



**Sergio Henrique Sirufo**

**Análise de Desempenho de Redes  
IEEE 802.11b Utilizando  
Mecanismos de Segurança**

**Dissertação de Mestrado**

Dissertação apresentada como requisito parcial para obtenção do título de Mestre pelo Programa de Pós-Graduação em Engenharia Elétrica do Departamento de Engenharia Elétrica da PUC-Rio.

Orientador: Prof. Luiz Alencar Reis da Silva Mello

Co-orientador: Prof. Rodolfo Sabóia Lima de Souza

Rio de Janeiro

Maio de 2005



**Sergio Henrique Sirufo**

**Análise de Desempenho de Redes  
IEEE 802.11b Utilizando  
Mecanismos de Segurança**

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-Graduação em Engenharia Elétrica do Departamento de Engenharia Elétrica do Centro Técnico Científico da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

**Prof. Luiz Alencar Reis da Silva Mello**  
**Orientador**

Centro de Estudos em Telecomunicações - PUC-Rio

**Prof. Rodolfo Sabóia Lima de Souza**  
**Co-Orientador**

Centro de Estudos em Telecomunicações - PUC-Rio

**Prof. Ewerton Longoni Madruga**  
Universidade Estácio de Sá

**Prof. Luiz Henrique da Costa Araújo**  
IME

**Prof. José Eugenio Leal**  
Coordenador Setorial do Centro  
Técnico Científico - PUC-Rio

Rio de Janeiro, 31 de maio de 2005

Todos os direitos reservados. É proibida a reprodução total ou, parcial do trabalho sem autorização da universidade, do autor e do orientador.

### **Sergio Henrique Sirufo**

Graduou-se em Engenharia Eletrônica pelo Instituto Militar de Engenharia – IME em 1991. Coursou Pós-Graduação *Lato-sensu* em redes de Computadores, em 2000, e Sistemas de Telecomunicações, em 1998, ambos pelo CCE/PUC-Rio. Responsável pelo planejamento, implantação e gerência de projetos em redes do Exército no âmbito do RJ e ES, utilizando tecnologias de comunicação ótica e wireless.

#### Ficha Catalográfica

Sirufo, Sergio Henrique

Análise de desempenho de redes IEEE 802.11b utilizando mecanismos de segurança / Sergio Henrique Sirufo ; orientador: Luiz Alencar Reis da Silva Mello ; co-orientador: Rodolfo Sabóia Lima de Souza. – Rio de Janeiro : PUC, Departamento de Engenharia Elétrica, 2005.

162 f. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Engenharia Elétrica.

Inclui referências bibliográficas.

1. Engenharia elétrica – Teses. 2. WLAN. 3. WEP. 4. IEEE 802.1x. 5. EAP. 6. TLS. I. Mello, Luiz Alencar Reis da Silva. II. Souza, Rodolfo Sabóia Lima de. III. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Engenharia Elétrica. III. Título.

CDD: 621.3

## Agradecimentos

À minha família, em especial, minha esposa, pelo incentivo e compreensão durante o período do desenvolvimento deste trabalho.

Ao Professor Rodolfo Sabóia Lima de Souza pela orientação, entusiasmo e parceria para a realização deste trabalho.

Ao Cel Alberto Tavares da Silva e TC Clayton Jones Alves da Silva, chefes do 2º CTA, Órgão do Exército Brasileiro, pelo apoio concedido, sem o qual este trabalho não poderia ter sido realizado.

A todos os amigos e familiares que de uma forma ou de outra me estimularam ou me ajudaram.

## Resumo

Sirufo, Sergio Henrique; Silva Mello, Luiz Alencar Reis (Orientador). **Análise de Desempenho de Redes IEEE 802.11b Utilizando Mecanismos de Segurança.** Rio de Janeiro, 2005. 162p. Dissertação de Mestrado – Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Enquanto o uso das WLAN cresce em ritmo acelerado, inúmeros problemas relacionados à tecnologia de segurança, definida no IEEE 802.11b, têm sido abordados em publicações técnicas, apontando deficiências e vulnerabilidades, através dos quais indivíduos não autorizados podem ter acesso às informações disponibilizadas pela rede. A precariedade na autenticação, confidencialidade e integridade dos dados dos mecanismos internos do Padrão IEEE 802.11b exige a operação conjunta com o Padrão IEEE 802.1x. Esta combinação possibilita a autenticação e criptografia dos dados de forma mais eficiente e confiável. No entanto, é possível que haja sobrecarga de pacotes, devido à inserção de tráfego extra para autenticação dos usuários e criptografia das mensagens, podendo ocasionar comprometimento na *performance* da rede. Desta forma, avaliou-se qual a efetiva degradação no desempenho das redes IEEE 802.11b, devido à implementação dos mecanismos de segurança, sejam eles intrínsecos ao Padrão ou combinados com o Padrão IEEE 802.1x, utilizando os protocolos FTP (*File Transfer Protocol*) e HTTP (*Hipertext Transfer Protocol*).

## Palavras-chave

WLAN; WEP; IEEE 802.1x; EAP; TLS.

## Abstract

Sirufo, Sergio Henrique; Silva Mello, Luiz Alencar Reis (Advisor). **Performance Analysis of IEEE 802.11b Networks by Means of Security Mechanisms**. Rio de Janeiro, 2005. 162p. MSc. Dissertation – Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Meanwhile the use of WLAN grows in accelerate pass, a large number of problems related to the security issues in the IEEE 802.11b have been discussed in technical papers, pointing vulnerabilities and deficiencies, from where a non authorized access to the informations passing on the network could be possible. The lack of strong solutions in authentication, confidentiality, and integrity of the data in the internal mechanisms of the protocol IEEE 802.11b, demands to operate in conjunction with the protocol IEEE 802.1x. Therefore it is possible to get authentication and cryptography in a efficient and trustful manner. The amount of extra packets, inserted for authentication and cryptography of the messages, could have a negative impact in the performance of the network. A experimental measurements of the degradation of the network throughput, when the mechanisms of IEEE 802.1x are used, were done and presented here.

## Keywords

WLAN; WEP; IEEE 802.1x; EAP; TLS.

# Sumário

1	Introdução	15
1.1	Motivação	16
1.2	Objetivo	18
1.3	Composição da Dissertação	20
2	Padrão IEEE 802.11	21
2.1	Topologia	22
2.2	Estrutura das Camadas do Padrão IEEE 802.11	23
2.3	Camada Física	24
2.3.1	Operações da Camada Física	25
2.3.1.1	Detecção de Portadora	26
2.3.1.2	Transmissão	26
2.3.1.3	Recepção	27
2.3.2	<i>Frequency Hopping Spread Spectrum</i> (FHSS)	27
2.3.3	<i>Direct Sequence Spread Spectrum</i> (DSSS)	29
2.4	Camada de Enlace	31
2.4.1	Controle de Acesso ao Meio (MAC)	31
2.4.2	DCF ( <i>Distributed Coordination Function</i> )	33
2.4.3	PCF ( <i>Point Coordination Function</i> )	34
2.4.4	Pacotes da Camada MAC	40
2.4.4.1	Quadro MAC	40
2.4.4.2	Campo FC – <i>Frame Control</i>	42
2.4.4.3	Pacotes de Controle	43
2.4.4.4	Pacote de Dados	45
2.5	Serviços em Redes IEEE 802.11	45
2.5.1	Tipos de Mensagens	45
2.5.2	Serviços de Estação	46
2.5.3	Serviços de Sistema de Distribuição	47
3	Aspectos e Mecanismos de Segurança no Padrão IEEE 802.11	49
3.1	Redes com Fio x Redes sem Fio	49
3.2	Mecanismos Básicos de Segurança no Padrão IEEE 802.11	50
3.2.1	Controle de Acesso pela Identificação do Endereço MAC ( <i>MAC Address Filtering</i> )	50
3.2.2	Controle de Acesso pela Identificação do SSID ( <i>Network ID</i> )	51
3.3	WEP – <i>Wired Equivalent Privacy</i>	52
3.3.1	Características	52
3.3.2	Tipo de Criptografia	53
3.3.3	Algoritmo RC4	55
3.3.4	Criptografia no WEP	55
3.3.5	Autenticação no WEP	58
3.3.6	Integridade no WEP	61
3.3.7	Fragilidades e Vulnerabilidades do WEP	61
3.3.7.1	Fragilidade na Criptografia	61
3.3.7.2	Fragilidade Provocada pelo Vetor de Inicialização	62
3.3.7.3	Fragilidade na Integridade dos Dados	63

3.3.7.4 Fragilidade na Autenticação (Controle de Acesso)	65
3.3.7.5 Gerenciamento da Chave Secreta	66
3.3.8 Ameaças mais Importantes	67
3.3.9 Conclusão sobre o WEP	68
3.4 Padrão IEEE 802.1x ( <i>Port-Based Network Access Control</i> )	69
3.5 Protocolo EAP - <i>Extensible Authentication Protocol</i>	71
3.6 Servidor RADIUS	74
3.6.1 Autenticação no Padrão IEEE 802.1x	75
3.7 Protocolo TLS – Transport Layer Security	77
3.8 Protocolo EAP- TLS	81
3.9 Protocolo PEAP - Protected Extensible Authentication Protocol	86
3.10 Protocolo EAP-TTLS - Tunnuled Transport Layer Security	92
3.11 Protocolo LEAP - Lightweight Extensible Authentication Protocol	94
4 Metodologia e Implementação	95
4.1 Objetivo do Trabalho	96
4.2 Mecanismos de Segurança	96
4.3 Medidas de Desempenho	98
4.4 Procedimentos para Medição	99
4.5 Protocolos de Aplicação	99
4.6 Equipamentos Utilizados	100
4.7 Softwares e Ferramentas Utilizadas	102
4.8 Configuração da Arquitetura de Rede	103
4.8.1 Arquitetura Sem Autenticação Externa	103
4.8.2 Arquitetura Com Autenticação Externa	104
4.9 Operação da Rede Sem o AP	106
4.10 Operação da Rede Com Vários Clientes	107
4.10.1 Operação da Rede Com 02 Clientes	107
4.10.2 Operação da Rede Com 03 Clientes	110
4.10.3 Operação da Rede Com 04 Clientes	110
5 Avaliação e Análise dos Resultados	111
5.1 Experimentos Realizados	111
5.2 Sistema Sem Autenticação Externa	112
5.3 Sistema com Autenticação Externa	116
5.4 Análise do Impacto dos Mecanismos no Desempenho	120
5.5 Avaliação do Tempo de Autenticação	122
5.6 Avaliação do Desempenho com Vários Clientes	129
5.6.1 Avaliação do Desempenho com 02 Clientes	130
5.6.1.1 Clientes Configurados a 11Mbps	130
5.6.1.2 Clientes Configurados a 1Mbps e 11Mbps	131
5.6.2 Avaliação do Desempenho com 03 e 04 Clientes	133
6 Conclusão	135
6.1 Tecnologias Emergentes	138
6.2 Sugestões para Trabalhos Futuros	141
7 Referências Bibliográficas	142
Apêndice A: Tabelas com as Medidas Realizadas	146

## Lista de Figuras

Figura 1 - Sistema ESS	22
Figura 2 - Arquitetura com um AP	23
Figura 3 - Arquitetura sem AP	23
Figura 4 - Estrutura das camadas do padrão IEEE 802.11	24
Figura 5 - Estrutura da Camada Física	25
Figura 6 - Transmissão FHSS	28
Figura 7 - Formato do pacote PLCP para o FHSS	28
Figura 8 - Espectro de frequência do DSSS	30
Figura 9 - Formato do Pacote PLCP para o DSSS	30
Figura 10 - Estrutura da Subcamada MAC	34
Figura 11 - Períodos de acesso com e sem contenção	35
Figura 12 - Exemplo de funcionamento do CFP	35
Figura 13 - Problema da EM escondida	36
Figura 14 - Problema de colisão ( <i>hidden node</i> )	37
Figura 15 - Transmissão com quadros RTS e CTS	38
Figura 16 - Transmissão com quadros RTS e CTS ( <i>Four-Way Handshake</i> )	38
Figura 17 - Transmissão entre as EM A e B com reserva de recursos	39
Figura 18 - Intervalos de tempo que diferentes pacotes devem aguardar	40
Figura 19 - Formato do Quadro MAC	40
Figura 20 - Formato do Campo FC	42
Figura 21 - Formato do Pacote RTS	43
Figura 22 - Formato do Pacote CTS	44
Figura 23 - Formato do Pacote ACK	44
Figura 24 - Formato do Pacote <i>PS-Poll</i>	44
Figura 25 - Formato do Pacote <i>CF End</i>	45
Figura 26 - Formato do Pacote de Dados	45
Figura 27 - Diagrama de Estados - Autenticação e Associação	48
Figura 28 - Esquema de criptografia com chave simétrica	54
Figura 29 - Mecanismo de formação da chave Pseudo-Radômica	56
Figura 30 - Cifragem dos dados no WEP	57
Figura 31 - Cifragem dos dados no WEP (Diagrama em Blocos)	57
Figura 32 - Decifragem dos dados no WEP (Diagrama em Blocos)	58
Figura 33 - Troca de mensagens no sistema aberto	59
Figura 34 - Troca de mensagens no sistema com autenticação através da chave compartilhada	60
Figura 35 - Fluxo de mensagens no sistema com autenticação através da chave compartilhada	60
Figura 36 - Fluxo de mensagens entre duas estações	64
Figura 37 - Configuração básica do padrão IEEE 802.1x	70
Figura 38 - Formato do pacote EAP	73
Figura 39 - Pilha de protocolos IEEE 802.1x/RADIUS sobre uma rede IEEE 802.11	73
Figura 40 - Formato do pacote RADIUS	75
Figura 41 - Troca de mensagens para autenticação	77
Figura 42 - Mensagens trocadas entre cliente-servidor durante o	

	<i>handshake</i>	79
Figura 43 -	Seqüência de comandos no <i>handshake</i> para realizar a autenticação do servidor e do cliente	81
Figura 44 -	Configuração do Windows XP (EAP-TLS)	82
Figura 45 -	Conceito da solução baseada na autenticação EAP-TLS	83
Figura 46 -	Seqüência de comandos do mecanismo EAP-TLS	85
Figura 47 -	Esquema de autenticação PEAP (Túnel TLS)	86
Figura 48 -	Esquema de autenticação PEAP	87
Figura 49 -	Configuração do Windows XP (PEAP)	87
Figura 50 -	Conceito da solução baseada na autenticação PEAP	89
Figura 51 -	Seqüência de comandos do mecanismo PEAP	91
Figura 52 -	Esquema de Autenticação EAP-TTLS (Túnel TLS)	91
Figura 53 -	Configuração do Windows XP (EAP-TTLS)	93
Figura 54 -	Medição do tempo de resposta	99
Figura 55 -	Especificação da rede sem autenticação externa	103
Figura 56 -	Configuração da rede sem autenticação externa	104
Figura 57 -	Especificação da rede com autenticação externa	105
Figura 58 -	Configuração da rede com autenticação externa	105
Figura 59 -	Configuração da rede sem AP (Operação com HUB)	106
Figura 60 -	Configuração da rede sem AP (Operação com <i>Switch</i> )	107
Figura 61 -	Configuração da rede com 02 usuários configurados em 11Mbps	109
Figura 62 -	Configuração da rede com 02 usuários configurados em 11Mbps e 1Mbps	110
Figura 63 -	Valor médio de <i>throughput</i> - sem autenticação externa (Tráfego FTP)	114
Figura 64 -	Valor médio do tempo de resposta - sem autenticação externa (Tráfego FTP)	114
Figura 65 -	Valor médio de <i>throughput</i> - sem autenticação externa (Tráfego HTTP)	115
Figura 66 -	Valor médio do tempo de resposta - sem autenticação externa (Tráfego HTTP)	115
Figura 67 -	Valor médio de <i>throughput</i> (Tráfego FTP)	118
Figura 68 -	Valor médio do tempo de resposta (Tráfego FTP)	118
Figura 69 -	Valor médio de <i>throughput</i> (Tráfego HTTP)	119
Figura 70 -	Valor médio do tempo de resposta (Tráfego HTTP)	119
Figura 71 -	Tempo de Autenticação	125
Figura 72 -	Autenticação EAP-TLS (Medição no Coletor)	126
Figura 73 -	Autenticação EAP-TLS (Medição no Cliente)	126
Figura 74 -	Autenticação PEAP (Medição no Coletor)	127
Figura 75 -	Autenticação PEAP (Medição no Cliente)	127
Figura 76 -	Autenticação EAP-TTLS (Medição no Coletor)	128
Figura 77 -	Autenticação EAP-TTLS (Medição no Cliente)	128
Figura 78 -	Autenticação LEAP (Medição no Coletor)	129
Figura 79 -	Valor médio de <i>throughput</i> (01 à 04 Clientes)	133
Figura 80 -	Valor médio do tempo de resposta (01 à 04 Clientes)	134
Figura 81 -	Evolução da Criptografia	139
Figura 82 -	<i>Frames</i> no WEP e TKIP	139
Figura 83 -	Geração da Chave Pseudo-randômica no WEP	140
Figura 84 -	Geração da Chave Pseudo-randômica no TKIP	140

## Lista de Tabelas

Tabela 1 -	Velocidade do DSSS	30
Tabela 2 -	Possíveis combinações de <i>ToDS/FromDS</i>	42
Tabela 3 -	Comparativo dos métodos de autenticação EAP	72
Tabela 4 -	Consolidação dos valores médios de <i>Throughput</i> e Tempo de Resposta (mecanismos sem autenticação externa)	113
Tabela 5 -	Consolidação dos valores médios de <i>throughput</i> e tempo de resposta (todos os mecanismos)	117
Tabela 6 -	<i>Throughput</i> e Tempo de Resposta (HUB)	120
Tabela 7 -	<i>Throughput</i> e Tempo de Resposta ( <i>Switch</i> )	121
Tabela 8 -	Consolidação dos valores médios do tempo de autenticação	124
Tabela 9 -	Consolidação dos valores médios de <i>throughput</i> e tempo de resposta (02 Clientes à 11Mbps)	130
Tabela 10-	Consolidação dos valores médios de <i>throughput</i> e tempo de resposta (02 Clientes à 1Mbps e 11Mbps)	132
Tabela 11-	Consolidação dos valores médios de <i>throughput</i> e tempo de resposta (01 à 04 Clientes à 11Mbps)	133

## Lista de Siglas

AAA	<i>Authorization, Authentication, and Accounting</i>
ACK	<i>Acknowledgment Frame</i>
AES-CCMP	<i>Advanced Encryption Standard – CCM Protocol</i>
AP	<i>Access Point</i>
ASP	<i>Application Solution Provider</i>
BSA	<i>Basic Service Area</i>
BSS	<i>Basic Service Set</i>
BSSID	<i>Basic Service Set Identification</i>
CA	<i>Autoridade Certificadora</i>
CCK	<i>Complementary Code Keying</i>
CFP	<i>Contention Free Period</i>
CRC	<i>Check Redundancy Cyclic</i>
CSMA/CA	<i>Carrier Sense Multiple Access with Collision Avoidance</i>
CSMA/CD	<i>Carrier Sense Multiple Access with Collision Detection</i>
CTS	<i>Clear to Send</i>
DA	<i>Destination Address</i>
DBPSK	<i>Differential Binary Phase Shift Keying</i>
DCF	<i>Distributed Coordination Function</i>
DHCP	<i>Dynamic Host Control Protocol</i>
DIFS	<i>Distributed Interframe Space</i>
DoS	<i>Negação de serviço</i>
DQPSK	<i>Differential Quadrature Phase Shift Keying</i>
DS	<i>Distribution System</i>
DSS	<i>Distribution System Service</i>
DSSS	<i>Direct Sequence Spread Spectrum</i>
EAP	<i>Extensible Authentication Protocol</i>
EAP-GTC	<i>EAP - Generic Token Card</i>
EAPoL	<i>EAP Over Lan</i>
EAP-OTP	<i>EAP - One-Time Passwords</i>
EAP-SIM	<i>EAP - Subscriber Identity Module</i>
EAP-TLS	<i>EAP - Transport Layer Security</i>
EAP-TTLS	<i>EAP - Tunnuled Transport Layer Security</i>
EIFS	<i>Extended Interframe Space</i>
ESA	<i>Extended Service Área</i>
EM	<i>Estação Móvel</i>
ESS	<i>Extended Service Set</i>
FB	<i>Frame Body</i>
FC	<i>Frame Control</i>
FCS	<i>Frame Check Sequence</i>
FHSS	<i>Frequency Hopping Spread Spectrum</i>
FSK	<i>Frequency Shift Keying</i>
FTP	<i>File Transfer Protocol)</i>
HER	<i>Header Error Check</i>
HTTP	<i>Hipertext Transfer Protocol</i>

IBSS	<i>Independent Basic Service Set</i>
ICV	<i>Integrity Check Value</i>
IEEE	<i>Institute for Electrical and Eletronic Engineers</i>
IETF	<i>Internet Engineering Task Force</i>
IP	<i>Internet Protocol</i>
ISM	<i>Industrial, Scientific and Medical</i>
ISP	<i>Internet Solution Provider</i>
ITU	<i>International Telecommunications Union</i>
IV	<i>Inicialization Vector</i>
LAN	<i>Local Area Network</i>
LEAP	<i>Lightweight Extensible Authentication</i>
LLC	<i>Logical Link Control</i>
MAC	<i>Medium Access Control (Controle de Acesso ao Meio)</i>
MD5	<i>Message-Digest Algorithm</i>
MIC	<i>Message Integrity Check</i>
MITM	<i>Man in the Middle</i>
MPDU	<i>MAC Protocol Data Unit</i>
MS-CHAPv2	<i>Microsoft Challenge Authentication Protocol versão 2</i>
MSDU	<i>MAC Service Data Unit</i>
NAS	<i>Network Access Server</i>
NAV	<i>Network Allocation Vector</i>
NIST	<i>US National Institutes of Standards and Technology</i>
OFDM	<i>Orthogonal Frequency Domain Multiplexing</i>
PC	<i>Point Coordination</i>
PCF	<i>Point Coordination Function</i>
PEAP	<i>Protected Extensible Authentication Protocol</i>
PIFS	<i>Priority Interframe Space</i>
PKI	<i>Public Key Infrastructure</i>
PLCP	<i>Phisical Layer Convergence Procedure</i>
PLW	<i>PSDU Length Word</i>
PMD	<i>Phisical Médium Dependent</i>
PPDU	<i>PLCP Packet Data Unit</i>
PRGA	<i>Pseudo-Random Generating Algorithm</i>
PSF	<i>PLCP Signaling Field</i>
QoS	<i>Quality of Service</i>
RA	<i>Receiver Address</i>
RADIUS	<i>Remote Authentication Dial-In User Service</i>
RC4	<i>Ron's Cipher 4</i>
RFC	<i>Request for Comments</i>
RSN	<i>Robust Security Network</i>
RTS	<i>Request to Send</i>
SA	<i>Source Address</i>
SC	<i>Sequence Control</i>
SFD	<i>Start Frame Delimiter</i>
SIFS	<i>Short Interframe Space</i>
SS	<i>Station Service</i>
SSID	<i>Service Set Identification</i>
TA	<i>Transmitter Address</i>
TKIP	<i>Temporal Key Integrity Protocol</i>
TLS	<i>Transport Layer Security</i>

WECA  
WEP  
WLAN  
WPA

*Wi-Fi Ethernet Compatibility Alliance*  
*Wired Equivalent Privacy*  
*Wireless Local Area Network*  
*Wi-Fi Protected Access*