Pontifícia Universidade Católica
do Rio de Janeiro

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

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

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

Sergio Henrique Sirufo

Graduou-se em Engenharia Eletrônica pelo Instituto Militar de Engenharia – IME em 1991. Cursou 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 *performanc*e 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 (F*ile 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

Lista de Figuras

Lista de Tabelas

Lista de Siglas

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

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

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