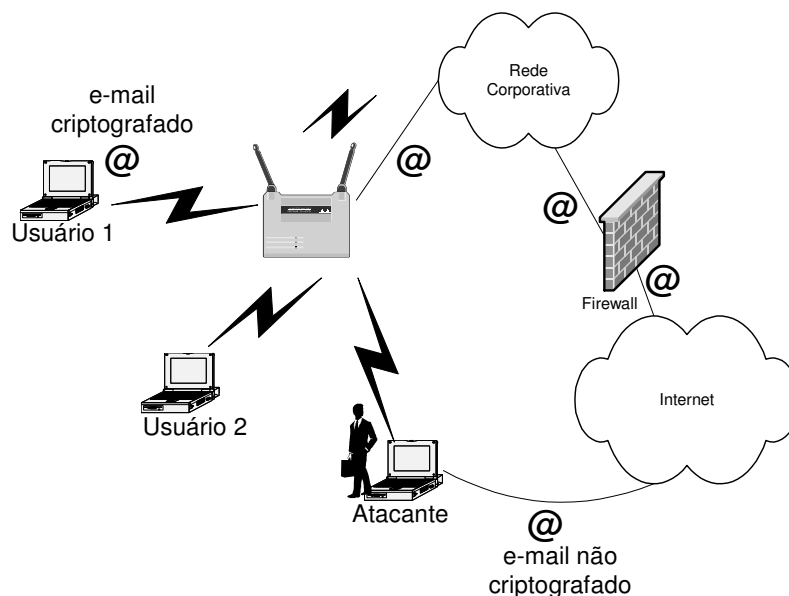


Figura 28 – Ataque por injeção de mensagem

1. Uma mensagem de conteúdo conhecido é enviada pelo atacante a um usuário da rede sem fio, por exemplo, uma mensagem de e-mail enviada pela Internet.
2. O atacante, coletando tráfego na rede em modo promíscuo, procura pelo tráfego criptografado correspondente à mensagem enviada.
3. O atacante encontra o quadro esperado e deriva a chave-fluxo utilizada.
4. O atacante pode expandir a chave-fluxo derivada usando o mesmo vetor de inicialização observado no quadro capturado.

Esse ataque pode ser repetido para gerar uma chave-fluxo grande o suficiente para subverter a rede.

Uma vez que uma chave-fluxo de qualquer tamanho tenha sido derivada, é possível expandi-la a qualquer tamanho desejável. Este processo é ilustrado pela figura 29 e descrito a seguir:

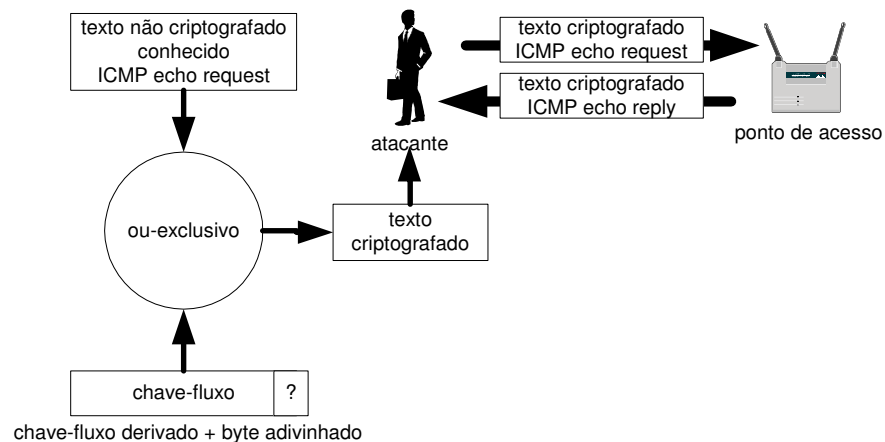


Figura 29 – Expansão de uma chave-fluxo

1. O atacante pode construir um quadro com 1 *byte* a mais do que a chave-fluxo conhecida. Uma opção é a geração de um pacote ICMP (*Internet Control Message Protocol*) do tipo *echo request*, pois este pacote solicita outro em resposta.
2. Para criptografar o pacote gerado, o atacante utiliza a chave-fluxo derivada, acrescida em 1 *byte*.
3. O *byte* adicional pode ser adivinhado, pois somente existem 256 possibilidades.
4. Quando o atacante adivinha o *byte* correto, a resposta ao pacote enviado é recebida, neste caso, um ICMP *echo reply*.
5. O processo é repetido até que o tamanho desejado seja conseguido.

4.5.3.2 Ataque por alteração de *bits*

Este ataque tem o mesmo objetivo do ataque anterior, mas sem a necessidade de inserção de uma mensagem de conteúdo conhecido.

O ataque é baseado na fraqueza do CRC32 definido no padrão IEEE 802.11. Ele é demonstrado na figura 30 e descrito a seguir:

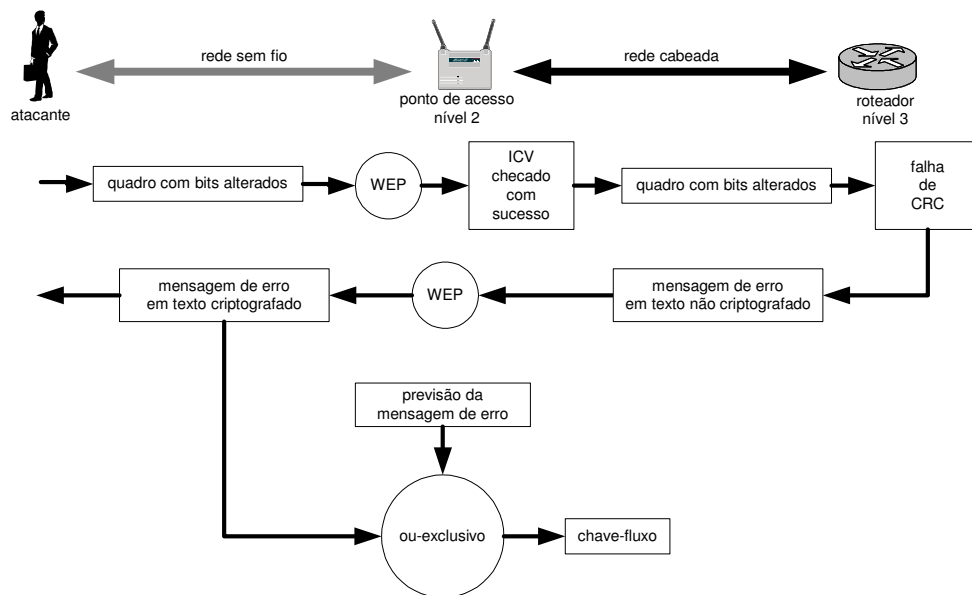


Figura 30 – Ataque por alteração de *bits*

1. O atacante coleta 1 quadro na rede sem fio.
2. O atacante troca alguns *bits*, de forma aleatória, na parte de dados do quadro capturado.
3. O atacante modifica o ICV, esta modificação é detalhada em breve.
4. O atacante transmite o quadro alterado.
5. O ponto de acesso, ao receber o quadro, verifica o ICV em nível 2 e repassa o quadro à estação de destino.
6. O receptor recalcula o ICV do quadro recebido e verifica-o contra o ICV constante no quadro recebido.
7. O receptor aceita o quadro, posto que o ICV foi igual.
8. O receptor desencapsula o quadro e o encaminha à camada 3 na forma de um pacote.
9. Devido a alteração realizada nos dados do quadro na camada 2, o processo de integridade da camada 3 falha.

10. A pilha IP do receptor gera um erro conhecido e predeterminado. Este erro é conhecido pelo atacante.
11. O atacante continua a capturar tráfego na rede sem fio, procurando pela mensagem de erro na forma criptografada.
12. O atacante de posse da mensagem de erro criptografada e da mensagem de erro inferida, visto que o erro é conhecido, deriva a chave-fluxo.

A essência desse ataque está na manipulação dos *bits* do quadro capturado de modo que o ICV seja reconhecido como correto pelo protocolo WEP. A figura 31 mostra como o ICV pode ser manipulado.

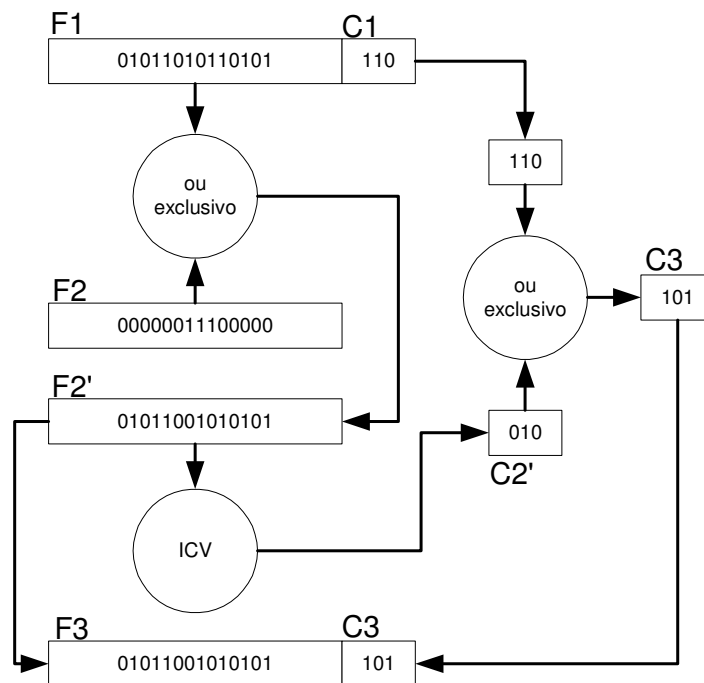


Figura 31 – Alteração de *bits* na mensagem criptografada

1. Captura-se um quadro F1 e seu ICV C1.
2. Um novo quadro F2, com o mesmo tamanho de F1, é escolhido de modo a alterar os *bits* desejados.

3. Outro quadro $F2'$ é gerado por intermédio do ou-exclusivo de $F1$ e $F2$. Este é o quadro com os *bits* alterados.
4. O ICV para $F2'$ é calculado utilizando o CRC32. Este ICV é referenciado por $C2'$.
5. O ICV para o pacote alterado, $C3$, é gerado através do ou-exclusivo de $C1$ e $C2'$.
6. O pacote alterado com ICV válido está pronto e é definido por $F3$ e seu ICV $C3$.

5 PROPOSTA DE MELHORIA DO NÍVEL DE SEGURANÇA DAS REDES LOCAIS SEM FIO

5.1 Introdução

O capítulo 3 evidencia uma série de vulnerabilidades associadas aos atuais esquemas de comunicação nas redes locais sem fio. Também no capítulo 4, as fragilidades do protocolo WEP são detalhadas. Com o objetivo de elevar o nível de segurança desses ambientes, é descrita uma proposta de melhoria do nível de segurança das redes locais sem fio. Esta proposta objetiva melhorar os mecanismos de segurança das redes locais sem fio, podendo ser considerada como uma extensão do padrão IEEE 802.11, posto que é compatível com as premissas e protocolos atualmente utilizados. Sua implementação pode ser feita por atualização do software sem a necessidade de expansão do *hardware* dos atuais equipamentos.

Um estudo de avaliação dessa proposta também é apresentado, evidenciando que, embora ocorra considerável aumento no tráfego de gerenciamento, este volume ainda é muito pequeno quando comparado com o tráfego total transmitido na rede. Porém percebe-se que grande confiança é agregada aos números pseudo-aleatórios, logo, cuidados adicionais devem ser tomados na geração e armazenamento destes, boa parte da segurança da solução depende disso.

A seção 5.2 exhibe o detalhamento da proposta de acordo com as fases de acesso. Na seção 5.3, são exibidas considerações sobre a redução das fraquezas do protocolo WEP. Na seção 5.4, a revogação de chaves é tratada. A seção 5.5 apresenta a nova estrutura dos quadros

de rede, mensagens e tamanho dos pacotes. A seção 5.6 mostra os resultados do estudo de avaliação da proposta. Finalmente, a seção 5.7 indica outras medidas, já conhecidas, que podem ser implementadas, de forma complementar, no sentido de elevar o nível de segurança desses ambientes.

5.2 Proposta de melhoria do nível de segurança de redes locais sem fio

A figura 32 apresenta um esquema de conexão à rede local sem fio, incluindo as fases de sondagem, autenticação e associação de acordo com a proposta. Sua interpretação é análoga à da figura 3 do capítulo 2 e é analisada nas seções seguintes.

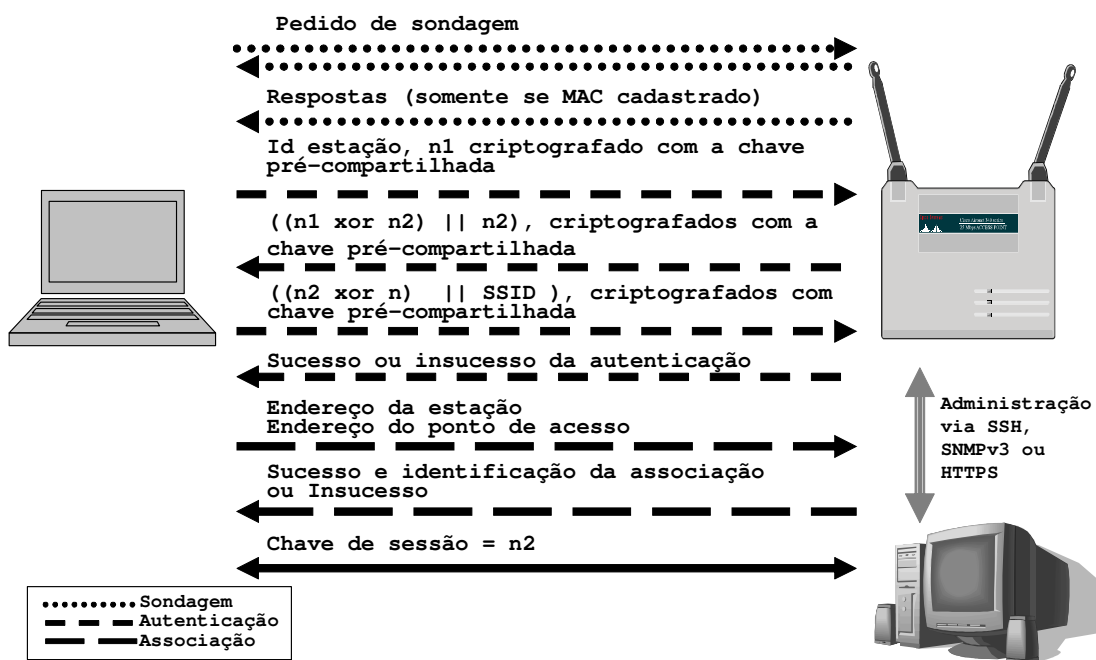


Figura 32 – Conexão à rede local sem fio, de acordo com esta proposta

5.2.1 Processo de sondagem

Esta seção descreve os mecanismos que dificultam o mapeamento da rede na fase de sondagem. Estes mecanismos se fundamentam na filtragem MAC.

Na proposta apresentada, o mapeamento da rede, por um intruso, é dificultado considerando a verificação do endereço MAC durante a fase de sondagem. Nesta fase, o endereço MAC do cliente é verificado contra uma base de endereços MAC cadastrados. Caso o endereço MAC do cliente não esteja armazenado na base, o ponto de acesso fica mudo e não transmite resposta alguma. Assim, a descoberta de uma rede sem fio é dificultada. Atualmente, os produtos que disponibilizam algum tipo de filtragem MAC consideram a filtragem em fases subseqüentes a de sondagem. Logo, mesmo tendo o acesso à rede negado, o invasor tem a chance de capturar dados sobre a rede.

Mesmo considerando os pontos citados, é possível que a filtragem MAC não seja adotada. Em redes grandes e dinâmicas, o custo de administração da base de endereços MAC deve ser observado.

O problema da captura e falsificação de um endereço MAC cadastrado continua existindo. No entanto, essa medida evita que *war drivers* e usuários comuns usem o *software* de suas interfaces de rede sem fio para mapear a rede. Entretanto, isto não confere à rede segurança diante de usuários mais experientes e determinados a mapeá-la. Portanto, este não é um mecanismo eficaz contra a falsificação ou clonagem de endereços MAC. Ele apenas dificulta o mapeamento da rede.

5.2.2 Processo de autenticação

A proposta apresentada neste capítulo também previne a captura do SSID na fase de autenticação. No esquema convencional, o SSID trafega de forma não criptografada, quando

enviado do cliente para o ponto de acesso. Isto permite que seja facilmente capturado e posteriormente utilizado.

No esquema desta proposta, o SSID é transmitido concatenado a outro valor e de forma criptografada pelo algoritmo WEP. Assim, a leitura do SSID fica impossibilitada devido à criptografia e impossibilidade de correlação dos valores. Neste caso, mesmo se o pacote for capturado para posterior utilização, o ataque não terá sucesso em razão do número pseudo-aleatório que compõe o valor concatenado ao SSID.

A partir do pacote criptografado, não é viável a extração das duas partes sem o uso da chave adequada. A correlação entre o desafio e a resposta entre os pacotes de autenticação não pode ser feita, visto que, em cada um destes pacotes, existe um valor composto por um número pseudo-aleatório diferente, concatenado aos valores do desafio e da resposta. Este processo é ilustrado entre a quarta e sétima linhas da figura 32.

Outro mecanismo proposto é a redução da quantidade de tráfego protegido pela chave pré-compartilhada. Considera-se o uso de uma chave pré-compartilhada, que é utilizada somente no processo de autenticação. Observa-se que, no padrão IEEE 802.11, a chave pré-compartilhada é utilizada no processo de autenticação e também para prover a confidencialidade dos dados no ar.

Nessa proposta, a chave pré-compartilhada somente é utilizada para autenticar o cliente, autenticar o ponto de acesso e, se necessário, revogar outras chaves. Assim, uma quantidade bem menor de tráfego é criptografada com esta chave. Desta forma, os ataques citados em [Roshan 2002] contra o protocolo WEP tornam-se inviáveis em decorrência da quantidade pequena de dados que trafegam sob a proteção da chave pré-compartilhada.

Com base no estudo realizado na seção 5.6, na rede analisada, existem, em média, 2.8 processos de autenticação por usuário a cada dia. Considerando 7 usuários e que cada autenticação necessita de 4 pacotes, existem, aproximadamente, 80 pacotes de autenticação

em um dia. Como o IV (*Initialization Vector*) é repetido a cada 2^{24} pacotes, e considerando o uso da chave pré-compartilhada apenas no processo de autenticação, seriam gastos, aproximadamente, 574 anos de coleta de tráfego para a quebra de chave WEP utilizando as vulnerabilidades já discutidas. O valor 574 é a divisão de 2^{24} por 80 pacotes/dia, novamente, dividido por 365 dias.

O processo de autenticação tem três propósitos: autenticar o cliente perante o ponto de acesso, autenticar o ponto de acesso perante o cliente e distribuir uma nova chave de sessão. Da mesma maneira que não se deseja que clientes quaisquer tenham acesso à rede, também se deseja que nenhum ponto de acesso clandestino possa fazer parte dela.

No primeiro passo, o pedido de autenticação é enviado do cliente para o ponto de acesso. O identificador da estação é concatenado ao pedido, juntamente com um primeiro número pseudo-aleatório ($n1$) gerado pela estação e criptografado pela chave pré-compartilhada. Este processo está ilustrado nos itens de 1 a 3 da figura 33. Os números pseudo-aleatórios gerados e utilizados na proposta são números de 128 bits, gerados pelo gerador do protocolo WEP.

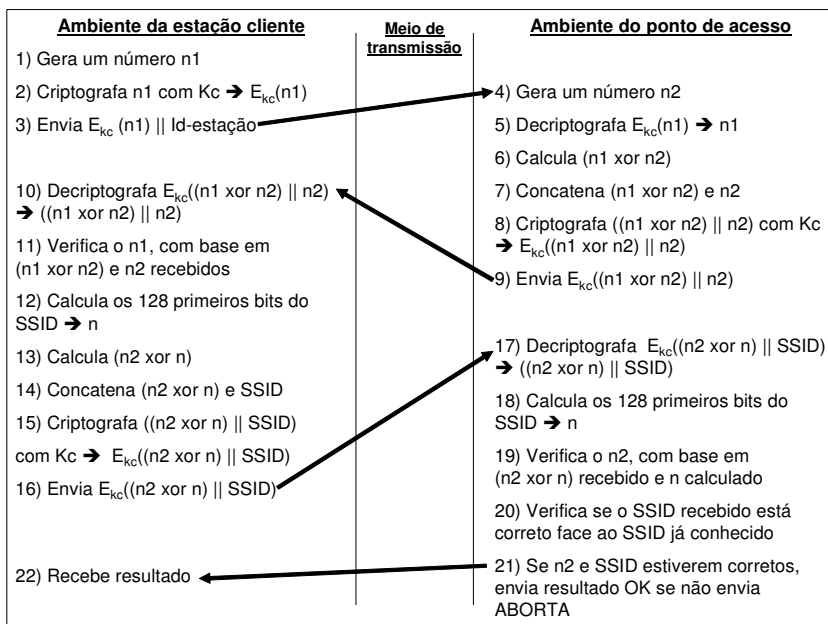


Figura 33 – Detalhamento da fase de autenticação, de acordo com esta proposta

O ponto de acesso gera um segundo número pseudo-aleatório (n_2), que é o desafio ao cliente. Ao receber o conjunto enviado pelo cliente, o ponto de acesso decriptografa o conjunto. O ponto de acesso deveria enviar de volta os dois números, no entanto, se estes dois números fossem apenas concatenados e criptografados para o envio, ainda seria possível correlacionar os pacotes, tornando possível a derivação da chave-fluxo. Logo, primeiro o ponto de acesso calcula o ou-exclusivo entre os dois números (n_1 e n_2). Este resultado é concatenado ao valor de n_2 . O resultado é criptografado e enviado ao cliente. Para que o ponto de acesso possa calcular o ou-exclusivo, ele tem que decifrar o n_1 recebido, e esta decriptografia é que garante ao cliente que o ponto de acesso possui a chave pré-compartilhada correta. Este processo está ilustrado nos itens de 4 a 9 da figura 33.

O cliente, ao receber o conjunto, deve decriptografá-lo e verificar se o desafio (n_1) que emitiu está correto, para isso, o cliente deve calcular o ou-exclusivo entre o resultado que recebeu ($n_1 \text{ xor } n_2$) e o valor de n_2 recebido. O resultado deve ser idêntico ao n_1 que o cliente gerou anteriormente. Caso a verificação de n_1 falhe, o processo é abortado. Em seguida o cliente responde ao desafio lançado pelo ponto de acesso. Entretanto, para que n_2 também seja protegido, o cliente o concatena com os 128 primeiros *bits* do SSID configurado no cliente. Esta metade do SSID é denominada por n , assim, o cliente calcula ($n_2 \text{ xor } n$) e concatena este valor ao SSID inteiro, cujo resultado é criptografado com a chave pré-compartilhada e enviado ao ponto de acesso. Este processo está ilustrado nos itens de 10 a 16 da figura 33.

Novamente, ao receber o conjunto, o ponto de acesso verifica o desafio que lançou ao cliente (n_2), para isso, o ponto de acesso decriptografa o conjunto recebido, calcula um novo n , baseado nos 128 primeiros *bits* do SSID configurado no ponto de acesso; depois o ponto de acesso calcula o ou-exclusivo entre ($n_2 \text{ xor } n$) recebido e o n calculado. O resultado deve ser idêntico ao n_2 gerado anteriormente. O ponto de acesso também verifica se o SSID recebido é

idêntico ao SSID configurado anteriormente. Se todas as verificações ocorrerem com sucesso, um resultado positivo é enviado ao cliente, caso contrário, um resultado negativo é enviado. Este processo está ilustrado nos itens de 17 a 21 da figura 33.

O número $n2$ é, a partir deste momento, utilizado como chave de sessão para garantir a confidencialidade dos dados. Esta chave é empregada até que seja revogada ou até que haja um processo de reautenticação.

O primeiro número pseudo-aleatório ($n1$), gerado pelo cliente, é utilizado no processo de autenticação do ponto de acesso. Isto evita que um cliente legítimo possa se conectar a um ponto de acesso inserido maliciosamente, com o propósito de capturar as credenciais de acesso.

O segundo número pseudo-aleatório ($n2$), gerado pelo ponto de acesso, é utilizado no processo de autenticação do cliente. Isto permite que seja verificado se o cliente conhece a chave pré-compartilhada e se tem a habilidade de utilizá-la de forma correta.

Essas autenticações ocorrem em esquema de desafio/resposta. Neste caso, os dados não trafegam isoladamente e nem de forma não criptografada. Isto evita que a chave-fluxo possa ser derivada do desafio e da resposta. Os dois campos somente podem ser correlacionados se não possuírem outras informações agrupadas.

Observa-se que a filtragem MAC, definida na fase de sondagem, é considerada como uma pré-autenticação. Com isso, passos adicionais, como os exibidos no capítulo 2, podem ser eliminados na fase de autenticação.

Um exemplo completo de um processo de autenticação é exibido na figura 34. Este exemplo emprega números pseudo-aleatórios de apenas 4 *bits*, ao contrário dos 128 *bits* desta proposta. Além disso, o SSID considerado é de apenas 8 *bits*. O processo de criptografia utilizado é definido como a substituição do texto não criptografado pelo valor de duas posições à frente, ou seja: para o texto não criptografado 7 o texto criptografado é 9, e assim

por diante. Este exemplo não é nada seguro devido ao tamanho das chaves e do processo de criptografia, é um exemplo didático e tem o objetivo único de mostrar, de forma simples, a utilização do processo de autenticação dessa proposta. O protocolo de criptografia utilizado na proposta continua sendo o WEP, o protocolo simplificado é aqui utilizado apenas para facilitar o acompanhamento deste exemplo.

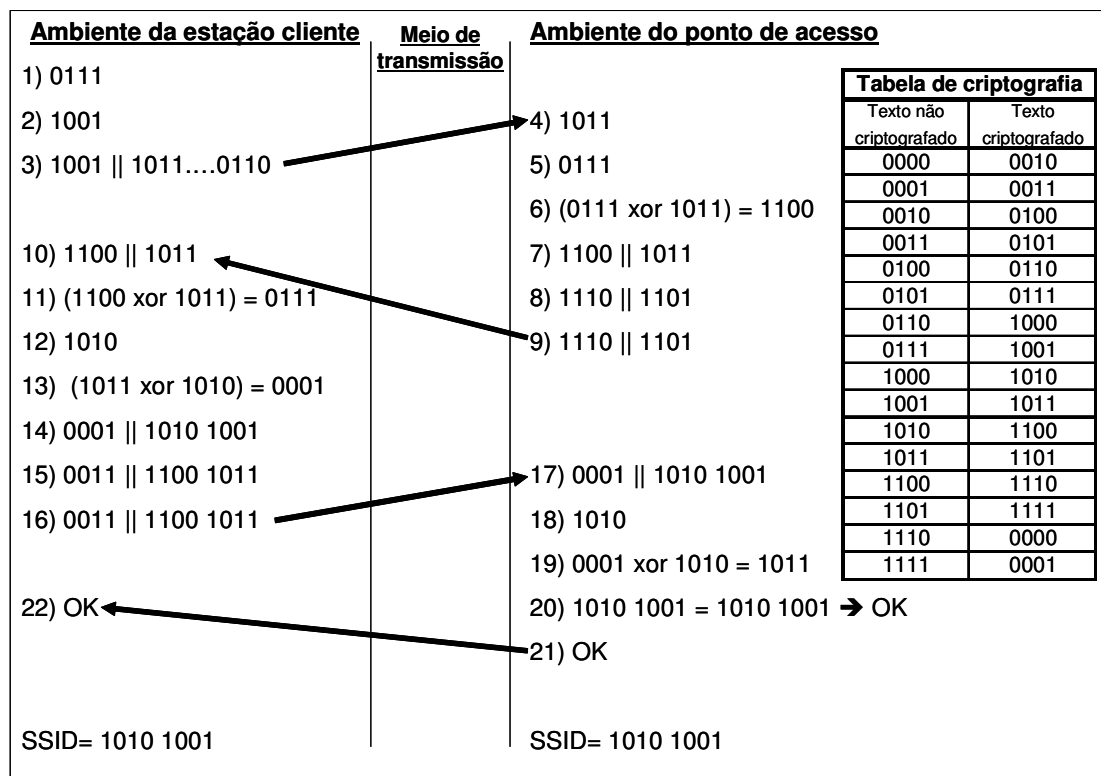


Figura 34 – Exemplo didático de uma autenticação, de acordo com esta proposta

5.2.3 Processo de reautenticação

O processo de reautenticação é similar ao processo de autenticação. Porém ele é iniciado pelo ponto de acesso responsável por controlar os períodos de reautenticação. O processo de reautenticação é exibido na figura 35

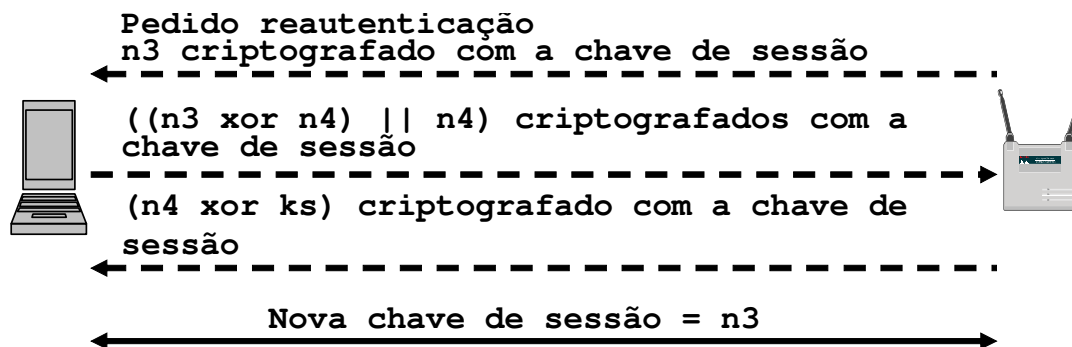


Figura 35 – Processo de reautenticação

Outra grande diferença está na chave utilizada para a troca das informações. Enquanto o processo de autenticação usa a chave pré-compartilhada, o processo de reautenticação emprega a chave de sessão até então utilizada. Esta chave ainda é segura, desde que não tenha sido revogada.

O ponto de acesso, ao requisitar a reautenticação, envia um número pseudo-aleatório $n3$, criptografado pela atual chave de sessão. Este número deve ser descriptografado pelo cliente, que gera um segundo número pseudo-aleatório ($n4$), calcula o ou-exclusivo entre $n3$ e $n4$, concatena este resultado ao valor de $n4$. Estas informações são criptografadas pela chave de sessão e, depois, enviadas ao ponto de acesso.

O ponto de acesso verifica se o cliente conseguiu responder ao desafio lançado ($n3$) e recebe um novo desafio ($n4$), que deve ser extraído da concatenação recebida $((n3 \text{ xor } n4) || n4)$ e devolvido para o cliente. Para que o ponto de acesso possa provar ao cliente que consegue obter o valor de $n4$, este calcula o ou-exclusivo com a atual chave de sessão em uso, este conjunto é criptografado e enviado ao cliente. O número $n3$ é utilizado, a partir deste momento, como a nova chave de sessão.

5.2.4 Processo de desautenticação

O processo de desautenticação é iniciado pelo cliente. O objetivo é encerrar sua participação na rede. Esta notificação é muito importante para evitar que outros clientes tentem se passar pelo cliente que deixa a rede. Isto seria um ataque do tipo seqüestro de sessão. Este processo é mostrado na figura 36.

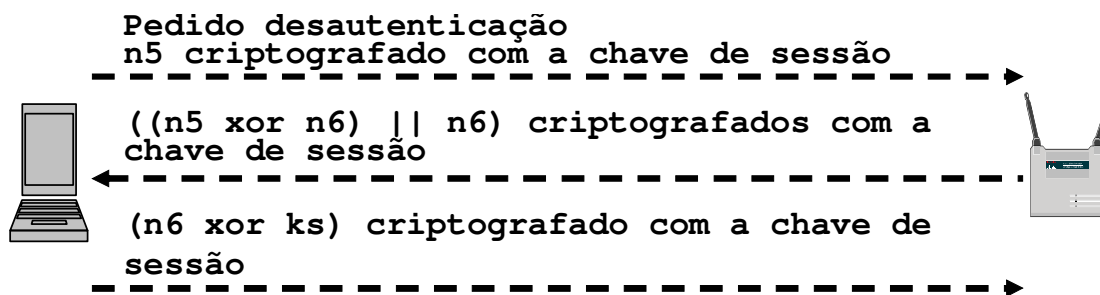


Figura 36 – Processo de desautenticação

A interpretação deste processo é análoga à interpretação do processo de reautenticação. Contudo nenhuma nova chave é utilizada após o processo, pois o objetivo da estação que solicita a desautenticação é deixar de participar na rede.

O processo de desautenticação pode ser omitido implementando-se assim uma otimização. Neste caso o ponto de acesso ao tentar reautenticar o cliente e não obter resposta poderia encerrar a referida sessão. No entanto se esta otimização não for necessária para um melhor desempenho ela não é aconselhada do ponto de vista de segurança, ainda mais nos casos onde o período de reautenticação for maior.

5.3 Redução dos efeitos das fraquezas do protocolo WEP

Esta seção expõe os mecanismos que reduzem as deficiências do protocolo WEP. Isto é conseguido por meio da distribuição e uso de chaves de sessão de forma periódica e dinâmica.

Um processo de distribuição dinâmica de chaves de sessão é adicionado dentro da fase de reautenticação. O processo consiste no aproveitamento de um dos números pseudo-aleatórios utilizados no processo de reautenticação como a nova chave de sessão. Este número passa a ser empregado como chave de sessão. Esta chave de sessão garante a confidencialidade dos dados trafegados na rede até o próximo período de reautenticação ou até que seja revogada.

Uma nova chave de sessão é gerada e distribuída a cada processo de reautenticação, que ocorre periodicamente. Neste caso, os dados estão protegidos, pois, mesmo se a chave WEP for quebrada, a chave revelada não estará mais em uso.

O processo de quebra da chave WEP somente é viável após a coleta de uma certa quantidade de tráfego. Assim, o período de reautenticação deve ser menor que o período necessário para a coleta dessa quantidade de tráfego. Este tempo depende da quantidade de tráfego sendo transmitido na rede e da velocidade de transmissão dos equipamentos. O período para a reautenticação deve ser especificado de acordo com a carga da rede, quanto maior a carga, menor o tempo de reautenticação. Alguns parâmetros de carga são considerados em [Mahan 2001]. A seção 5.6 apresenta os cálculos dos períodos de reautenticação utilizados na avaliação dessa proposta.

Esse processo de geração e distribuição da chave de sessão é apresentado na última linha das figuras 32 e 35.

5.4 Revogação de chaves de sessão

Esta seção apresenta mecanismos que possibilitam a revogação de chaves de sessão em uso. Estas chaves são revogadas quando são consideradas comprometidas ou inseguras.

O administrador, ao identificar uma chave comprometida, pode revogá-la. Para isso, o administrador, deve iniciar o processo por meio do ponto de acesso. Este processo é muito similar às últimas etapas da fase de autenticação, pois tanto o ponto de acesso quanto a estação são novamente autenticados. A autenticação é realizada com base na chave pré-compartilhada e não na chave de sessão comprometida.

Assim que a estação e o ponto de acesso estão autenticados, o número que foi gerado pelo ponto de acesso passa a ser utilizado como a nova chave de sessão.

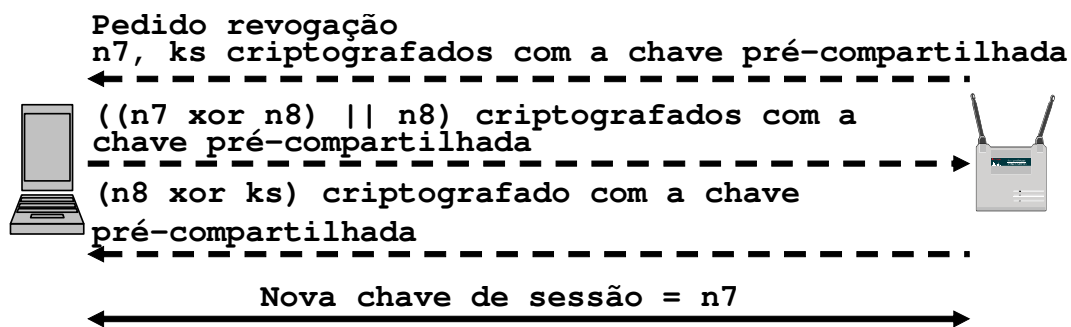


Figura 37 – Processo de revogação de chaves

O processo de revogação de chaves é descrito na figura 37. Ele segue o mesmo modelo que o processo de reautenticação e tem interpretação análoga. No entanto, como a chave de sessão em uso foi considerada insegura, esta não deve ter qualquer participação no processo. O uso da chave indicada como insegura pode comprometer a segurança, permitindo ao atacante o acesso à nova chave de sessão.

5.5 Formato e tamanho dos quadros de rede e processos

Esta seção descreve o formato e o tamanho dos quadros utilizados nesta proposta, bem como o detalhamento das mensagens dos principais processos.

O quadro MAC utilizado na proposta é o mesmo empregado no padrão IEEE 802.11. As mudanças ocorrem apenas nos conteúdos, quantidade e sequência das mensagens transportadas por esses pacotes.

Em sequência, a estrutura dos processos de autenticação, reautenticação, revogação e desautenticação são apresentados de modo a se encaixarem no *frame body* de um quadro.

Dentro do campo de dados do pacote MAC de gerenciamento, existe mais um nível de estruturação, onde existem três campos de tamanho fixo e um último de tamanho variável. O esquema deste sub-quadro é apresentado na figura 38.

Alg. Number	Seq. Number	Status Code	Text	Campos
2	2	2	0-2306	Tamanho em <i>bytes</i>

Figura 38 – Formato do *frame body*

O campo *Algorithm Number* indica o tipo de processo que está sendo transportado. O campo *Sequence Number* aponta a sequência daquela mensagem dentro do processo. O campo *Status Code* indica um estado associado ao processo. Os possíveis valores deste campo não são alterados nesta proposta e podem ser consultados em [IEEE 1999]. O campo *Text* transporta os dados propriamente ditos.

A seguinte relação pode ser utilizada para o campo *Algorithm Number*:

0 ➔ Autenticação padrão OSA (não utilizado)

1 ➔ Autenticação padrão SKA

2 ➔ Reautenticação

3 ➔ Revogação

4 ➔ Desautenticação

Os possíveis valores para os campos *Sequence Number* e *Text* são detalhados, a seguir, em separado para cada processo.

Para que a rede local sem fio possa operar normalmente, alguns processos são necessários. Estes processos são exibidos a seguir de modo que possam ser comparados com os processos do padrão IEEE 802.11.

Vale notar que o processo que define se a garantia de confidencialidade é ou não utilizada deixa de existir, pois o uso do protocolo WEP para a proteção da confidencialidade é mandatário nesta proposta. Sendo mandatário não é necessário um processo ou mensagem que ative o uso do protocolo WEP para garantir a confidencialidade dos dados. Além disso, o processo de autenticação OSA também deixa de existir, posto que as redes concordantes com esta proposta não são redes públicas, necessitando de um processo de autenticação mais robusto.

Por outro lado, processos como o de reautenticação e revogação de chaves foram criados, e outros, como autenticação e desautenticação, foram totalmente alterados.

5.5.1 Processo de transferência de dados

O processo de transferência de dados é utilizado por uma estação para o envio de dados para outra estação, seja um sistema terminal na rede ou um ponto de acesso.

Este processo opera com mensagens com o seguinte formato:

Nome da mensagem : Mensagem de dados

Tipo da mensagem : Dados

Subtipo da mensagem : Dados

Itens de informação	: Endereço de origem
	Endereço de destino
	Identificador da rede
	Dados
Sentido	: De uma estação para outra estação

5.5.2 Processo de associação

O processo de associação é utilizado por uma estação, para que esta possa associar-se à rede após o processo de autenticação.

Este processo opera com mensagens com o seguinte formato:

Nome da mensagem	: Pedido de associação
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Pedido de associação
Itens de informação	: Endereço da estação que faz o pedido
	Endereço do ponto de acesso envolvido
	Endereço MAC da estação
	Identificador da rede
Sentido	: De uma estação para o ponto de acesso
Nome da mensagem	: Resposta de associação
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Resposta de associação
Itens de informação	: Sucesso e resultado somente se o MAC estiver cadastrado
	No caso de sucesso, o identificador da associação é enviado
Sentido	: Do ponto de acesso para uma estação

5.5.3 Processo de reassociação

O processo de reassociação é utilizado por uma estação para que esta possa associar-se a outro ponto de acesso. O requisito é que a estação já esteja associada a algum outro ponto de acesso.

Este processo opera com mensagens com o seguinte formato:

Nome da mensagem : Pedido de reassociação

Tipo da mensagem : Gerenciamento

Subtipo da mensagem : Pedido de reassociação

Itens de informação : Endereço da estação que faz o pedido
 Endereço do ponto de acesso associado
 Endereço do novo ponto de acesso
 Endereço MAC da estação
 Identificador da rede

Sentido : De uma estação para o novo ponto de acesso

Nome da mensagem : Resposta de reassociação

Tipo da mensagem : Gerenciamento

Subtipo da mensagem : Resposta de reassociação

Itens de informação : Sucesso e resultado somente se o MAC estiver cadastrado
 No caso de sucesso, o identificador da nova associação é enviado

Sentido : Do novo ponto de acesso para uma estação

5.5.4 Processo de desassociação

O processo de desassociação é utilizado por uma estação, para que esta deixe de participar da rede local sem fio.

Este processo opera com mensagens com o seguinte formato:

Nome da mensagem : Desassociação

Tipo da mensagem : Gerenciamento

Subtipo da mensagem	: Desassociação
Itens de informação	: Endereço da estação que faz o pedido Endereço do ponto de acesso envolvido
Sentido	: De uma estação para o ponto de acesso ou de um ponto de acesso para uma estação

5.5.5 Processo de autenticação SKA

O processo de autenticação SKA utiliza o algoritmo WEP para validar a estação que solicita a autenticação.

Este processo opera com mensagens com o seguinte formato:

Nome da mensagem	: Autenticação SKA – pacote inicial
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Autenticação
Itens de informação	: Algoritmo de autenticação = SKA Seqüência de transação da autenticação = 1 Identificador da estação Número pseudo-aleatório n1, criptografado
Sentido	: De uma estação para o ponto de acesso

Nome da mensagem	: Autenticação SKA – pacote intermediário
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Autenticação
Itens de informação	: Algoritmo de autenticação = SKA Seqüência de transação da autenticação = 2 $((n1 \text{ xor } n2) \parallel n2)$, criptografados
Sentido	: Do ponto de acesso para uma estação

Nome da mensagem	: Autenticação SKA – pacote intermediário
Tipo da mensagem	: Gerenciamento

Subtipo da mensagem	: Autenticação
Itens de informação	: Algoritmo de autenticação = SKA Sequência de transação da autenticação = 3 $((n2 \text{ xor } n) \parallel \text{SSID})$, criptografados
Sentido	: De uma estação para o ponto de acesso
Nome da mensagem	: Autenticação SKA – pacote final
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Autenticação
Itens de informação	: Algoritmo de autenticação = SKA Sequência de transação da autenticação = 4 Resultado = Sucesso ou Insucesso
Sentido	: Do ponto de acesso para uma estação

5.5.6 Processo de reautenticação

O processo de reautenticação utiliza o algoritmo WEP para revalidar a estação e distribuir nova chave e sessão.

Este processo opera com mensagens com o seguinte formato:

Nome da mensagem	: Reautenticação – pacote inicial
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Reautenticação
Itens de informação	: Algoritmo de reautenticação = SKA Sequência de transação da reautenticação = 1 Identificador da estação Número pseudo-aleatório $n3$, criptografado
Sentido	: Do ponto de acesso para uma estação
Nome da mensagem	: Reautenticação – pacote intermediário
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Reautenticação
Itens de informação	: Algoritmo de reautenticação = SKA

	Seqüência de transação da reautenticação = 2
	$((n3 \text{ xor } n4) \parallel n4)$, criptografados
Sentido	: Da estação para o ponto de acesso
Nome da mensagem	: Reautenticação – pacote final
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Reautenticação
Itens de informação	: Algoritmo de reautenticação = SKA
	Seqüência de transação da reautenticação = 3
	$(n4 \text{ xor } ks)$, criptografados
Sentido	: Do ponto de acesso para uma estação

5.5.7 Processo de desautenticação

O processo de desautenticação é utilizado por uma estação, para que esta deixe de participar da rede local sem fio. Este processo também foi melhorado para evitar que outra estação se passe pela que está deixando a rede.

Este processo opera com mensagens com o seguinte formato:

Nome da mensagem	: Desautenticação – pacote inicial
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Desautenticação
Itens de informação	: Algoritmo de reautenticação = SKA
	Seqüência de transação da desautenticação = 1
	Identificador da estação
	Número pseudo-aleatório $n5$, criptografado
Sentido	: Da estação para o ponto de acesso
Nome da mensagem	: Desautenticação – pacote intermediário
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Desautenticação
Itens de informação	: Algoritmo de reautenticação = SKA

	Seqüência de transação da desautenticação = 2
	$((n5 \text{ xor } n6) \parallel n6)$, criptografados
Sentido	: Do ponto de acesso para uma estação
Nome da mensagem	: Desautenticação – pacote final
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Desautenticação
Itens de informação	: Algoritmo de reautenticação = SKA
	Seqüência de transação da desautenticação = 3
	$(n6 \text{ xor } ks)$, criptografados
Sentido	: Da estação para o ponto de acesso

5.5.8 Processo de revogação

O processo de revogação de chaves é utilizado pelo administrador, que, por meio do ponto de acesso, pode revogar uma determinada chave de sessão. Esta chave teria sido comprometida e não mais se adequaria ao uso na rede.

Este processo opera com mensagens com o seguinte formato:

Nome da mensagem	: Revogação – pacote inicial
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Revogação
Itens de informação	: Algoritmo de revogação = SKA
	Seqüência de transação da reautenticação = 1
	Identificador da estação
	Número pseudo-aleatório $n7$ concatenado a chave de sessão, criptografados
Sentido	: Do ponto de acesso para uma estação
Nome da mensagem	: Revogação – pacote intermediário
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Revogação

Itens de informação	: Algoritmo de revogação = SKA Sequência de transação da reautenticação = 2 $((n7 \text{ xor } n8) \parallel n8)$, criptografados
Sentido	: Da estação para o ponto de acesso
Nome da mensagem	: Revogação – pacote final
Tipo da mensagem	: Gerenciamento
Subtipo da mensagem	: Revogação
Itens de informação	: Algoritmo de revogação = SKA Sequência de transação da reautenticação = 3 $(n8 \text{ xor } ks)$, criptografados
Sentido	: Do ponto de acesso para uma estação

As tabelas 16, 17, 18 e 19 apresentam um resumo da informação trafegada em cada um dos processos, incluindo uma relação de tamanho destes quadros. Estes valores são úteis no momento da avaliação da proposta em termos de *overhead* de tráfego inserido.

Vale notar que o tamanho do campo *Text* é apresentado em *bits*, e o tamanho total do pacote é apresentado em *bytes*.

Nas tabelas a seguir, E_{ks} significa um processo de criptografia (*Encryption*) com a chave secreta ks (chave de sessão), e E_{kc} indica um processo de criptografia com a chave secreta kc (chave pré-compartilhada). O número 34 no campo Total é o tamanho total do cabeçalho: (24 *bytes*) do pacote de gerenciamento mais o FCS (4 *bytes*) do pacote MAC, de acordo com o capítulo 2, mais o cabeçalho do *frame-body* (6 *bytes*). Os outros números componentes da soma exibida no campo Total são a conversão para *bytes* do tamanho do campo “Texto” expressa em *bits* na terceira coluna. Cada número pseudo-aleatório possui 128 *bits*, mantendo a compatibilidade com a chave de 128 *bits* suportada pelas versões mais atuais do WEP. A estação ou o ponto de acesso são identificados por seus endereços MAC com 48 *bits* cada. Conforme [IEEE 1999], o valor do campo SSID possui 32 *bytes* ou 256 *bits*.

Tabela 16 – Processo de autenticação

Seqüência	Texto	Tam. bits	Total bytes
1	$E_{kc}(n1) \parallel id$	176	$22+34=56$
2	$E_{kc}((n1 \text{ xor } n2) \parallel n2)$	256	$32+34=66$
3	$E_{kc}((n2 \text{ xor } n) \parallel SSID)$	384	$48+34=82$
4	Resultado	0	$0+34=34$

Tabela 17 – Processo de reautenticação

Seqüência	Texto	Tam. bits	Total bytes
1	$E_{ks}(n3)$	128	$16+34=50$
2	$E_{ks}((n3 \text{ xor } n4) \parallel n4)$	256	$32+34=66$
3	$E_{ks}(n4 \text{ xor } ks)$	128	$16+34=50$

Tabela 18 – Processo de desautenticação

Seqüência	Texto	Tam. bits	Total bytes
1	$E_{ks}(n5)$	128	$16+34=50$
2	$E_{ks}((n5 \text{ xor } n6) \parallel n6)$	256	$32+34=66$
3	$E_{ks}(n6 \text{ xor } ks)$	128	$16+34=50$

Tabela 19 – Processo de revogação de chaves

Seqüência	Texto	Tam. bits	Total bytes
1	$E_{kc}(n7 \parallel ks)$	256	$32+34=66$
2	$E_{kc}((n7 \text{ xor } n8) \parallel n8)$	256	$32+34=66$
3	$E_{kc}(n8 \text{ xor } ks)$	128	$16+34=50$

5.6 Avaliação da proposta

Esta seção apresenta uma avaliação desta proposta. O objetivo é estimar o desempenho da rede face aos controles adicionados. Além do incremento de tráfego, o cálculo do período de reautenticação é feito com base na carga, número e tamanho de pacotes.

Uma avaliação mais precisa e real somente poderá ser realizada após implementação desta proposta. A implementação desta proposta não está contemplada no escopo deste trabalho, porém vale destacar que a maior dificuldade seria a implementação do lado do cliente, haja vista a necessidade de portar o código desenvolvido como um *driver* para a interface de rede. Já no lado servidor poderia ser adotado um ponto de acesso baseado em Linux, o que evitaria tal trabalho.

5.6.1 *Overhead* de banda inserido

Esta proposta tem um incremento de banda quando comparada com a estrutura do padrão IEEE 802.11. Em especial, pelo fato do padrão não contemplar as mensagens de reautenticação. A tabela 20 descreve o incremento em *bytes* para cada um dos processos.

Tabela 20 – Tamanho dos processos no padrão e na proposta

Fase	IEEE 802.11 em bytes	Proposta em bytes	Incremento em bytes
Autenticação	206	238	32
Reautenticação	0	166	166
Revogação	0	182	182
Desautenticação	40	166	126

Observa-se que as informações da tabela 20 não permitem calcular o incremento gerado na rede de forma real. Para determinar o incremento de tráfego na rede, foi realizado um estudo do perfil dos usuários de uma rede local sem fio. O objetivo do estudo foi a identificação do número médio de processos de autenticação e desautenticação. Com base nessas informações, tornou-se possível uma análise mais aproximada da realidade do tráfego determinado pelas modificações definidas pela proposta apresentada.

A tabela 21 apresenta o resumo do levantamento realizado [Silva e Souza 2003-2]. A tabela foi gerada com base nos *logs* do ponto de acesso e através de um analisador de protocolos, coletado por 5 dias úteis, entre 7 horas da manhã e 7 horas da noite. A rede analisada contém apenas um ponto de acesso, operando a 11Mbps/s, de acordo com o padrão IEEE 802.11 e com o máximo de 7 usuários.

Tabela 21 – Perfil de autenticação e desautenticação

Usuário	Seg.	Ter.	Qua.	Qui.	Sex.	Média
1	3	2	4	0	3	2,4
2	2	2	2	2	2	2
3	5	3	2	2	4	3,2
4	1	1	0	2	1	1
5	6	7	5	6	6	6
6	3	2	2	1	3	2,2
7	0	0	5	4	4	2,6
Média	2,86	2,43	2,86	2,43	3,29	2,77

Com os dados da tabela 21 e com o tamanho dos processos, é calculada a quantidade de tráfego utilizada para implementar os mecanismos de segurança.

Tráfego no padrão IEEE 802.11:

$$2,8 \text{ autenticações} * 7 \text{ usuários} * 206 \text{ bytes} = 4Kbytes$$

$$2,8 \text{ desautenticações} * 7 \text{ usuários} * 40 \text{ bytes} = 0,8Kbytes$$

Com base nesses cálculos, em um dia, cerca de 4,8Kbytes são transmitidos nessa rede com o objetivo de implementar os controles de segurança. O número 206 é o tamanho total de um processo de autenticação, e 40 é o tamanho total de um processo de desautenticação no padrão IEEE 802.11, conforme as tabelas 13 e 15.

Tráfego na proposta apresentada:

$$2,8 \text{ autenticações} * 7 \text{ usuários} * 238 \text{ bytes} = 4,7Kbytes$$

$$2,8 \text{ desautenticações} * 7 \text{ usuários} * 166 \text{ bytes} = 3,2Kbytes$$

$$24 \text{ reautenticações} * 7 \text{ usuários} * 166 \text{ bytes} = 27,8Kbytes$$

Com base nesses cálculos, em um dia, cerca de 36Kbytes são transmitidos nessa rede com o objetivo de implementar os controles de segurança.

De acordo com as tabelas anteriores, o número 238 é o tamanho total de um processo de autenticação, e 166 é o tamanho total de um processo de desautenticação ou reautenticação. O número de reautenticações, 24, foi definido de modo a ocorrer uma reautenticação a cada meia hora. Este valor é calculado como apresentado na seção 5.6.2 deste capítulo, mas deve ainda levar outros fatores em consideração, como, por exemplo, o valor da informação trafegada na rede.

Com base nas informações das tabelas 20 e 21, conclui-se que o incremento em termos de banda inserida na rede por esta proposta é em média de 650%.

O que parece, a priori, ser inviável, um aumento de 650% pode ser muito satisfatório. Comparando a quantidade de tráfego utilizada pelos processos acima com a quantidade total de tráfego transmitida na rede no mesmo período, obtêm-se percentuais pequenos.

Supondo uso da capacidade máxima da rede, no caso do padrão IEEE 802.11, apenas 0,000008% do total do tráfego transmitido na rede é referente aos processos de autenticação e desautenticação. No caso da proposta, apenas 0,00006% do tráfego total transmitido é

referente aos processos de autenticação, reautenticação e desautenticação [Silva e Souza 2003-3]. Estes cálculos baseiam-se na capacidade de transmissão da rede e nos dados calculados anteriormente e são apresentados em seguida. O *overhead* ocasionado pela criptografia dos dados transmitidos não foi levado em consideração, pois existe sem alterações tanto no padrão quanto na proposta.

A capacidade da rede é de 11Mbps/s ou 1,375Mbytes/s, o que equivale a 4,95Gbytes/h. A capacidade multiplicada por 12 horas dá um total de 59,4Gbytes por dia. Considerando um dia formado por 12 horas úteis, como considerado no levantamento de dados na rede local sem fio.

Como, no caso do padrão, 4,8Kbytes são utilizados diariamente pelos controles de segurança e, no caso da proposta, 36Kbytes são utilizados diariamente, tem-se que 0,000008% e 0,00006% do tráfego total são utilizados pelos controles de segurança no padrão e na proposta respectivamente. O cálculo é baseado em uma regra de três simples.

No levantamento observado, a capacidade total da rede não foi atingida, a média de utilização do ponto de acesso girou em torno de 7Mbps/s ou 0,875Mbytes/s, o que equivale a 3,15Gbytes/h ou 37,8Gbytes por dia, novamente contando um dia de 12 horas. A figura 39 mostra o gráfico do tráfego de um dia de utilização da rede, a média das 12 horas é um valor aproximado a 7Mbps/s. Desta forma, com uma utilização da rede menor e com a quantidade de tráfego gasta nos processos de segurança constante, a relação de porcentagem de tráfego utilizada para os controles de segurança sobe um pouco. No caso do padrão, 0,000012% do tráfego é utilizado pelos mecanismos de segurança e, no caso desta proposta, 0,000095%. Estes valores ainda permanecem em patamares completamente aceitáveis, posto que representam muito pouco sobre o tráfego total.

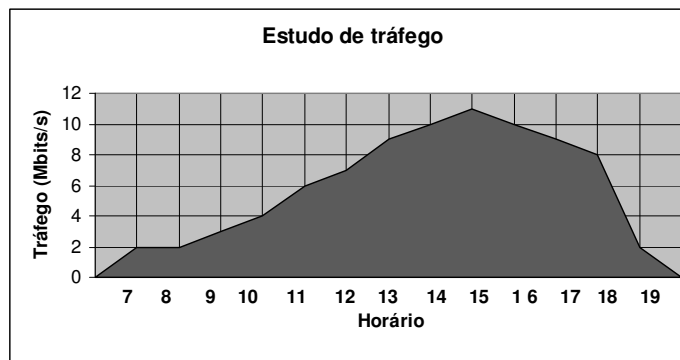


Figura 39 – Gráfico do tráfego da rede em um dia

5.6.2 Período de reautenticação e quebra da chave

Esta seção apresenta considerações sobre o período necessário para quebra da chave WEP e a relação com o período de reautenticação.

O período de reautenticação deve ser cuidadosamente observado. É devido à reautenticação e à distribuição de nova chave de sessão de forma periódica que as fragilidades do protocolo WEP são minimizadas.

Com base no tráfego da rede, calcula-se o tempo necessário para que um invasor possa coletar a quantidade necessária de tráfego que lhe permita revelar as informações transmitidas. Logo, o período de reautenticação deve ser inferior a este tempo.

A análise, a seguir, considera como base o cálculo do número de pacotes que leva à repetição dos valores dos vetores de inicialização. Como o IV tem 3 *bytes*, ou seja, 24 *bits*, existem 2^{24} (16.777.216) possibilidades para este. Assim, em média, a cada 2^{24} pacotes, o valor do IV é repetido.

Considerando que os quadros MAC variam entre 34 (um quadro de dados com o *frame body* vazio) e 2346 *bytes* e que cada pacote utiliza um e apenas um IV, têm-se dois cálculos:

Pior caso, pacotes com tamanho mínimo:

$$2^{24} \text{ pacotes} * 34 \text{ bytes} = 570 \text{ Mbytes} = 4,5 \text{ Gbits}$$

Logo, neste caso, após 4,5*Gbits* transmitidos, o primeiro IV utilizado é considerado novamente.

Melhor caso, pacotes com tamanho máximo:

$$2^{24} \text{ pacotes} * 2346 \text{ bytes} = 40\text{Gbytes} = 320\text{Gbits}$$

De forma análoga, neste caso, após 320*Gbits* transmitidos, o primeiro IV utilizado é considerado novamente.

Para o cálculo dos períodos de reautenticação, considera-se a capacidade total da rede que representa o pior caso. Este é o caso em que a quebra ocorre em menor tempo. Considerando que um ponto de acesso pode transmitir no máximo 11Mbits/s, o que equivale a 39,6Gbits/hora, tem-se que 4,5*Gbits* gastam cerca de 7 minutos para serem transmitidos, e 320*Gbits* cerca de 8 horas. Logo, nestes casos, os períodos de reautenticação devem ser menores que os referidos tempos.

Considerando-se a média de utilização observada igual a 7Mbits/s, o que equivale a 25,2Gbits/hora, tem-se que os 4,5*Gbits* necessários para a quebra, com pacotes em menor tamanho, gastam cerca de 11 minutos para serem coletados. Quando se consideram os pacotes com tamanho máximo, os 320*Gbits* gastam cerca de 12 horas e meia para serem coletados [Silva e Souza 2003-2].

5.7 Outras medidas para melhorar a segurança das redes locais sem fio

Um dos princípios básicos da segurança é trabalhar os mecanismos de defesa em camadas, ou seja: vários níveis de proteção.

Existem algumas ações, que, seguindo esse princípio, elevam consideravelmente o nível de segurança das redes locais sem fio. Neste caso, o objetivo não é eliminar as vulnerabilidades existentes, como estudado até aqui, mas, sim, fazer com que essas fraquezas não possam ser exploradas, ou, se exploradas, que o objetivo da ação não tenha sucesso.

Muitas ações são possíveis, dentre elas, algumas destacadas em [Craig 2002] e [Arora 2003]:

5.7.1 Projeto físico da cobertura dos pontos de acesso

Os pontos de acesso das redes locais sem fio não devem ser instalados aleatoriamente, baseados somente em estética ou em pequenos testes. Deve existir um projeto adequado, que leve em conta todos os raios de coberturas, não somente com o foco em maximizar a qualidade e área de cobertura, mas também como o foco em tentar manter a área de cobertura o mais interna à área física possível, ou seja, tentar evitar que o sinal da rede seja propagado para o estacionamento ou para empresa ao lado. Não raro, simples ajustes podem permitir ganhos significativos neste sentido.

5.7.2. Habilitação de todos os mecanismos de segurança existentes

Como já discutido, cada fabricante agrega alguns mecanismos de proteção em seus equipamentos. Entretanto muitos mecanismos são vulneráveis, mas, ainda assim, um estudo de viabilidade deve ser feito no sentido de habilitá-los, a não ser que a vulnerabilidade leve a um risco ainda maior do que quando comparado com o risco da inexistência do referido mecanismo. Na maioria das vezes, tais mecanismos podem ser quebrados por usuários avançados, mas, mesmo assim, agregam proteção a usuários menos experientes e menos determinados a quebrar a segurança do ambiente.

Estes mecanismos incluem:

- habilitar a Rede Fechada, que é o não envio do SSID por *broadcast*;
- troca do SSID padrão por um outro valor;
- uso do WEP em todos os pontos de acesso;
- uso da filtragem MAC, incluindo uma lista dos usuários da rede;
- evitar o uso de DHCP na rede sem fio;
- uso do padrão IEEE 802.1X quando possível;
- uso de múltiplas chaves WEP quando possível;
- escolha de boas senhas e chaves com troca periódica.

5.7.3 Uso de VPN (*Virtual Private Network*)

O uso de proteção no nível IP ou superiores, como VPN's IPSec (*Internet Protocol Secure*), SSL (*Secure Sockets Layer*) e outros, garantem a confidencialidade e integridade independente das vulnerabilidades na rede sem fio. Além disso, a VPN colabora em muito no controle de acesso, pois, ainda que se permita acesso não autorizado a rede sem fio, não se terá acesso a rede da VPN. Sabe-se que a VPN agrega *overhead*, portanto, um estudo deve ser feito para identificar se as aplicações que operam nesse ambiente suportarão tal *overhead*.

5.7.4 Utilização de *firewall* e IDS

Sempre que possível, deve-se utilizar sistemas de *firewall* e IDS (*Intrusion Detection System*) segregando as redes conectadas e provendo maior poder de identificação de ataques em progresso.

5.7.5 Monitoração e gerenciamento

Monitorar a rede local sem fio, gerenciar os pontos de acesso e analisar seus *logs*, são ações muito úteis no sentido de identificar comportamentos anômalos.

Existem ferramentas que podem detectar endereços MAC anômalos, pontos de acesso falsos, ferramentas que injetam tráfego e outras, conforme descrito em [Wright 2003].

5.7.6 Constante atualização

O *software* e *firmware* dos pontos de acesso e das interfaces de rede sem fio devem ser constantemente atualizados.

CONCLUSÃO

O estudo realizado sobre as redes locais sem fio, seus padrões e suas vulnerabilidades, permitiu ao autor um bom entendimento das fraquezas e perigos associados à utilização das redes locais sem fio.

Com isso, foi possível a condução de um teste de invasão, bem sucedido, em um ambiente de testes que possui, habilitados, os principais mecanismos de proteção disponíveis no mercado.

Assim, foi produzida uma proposta que elimina grande parte das atuais vulnerabilidades e minimiza outras. A proposta considera a utilização do mesmo *hardware* disponível atualmente, conseguindo elevar o nível de segurança desses ambientes sem a necessidade de expansão de *hardware*. A proposta, embora não implementada, foi avaliada de forma teórica. Tal avaliação se baseia em um estudo de caso realizado em uma rede local sem fio real em operação.

Certamente, esta proposta pode auxiliar no desenvolvimento de novas soluções para redes locais sem fio e, como trabalho futuro, sua implementação pode ser desenvolvida. Durante a elaboração dessa dissertação o IEEE estava trabalhando no padrão 802.11i, assim este trabalho contemplou apenas o padrão WPA, que antecipou o 802.11i, pois quando este foi publicado o escopo e produção desta dissertação já estava fechado e finalizado. Assim, outros trabalhos futuros incluem a avaliação do IEEE 802.11i quanto aos requisitos de segurança.

Finalmente, outra linha de trabalho, já em desenvolvimento e com a participação do autor desta dissertação consiste no uso do protocolo SRP (*Secure Remote Password*) para as funcionalidades de segurança das redes locais sem fio.

REFERÊNCIAS BIBLIOGRÁFICAS

AGERE, S., Agere Systems v7.82 NDIS 5.x Miniport Driver, 2002. Disponível em <http://www.wildpackets.com/support/hardware/ap_lucent_driver/lucent6.28driver.exe>.

Acesso em Dezembro de 2003.

ARBAUGH, W., WAN, Y. e SHANKAR, N., Your 802.11 Wireless Network has No Clothes, Março de 2001. Disponível em <<http://www.cs.umd.edu/~waa/wireless.pdf>>. Acesso em Dezembro de 2003.

ARORA, R., State of Affairs of Wireless Networks, Janeiro de 2003. Disponível em <<http://www.sans.org/rr/papers/index.php?id=944>>. Acesso em Janeiro de 2004.

BORISOV, N., GOLDBERG, I., WAGNER, D., Detecting Wireless LAN MAC Address Spoofing , Julho de 2001. Disponível em <<http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>>. Acesso em Março de 2004.

COMBS, G., Ethereal, 2004. Disponível em <<http://www.ethereal.com/distribution/win32/>>. Acesso em Dezembro de 2004.

CRAIGER, J., 802.11, 802.1X, and Wireless Security, Junho de 2002. Disponível em <<http://www.sans.org/rr/papers/index.php?id=171>>. Acesso em Dezembro de 2003.

DESPHANDE, S., Who's watching your wireless network? , Fevereiro de 2003. Disponível em <<http://www.cs.plu.edu/courses/netsec/arts/wp.pdf> >. Acesso em Dezembro de 2003.

ETTER, A., A Guide to Wardriving and Detecting Wardrivers, Setembro de 2002. Disponível em <<http://www.sans.org/rr/papers/68/174.pdf>>. Acesso em Janeiro de 2004.

FERGUSON, N. e SCHNEIER, B., Practical Cryptography, Wiley Publishing, 2003.

FLUHRER, S., MARTIN, I. e SHAMIR, A., Weaknesses in the Key Scheduling Algorithm of RC4, Julho de 2001. Disponível em <http://www.crypto.com/papers/others/rc4_ksaproc.ps>. Acesso em Março de 2004.

GORLANI, M., MACMakeUp, 2003. Disponível em <<http://www.gorlani.com/publicprj/macmakeup/itmacmakeup.asp>>. Acesso em Janeiro de 2005.

HUEY, B., Penetration Testing On 802.11b Networks, Fevereiro de 2003. Disponível em <<http://www.sans.org/rr/papers/index.php?id=167>>. Acesso em Janeiro de 2004.

IEEE Std 802.11-1999. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Março de 1999.

IEEE Std 802.1X-2001. Port-Based Network Access Control. Junho de 2001.

KERSHAW, M., Kismet Wireless, 2003. Disponível em <<http://www.kismetwireless.net/>>. Acesso em Dezembro de 2004.

LAWRENCE, B., Tcpdump, 2002. Disponível em < <http://www.tcpdump.org/> >. Acesso em Dezembro de 2004.

LAWRENCE, B., WinDump: tcpdump for Windows, 2004. Disponível em < <http://www.winpcap.org/windump/> >. Acesso em Dezembro de 2004.

LIM, K., Security Guidelines for Wireless LAN Implementation, Agosto de 2003. Disponível em <<http://www.sans.org/rr/papers/68/1233.pdf>>. Acesso em Dezembro de 2003.

MAHAN, R., Security in Wireless Network, Novembro de 2001. Disponível em <<http://www.sans.org/rr/papers/index.php?id=157>>. Acesso em Dezembro de 2003.

MILNER, M., NetStumbler, 2002. Disponível em <<http://www.netstumbler.com/>>. Acesso em Dezembro de 2004.

MISHRA, A. e ARBAUGH, W., An Initial Security Analysis of the IEEE 802.1X Standard, Fevereiro de 2002. Disponível em <<http://www.cs.umd.edu/~waa/1x.pdf>>. Acesso em Dezembro de 2003.

MOSKOWITZ, R., Weakness in Passphrase Choice in WPA Interface, Novembro de 2003. Disponível em <<http://wifinetnews.com/archives/002452.html>>. Acesso em Janeiro de 2004.

ORINOCO, Firmware Orinoco Gold Winter 2001, 2001. Disponível em <ftp://ftp.orinocowireless.com/pub/software/ORiNOCO/pc_card/win_2000/R6.4winter2001>. Acesso em Dezembro de 2003.

ORINOCO, ORiNOCO security paper v2.2, 2003. Disponível em <<http://www.umanitoba.ca/campus/acn/reports/wireless-security.pdf>>. Acesso em Setembro de 2003.

OW, E., IEEE 802.11b Wireless LAN: Security Risks, Setembro de 2001. Disponível em <<http://www.sans.org/rr/papers/68/151.pdf>>. Acesso em Março de 2004.

PEIKARI, C. e FOGIE, S., Wireless Maximum Security, SAMS Publishing, 2003.

PERES, A. e WEBER, R., Considerações sobre Segurança em Redes Sem Fios. In: III WORKSHOP EM SEGURANÇA DE SISTEMAS COMPUTACIONAIS. Maio de 2003.

RAGER, A., WEPCrack, 2002. Disponível em <<http://wepcrack.sourceforge.net/>>. Acesso em Dezembro de 2004.

ROSHAN, P., 802.11 Wireless LAN Security White Paper, 2002. Disponível em <http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf>. Acesso em Dezembro de 2003.

SEEBACH, P., Building a wireless access point in linux, Julho de 2003. Disponível em <<ftp://www6.software.ibm.com/software/developer/library/l-wap.pdf>>. Acesso em Dezembro de 2003.

SHMOO, G., Airtsnort, 2002. Disponível em <<http://airsnort.shmoo.com/>>. Acesso em Dezembro de 2004.

SILVA, G. e SOUZA, J., Uma análise dos mecanismos de segurança das redes locais sem fios e uma proposta de melhoria. In: III WORKSHOP EM SEGURANÇA DE SISTEMAS COMPUTACIONAIS. Maio de 2003.

SILVA, G. e SOUZA, J., Proposta de melhoria dos mecanismos de segurança das redes locais sem fios. In: V SIMPÓSIO DE SEGURANÇA EM INFORMÁTICA. Novembro de 2003 [2].

SILVA, G. e SOUZA, J., Estudo e melhoria dos mecanismos de segurança em redes locais sem fios. In: INTERNATIONAL INFORMATION AND TELECOMMUNICATION TECHNOLOGIES. Novembro de 2003 [3].

STALLINGS, W., Cryptography and Network Security, Prentice Hall, 1998.

STONE, A., The Michael Vulnerability, Dezembro de 2003. Disponível em < <http://www.wi-fiplanet.com/columns/article.php/1556321>>. Acesso em Janeiro de 2004.

WALKER, J., Unsafe at any key size; An analysis of the WEP encapsulation, Outubro de 2000. Disponível em <<http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip>>. Acesso em Dezembro de 2003.

WONG, S., The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards, Maio de 2003. Disponível em <<http://www.sans.org/rr/papers/68/1109.pdf>>. Acesso em Dezembro de 2003.

WRIGHT, J., Detecting Wireless LAN MAC Address Spoofing, Janeiro de 2003. Disponível em <<http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf>>. Acesso em Janeiro de 2004.