PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

MANOEL PELUSO DE CARVALHO FILHO

ANÁLISE DO DESEMPENHO DE WLAN COM A IMPLEMENTAÇÃO DOS PROTOCOLOS DE SEGURANÇA WEP E WPA/TKIP

PUC CAMPINAS

2008

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

GRÃO-CHANCELER

Dom Bruno Gamberini

MAGNÍFICO REITOR

Prof. Pe. Wilson Denadai

VICE-REITOR

Prof[a]. Dra. Ângela de Mendonça Engelbrecht

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

Prof[a]. Dra. Vera Engler Cury

DIRETOR DO CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

Prof. Dr. Orandi Mina Falsarella

COORDENADOR DO PROGRAMA DE

PÓS-GRADUAÇÃO *STRICTO SENSU* EM ENGENHARIA ELÉTRICA

CURSO DE MESTRADO PROFISSIONAL EM GESTÃO DE REDES DE TELECOMUNICAÇÕES

ÁREA DE CONCENTRAÇÃO: GESTÃO DE REDES E SERVIÇOS

Prof. Dr. Marcelo Luís Francisco Abbade

MANOEL PELUSO DE CARVALHO FILHO

ANÁLISE DO DESEMPENHO DE WLAN COM A IMPLEMENTAÇÃO DOS PROTOCOLOS DE SEURANÇA WEP E WPA/TKIP

Dissertação apresentada como exigência para obtenção do Título de Mestre em Engenharia Elétrica, ao Programa de Pós-Graduação na área de concentração Gestão de Rede e Serviços, Pontifícia Universidade Católica de Campinas.

Orientador: Prof. Dr. David Bianchini

PUC CAMPINAS

2008

Ficha Catalográfica
Elaborada pelo Sistema de Bibliotecas e
Informação - SBI - PUC-Campinas

t621.3845 Carvalho Filho, Manoel Peluso de.
C331a Análise do desempenho de WLAN com a implementação dos protocolos de segurança WEP e WPA/TKIP / Manoel Peluso de Carvalho Filho. - Campinas: PUC-Campinas, 2008.
113p.

Orientador: David Bianchini.
Dissertação (mestrado) - Pontifícia Universidade Católica de Campinas, Centro de Ciências Exatas, Ambientais e de Tecnologias, Pós-Graduação em Engenharia Elétrica.
Inclui bibliografia.

1. Sistemas de comunicação sem fio. 2. Sistemas de telecomunicações. 3. Sistemas de segurança. 4. Redes de computação. 5. Telecomunicações. I. Bianchini, David. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Exatas, Ambientais e de Tecnologias. Pós-Graduação em Engenharia Elétrica. III. Título.

22.ed.CDD - t621.3845

MANOEL PELUSO DE CARVALHO FILHO

"ANÁLISE DO DESEMPENHO DE WLAN COM A IMPLEMENTAÇÃO DOS PROTOCOLOS DE SEGURANÇA WEP E WPA/TKIP"

Dissertação apresentada ao Curso de Mestrado Profissional em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre em Gestão de Redes de Telecomunicações.
Área de Concentração: Gestão de Redes e Serviço.
Orientador: Prof. Dr. David Bianchini

Dissertação defendida e aprovada em 24 de novembro de 2008 pela Comissão Examinadora constituída dos seguintes professores:

Prof. Dr. David Bianchini
Orientador da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

Prof. Dr. Omar Carvalho Branquinho
Pontifícia Universidade Católica de Campinas

Prof. Dr. Edson Luiz Ursini
Universidade Estadual de Campinas

A Sandra minha esposa e ao meu filho William,
que desde o momento em que decidi aceitar
esse desafio estiveram comigo, me
incentivando nos momentos difíceis, como
também nas vitórias conseguidas durante esse
percurso.

AGRADECIMENTOS

Agradeço a Deus acima de tudo por ter me dado saúde e forças para prosseguir com essa pesquisa, e espero que de alguma maneira esse trabalho possa ajudar alguém.

À minha mãe Professora Diva Bernardes e ao meu pai Manoel Peluso, pelos ensinamentos que jamais serão esquecidos.

Ao Professor e Orientador Dr. David Biachini, pelas orientações, reuniões, paciência e amizade, cuja ajuda foi fundamental para a realização deste trabalho.

Ao Professor Dr. Omar Carvalho Branquinho pelo incentivo, disponibilidade e conhecimentos compartilhados.

À Professora Dra. Norma Reggiani pelas revisões e sugestões, os quais enriqueceram este trabalho.

Ao Professor Dr. Edson Ursini colaborador em suas sugestões e interesse demonstrado pelo trabalho.

Aos alunos da Engenharia Elétrica da PUC Campinas: Eduardo Coco e Alberto Iamanura, pela colaboração e ajuda na utilização do laboratório de pesquisa de sistema de rádio da PUC Campinas.

Aos Professores Dr. Marcelo Luís Francisco Abbade, Dr. Amilton da Costa Lamas, Dr. Eric Alberto de Mello Fagotto pelos conhecimentos que nos foram passados.

Aos colegas da turma Adenilson, Diego, Eduardo, Luis Fabiano, Marcelus, Márcia, Samuel, Sara e Rafael, que conviveram comigo durante esse período e muito me apoiaram e incentivaram nos momentos de alegria e nos momentos difíceis.

Aos funcionários do Centro de Ciências Exatas, Ambientais e de Tecnologias da PUC-Campinas, que muito contribuíram para que este trabalho fosse concluído.

À Luzia de Fátima A. C. Ferraz e Marcelo Jorge Agostinho, pelas informações e paciência durante a realização desse trabalho.

Aos meus familiares e amigos que compreenderam minha ausência durante esse período e torceram pelo meu sucesso.

À FINEP (Financiadora de Estudos e Projetos) pelo apoio fornecido no desenvolvimento do Laboratório de Pesquisa em Sistema de Rádio (LI-SiRa) da PUC Campinas.

À todos que de alguma maneira ajudaram para a conclusão deste trabalho, ficarei eternamente agradecido.

“A mente que se abre a uma nova idéia jamais voltará ao seu tamanho original."

Albert Einstein
(1879-1955))

RESUMO

PELUSO, Manoel de Carvalho Filho. Análise do desempenho de WLAN com a implementação dos protocolos de segurança WEP e WPA/TKIP. Campinas, 2007. 113p. Dissertação (Mestrado) – Pós Graduação em gestão de redes e telecomunicações, Pontifícia Universidade Católica de Campinas, Campinas, 2007.

A utilização da tecnologia de rede sem fio tem crescido ultimamente motivado principalmente pelo preço dos equipamentos, facilidade de instalação, manutenção da rede e ampliação das técnicas de segurança. Quanto mais se utiliza o recurso de rede sem fio maior tem de ser o tratamento em relação ao aspecto de segurança. A medida que aumenta o nível de segurança, decresce a quantidade de informação transmitida entre os equipamentos. Esse trabalho visa analisar o desempenho de rede WLAN(Wireless Local Área Network) com a implementação dos protocolos de segurança WEP(Wired Equivalent Privacy) e WPA/TKIP(WI-FI Protected Access / Temporal Key Integrity Protocol). É utilizado o *software* LanTraffic^{TM} para gerar tráfego na rede e também para capturar a taxa de transmissão em Kbps trafegados entre as STAs. São emulados três cenários variando a distância entre os equipamentos. Para cada cenário foi confeccionado um comparativo e analisado o comportamento da WLAN configurado sem segurança, com o WEP habilitado e finalmente com o WPA/TKIP configurado. Para executar os experimentos utilizou-se uma rede WLAN no laboratório de pesquisa em sistema de rádio (LP-SiRa) da PUC Campinas em um ambiente controlado. Com isso não há interferências na transmissão dos sinais emitidos pelos equipamentos Ou seja, sem interferência externa no sinal transmitido entre os equipamentos.

Termos de indexação: Segurança em WLAN, Protocolos de segurança WEP e WPA/TKIP, Redes *Wireless*, Padrão 802.11, Desempenho em WLAN.

ABSTRACT

PELUSO, Manoel de Carvalho Filho. *Performance analysis of WLAN with the implementation of WEP and WPA/TKIP security protocols.* Campinas, 2007. 111p. Dissertação (Mestrado) – Pós Graduação em gestão de redes e telecomunicações, Pontifícia Universidade Católica de Campinas, Campinas, 2007.

Nowadays, the use of the wireless network technology has grown mainly motivated by the price of equipments, ease of installation, network maintenance and expansion of technical safety. The more you use the wireless network resource, the better should be the treatment related to its safety aspect. As the security level increases, the amount of information transmitted between the equipment decreases. This thesis aims to analyze the performance of WLAN network with the implementation of WEP and WPA / TKIP security protocols in an environment that uses applications whose characteristic is to generate small packets on the network. The LanTraffic ™ software is used to generate traffic and also to capture the transmission rate in Kbps that flows through the stations. Three scenarios are simulated varying in the distance between the equipments. For each scenario, a comparative study was made and the WLAN behavior without the security resource analyzed, then it was analyzed with the WEP fitted and finally with the WPA/TKIP configured. To develop the experiments it was used a WLAN network in a controlled environment in the Laboratory Research on Radio System in PUC Campinas. Therefore, there is not external interference in the signal transmitted by equipments.

Index terms: WLAN Security, WEP and WPA/TKIP security protocols, Wireless Network, Standard 802.11, WLAN Performance.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

APs	=	Access Points
BPSK	=	Binary Phase Shift Keying
BSA	=	Basic Service Area
BSS	=	Basic Service Set
CCK	=	Complementary Code Keing
CPU	=	Central Processing Unit
DA	=	Destination Address
DBPSK	=	Differential Binary Phase Shift Keying
DS	=	Distribution System
DSSS	=	Direct Sequence Spread Spectrum
DQPSK	=	Differential Quadrature Phase Shift Keying
ERPs	=	Enterprise Resource Planning
ESA	=	Extend Service Área
ESS	=	Extended Service Set
FTP	=	File Transfer Protocol
FCS	=	Frame Check Sequence
HR-DSSS	=	High Direct Rate Sequence Spread Spectrum
HTTP	=	Hyper Text Transfer Protocol
IEEE	=	Institute of Electrical and Electronics Engineers
ICV	=	Integrity Check Value
IP	=	Internet Protocol
IV	=	Inicialization Vector
LAN	=	Local Area Network
LLC	=	Logic Link Control

MAC	=	Médium Access Control
MIC	=	Message Integrity Code
OFDM	=	Orthogonal Frequency Division Multiplexing
OSI	=	Open Systems Interconnection
PLCP	=	*Physical Layer Convergence Protocol*
PRNG	=	Pseudo Random Number Generator
QAM	=	Quadrature Amplitude Modulation
QPSK	=	Quadrature Phase Shift Keying
RC4	=	Ron's cipher 4
SA	=	Source Address
STAs	=	Stations
TA	=	Trasmiter Address
TCP	=	Transport Control Protocol
TK	=	Temporal Key
TKIP	=	Temporal Key Integraty Protocol
TSC	=	TKIP sequence counter
TTAK	=	TKIP-mixed transmit address and key
WEP	=	Wired Equivalent Privacy
WLAN	=	Wireless Local Area Network
WM	=	Wireless Médium
WNIC	=	Wireless Network Interface Card
WPA	=	WI-FI Protected Access
XOR	=	Exclusive OR

SUMÁRIO

1 INTRODUÇÃO

O surgimento da utilização de LANs, pelas empresas e nas residências, a partir do início da década de 1990, traz diversas soluções e diferentes fabricantes como a IBM, CISCO, 3COMM e outras. Dentre estas soluções a rede local sem fio WLAN (*Wireless Local Área Network*) são redes que não utilizam qualquer tipo de cabeamento para transmitir dados entre vários equipamentos fixos ou móveis.

A utilização da tecnologia de rede sem fio tem crescido a partir da década de 90 motivada principalmente pelo preço dos equipamentos, melhoria da segurança e facilidade de instalação e manutenção da rede. Stallings (2003) cita que uma WLAN também tem de fornecer algumas funções da LAN (*Local Area Network*), abrangendo alta taxa de transferência de dados, capacidade de cobrir pequenas distâncias, total conectividade entre as STAs e segurança. Assim, a WLAN não irá substituir a LAN cabeada, mas sim complementá-la em lugares e situações em que sua utilização trará melhores benefícios.

Dada esta diversidade de soluções relata Soares; Lemos; Colcher (2000), o IEEE (*Institute of Electrical and Electronics Engineers*) formou um grupo denominado '*Wireless Local-Area Networks Standard Working Group, IEEE Project 802.11*', com o intuito de definir padrões para a WLAN. Em 1997 foi aprovado o padrão IEEE 802.11, que define as camadas físicas e MAC (*Medium Access Control*) para rede WLAN.

O IEEE é constituído de grupos que são incumbidos de desenvolver ou complementar padrões. Se um padrão, o qual possui uma identificação definida por um número, é modificado, esse número é acrescido de um digito ou uma letra. Tal fato ocorreu com o padrão IEEE 802.11.

Padrões derivados do IEEE 802.11 foram criados, em especial o 802.11i cuja característica principal é ampliar a segurança da WLAN. Em Março de 2001 o

IEEE criou o grupo 802.11i com o intuito de desenvolver padrões para ampliar a segurança da WLAN. Em 2004, o grupo sancionou o padrão 802.11i.

A primeira técnica de autenticação, ainda utilizada, é o sistema de compartilhamento de chave, que consiste de dígitos numéricos e alfanuméricos. As STAs e os APs (*Access Points*) utilizam uma chave comum ou compartilhada que será utilizada para autorizar a comunicação entre eles. A STA envia uma solicitação de acesso ao AP informando a sua chave, o AP compara a chave da STA com uma tabela de chaves. Se a chave existir na tabela, o AP autoriza a STA a enviar as informações.

No fim da década 1990, quando o padrão 802.11 estava sendo estabelecido foi desenvolvido o protocolo WEP (*Wired Equivalent Privacy*) para prover maior confidencialidade para a WLAN. Conforme afirma Duntemans's (2004), o WEP foi desenvolvido com o objetivo de dar mais segurança à rede sem fio protegendo-a contra os intrusos que tentem acessar a WLAN, atuando nos dados que circulam pela rede cifrando e decifrando os mesmos nos APs e nas STAs (*Stations*). O protocolo WEP utiliza o gerador de número PRNG (*Pseudorandom Number Generator*) do algoritmo RC4 (*Ron's cipher 4*), para gerar uma chave que cifra os dados através de um vetor de inicialização denominado IV (*Inicialization Vector*) e de uma chave que será utilizada para cifrar os dados. O WEP utiliza 3 *bytes* para gerar o IV, possibilitando a produção de 16 milhões de valores diferentes.

Em 2001 os especialistas em criptografia Fluhrer; Mantin; Shamir (2001) publicaram um documento relatando um ataque teórico de como capturar uma chave em uma WLAN protegida pelo protocolo WEP. A partir dessa publicação, surgiram vários *softwares* livres na Internet para transgredir a segurança WEP.

Devido a fragilidade detectada no WEP, surge em 2003 o primeiro padrão WPA (*WI-FI Protected Access)* apoiado nos padrão inicialmente estabelecido pelo grupo IEEE 802.11i. Nesse momento, a finalidade do WPA foi melhorar as duas maiores falhas do WEP, que são a vulnerabilidade do protocolo e a ineficiência na metodologia de distribuição de chave (MASICA, 2007, p.5). Em 2004, o IEEE

disponibilizou a tecnologia TKIP com o intuito de aumentar a segurança no padrão original WPA. “O protocolo TKIP utiliza o algoritmo de criptografia RC4 utilizado pelo WEP, porém insere outros algoritmos fazendo com que o TKIP aumente extensivamente o poder e a complexidade da criptografia em rede sem fio, tornando o *wireless* muito mais intricado, se não impossível, para um intruso adentrar em uma rede *wireless*.” (WI-FI ALLIANCE, 2003, p.7).

Quando surgiram as redes sem fio na década de 80, os desenvolvedores da tecnologia *wireless* pensaram principalmente em mobilidade, não se preocupando com a segurança que esse meio de comunicação necessita, sendo que os equipamentos foram fabricados sem essa funcionalidade. Atualmente as redes sem fio são uma realidade tanto para uso doméstico como, principalmente para a maioria das empresas. Dessa maneira, o quesito segurança na WLAN passou a ser a principal preocupação por parte dos administradores de rede. Para atender esses requisitos tanto o IEEE como os fabricantes desenvolveram vários protocolos que implementam segurança em rede sem fio. Essas novas técnicas utilizam processo, algoritmos e cálculos matemáticos para prover maior segurança em rede *wireless*. Logicamente, essas técnicas consomem mais recursos dos equipamentos tanto de CPU (*Central Processing Unit*) como de memória. Conforme relata Walker (2005) as primeiras gerações de APs, e que ainda estão em uso, foram desenvolvidas com a mesma tecnologia de processamento do Intel 80386 com 25 MHZ, onde 90% dos recursos dos APs são utilizados para a função de controle de transmissão de dados sem se preocupar com os aspectos de segurança. Tem-se que atentar para esses pontos antes de implementar os protocolos de segurança em WLAN, pois o impacto no desempenho poderá causar transtornos para os usuários. Portanto, para implementar segurança precisa conhecer o quanto um protocolo de segurança consome recursos em relação ao outro protocolo, mesmo sabendo que os equipamentos fabricados atualmente, para serem utilizados em WLAN, são desenvolvidos com o intuito de prover segurança e evitar ao máximo a degradação da performance da rede *wireless.*

Para implementar os protocolos de segurança pode ser necessário fazer *upgrade* nos *firmaware* dos equipamentos. Porém, na maioria dos casos não necessita trocar os equipamentos existentes, a não ser que o equipamento não permita. Implementação de novas técnicas de autenticação consome mais recursos dos equipamentos que as técnicas existentes. Portanto, antes de melhorar a segurança da WLAN com a implantação dos protocolos de segurança é necessário analisar quais serão os impactos no desempenho da rede.

Objetivo geral desse trabalho é avaliar o impacto no desempenho da rede WLAN com a implementação dos protocolos de segurança WEP e WPA/TKIP, com o intuito de prever a queda de desempenho na transmissão de informações em rede em fio. Esse trabalho pretende examinar através de experimento e posteriormente comparar o quanto o protocolo WEP impacta no desempenho da WLAN em relação a redes sem segurança. O mesmo será feito com o protocolo WPA/TKIP em relação ao WEP.

Conforme nos alerta Mattar apud Karkotli (2002, p. 13), sabemos que: “todo trabalho científico deve pressupor uma metodologia que dê sustentação teórica ao tema abordado na pesquisa, de modo que os objetivos delimitados possam ser alcançados com êxito”.

Dessa forma, essa dissertação está organizada em 6 capítulos.

O Capítulo 1 apresenta uma introdução ao tema, com o intuito de fornecer uma visão geral sobre a rede local sem fio. Também contêm informações sobre os objetivos dessa dissertação e a motivação para a pesquisa.

O Capítulo 2 destaca os conceitos referentes a WLAN, a terminologia utilizada nessa tecnologia e os componentes da rede sem fio mostrando o relacionamento entre eles, ilustrando a camada física e MAC e as tecnologias de rádio DSSS (*Direct Sequence Spread Spectrum*) e OFDM (*Orthogonal Frequency Division Multiplexing*), utilizadas para a transmissão de dados entre os componentes da WLAN. Também descreve os padrões 802.11, 802.11a, 802.11b, 802.11g e

802.11i estabelecidos pelo IEEE, destacando sua utilização, características, e diferenças entre eles.

O Capítulo 3 descreve as técnicas de segurança em WLAN, focando nos sistemas sem segurança ou abertos, o sistema de criptografia WEP, técnica de criptografia que o WPA/TKIP implementa e finaliza com uma estimativa da degradação do desempenho da WLAN, com a implantação dos protocolos de segurança.

O Caítulo 4 apresenta a metodologia, os materiais, os equipamentos e os experimentos executados no laboratório de pesquisa em sistema de rádio (LP-SiRa da PUC Campinas em um ambiente controlado.

No Capítulo 5, através da coleta dos dados obtidos nos experimentos é feito uma análise comparativa descritiva e grafica, contextualizando o desempenho da WLAN com a implementação dos protocolos de segurança WEP e WPA/TKIP.

O Capítulo 6 faz a conclusão e as considerações finais, apresentando o impacto de performance na implementação dos protocolos de segurança em WLAN e os trabalhos futuros.

2 ARQUITETURA DA WLAN

A principal funcionalidade da WLAN é a comunicação entre equipamentos, sem a utilização de cabos, suportando redes residenciais, pequenos escritórios e redes empresariais. Em 1997 foi aprovado o padrão IEEE 802.11 que regulamentou a WLAN, cuja arquitetura e os componentes poderão ser notados na Figura 1.

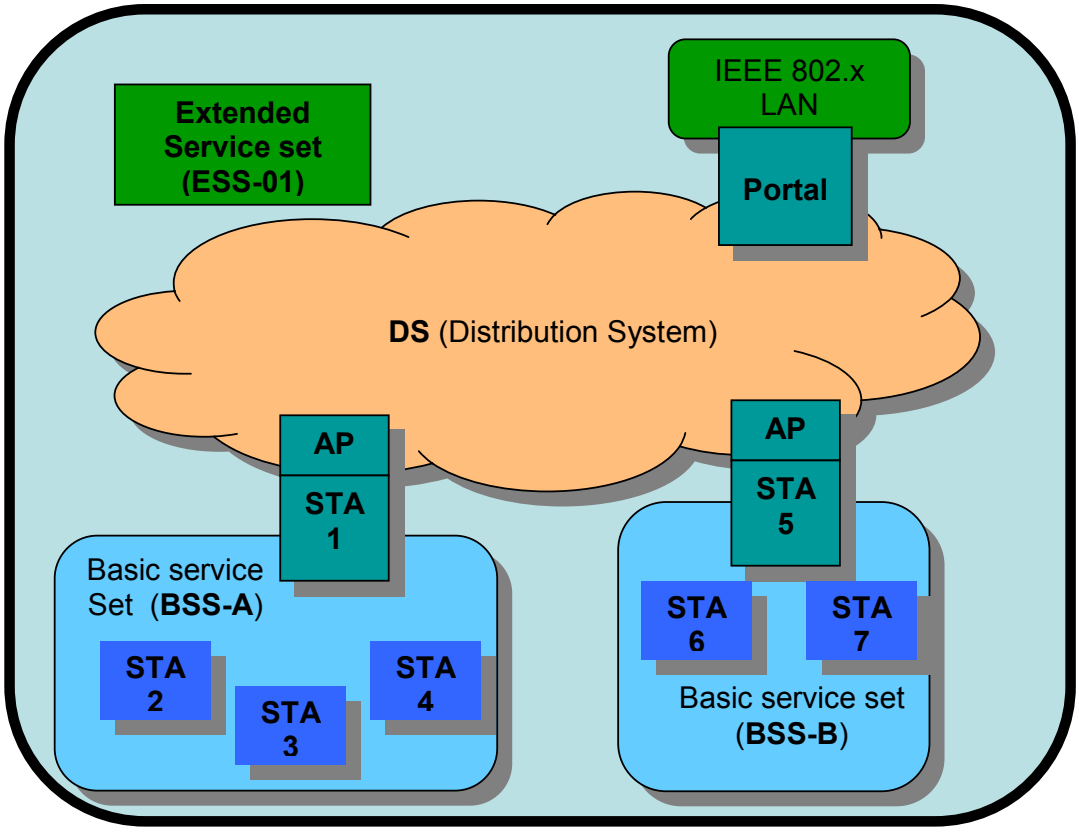


Figura 1 – Arquitetura 802.11 com seus componentes.
Fonte – IEEE802.11 (1999)

a) STA (*Station*)

São dispositivos computacionais com interface para conectar em um ambiente sem fio. É composto de um MAC, que está apresentada na Figura 2, e de uma interface da camada física e tem de estar em conformidade com o padrão IEEE 802.11. É o WNIC (*Wireless Network Interface Card*) da rede cabeada. Normalmente as STAs são PCs(*Personal Computers*) utilizados devido a necessidade de mobilidade. Porém, as STAs podem também ser computadores fixos com interface que permite conectar em uma rede sem fio.

b) BSS (*Basic Service Set*)

Conforme nos alerta O'HAra; Petrick (2001, p. 9): "A arquitetura WLAN IEEE 802.11 é construída em torno de um BSS. Um BSS é um conjunto de STAs que comunicam entre si." Conforme se observa na Figura 1, a formação de grupos de STAs em duas regiões distintas, onde em uma região está o grupo STA1(AP), STA2, STA3 e STA4 formando o BSS-A. Na outra região está o grupo STA5, STA6 e STA7 constituindo outro BSS-B.

c) BSA (*Basic Service Area*)

Uma área conceitual onde as STAs de um mesmo BSS podem se comunicar. Conforme descreve Gast (2002), todos os dispositivos *wireless* propagam seus sinais em três dimensões. Assim, o termo a ser usado poderia ser volume e não área. Porém, o termo área é amplamente utilizado em todos os lugares.

d) ESS (*Extended Service Set*)

A cobertura dentro de um BSS se restringe a pequenas áreas. O padrão 802.11 permite a criação de áreas maiores de cobertura através da interconexão de vários BSSs dentro de um ESS. Portanto, o ESS é um grupo de um ou mais BSS conectados através de um *backbone*, o qual é denominado de DS (*Distribution System*).

e) DS (*Distribution System*)

O DS é uma estrutura lógica que interliga as BSAs, possibilitando que as STAs situadas em diferentes BSSs troquem informações entre si. O padrão 802.11 não estipula uma tecnologia específica para o DS, o qual na prática fazem com que a BSS seja uma ESS. Devido a essa característica, atualmente utilizada nas redes sem fio, quando uma STA passa de um AP para outro, ocorre a interrupção da conexão da STA desse AP e a necessidade da STA se conectar no outro AP.

f) ESA (*Extend Service Area*)

Uma área conceitual onde as STAs de uma ESS podem se comunicar. Os BSAs conectados pelo DS através dos APs definem uma ESA. A extensão de uma ESA sempre será igual ou maior que uma BSA e pode conter vários BSSs.

g) AP (*Access Point*)

São equipamentos que se comunicam com as STAs através de rádio freqüência e provê acesso ao DS. Os APs têm a capacidade de capturar as informações das

STAs pertencentes a sua BSA e enviar para as STAs pertencentes a outras BSAs, utilizando o DS. Uma das funções mais utilizadas do AP é se conectar a um DS e também se conectar a uma rede cabeada.

h) *Portal*

Um ponto lógico o qual uma arquitetura diferente do padrão 802.11 se conecta no DS de uma rede 802.11 (IEEE802.11, 1999).

Conforme mostra a Figura 1, o *portal* está interligando uma rede 802.x ao DS da rede 802.11, onde os dados a partir da rede 802.x chegam a uma rede 802.11 através do *portal*.

Na prática, o mais utilizado é conectar uma WLAN com uma rede cabeada, onde o AP exerce a função de AP e de *portal*.

Na Figura 1 podemos notar os componentes definidos pela arquitetura IEEE 802.11. As STAs são os componentes básicos de uma WLAN. Essas STAs têm de possuir um periférico de rede sem fio, conhecido como WM (*Wireless Médium*). Cada STA pertence a uma BSS, ou seja, a STA 3 pertence a BSS-A e a STA 6 pertence a BSS-B. As STAs podem sair de uma BSS e entrar em outra BSS ou simplesmente sair de qualquer BSS. Por exemplo: A STA 3 pode desassociar da BSS-A e associar na BSS-B.

Conforme ilustrado na Figura 1, tem-se um ESS constituído pela conexão de dois BSS. Esse tipo de arquitetura é denominado rede sem fio com infra-estrutura. Outro tipo de rede sem fio ocorre quando as STAs comunicam entre si sem utilizar o AP, sendo que o ESS é constituído de um único BSS. Nesse caso a rede é chamada de rede WLAN *Ad Hoc*.

O ESS recebe uma identificação (ESS-ID) ESS-01. Dentro do ESS-01 os BSS também recebem uma identificação (BSS-ID). Na Figura 1 temos o BSS-A e BSS-B. A junção desses identificadores (ESS-ID e BSS-ID) forma a identificação (Network-ID) de uma WLAN. Na Figura 1 percebem-se dois network-id, um o ESS-01BSS-A e o outro ESS-01BSS-B.

De acordo com Stallings (2003), os serviços citados a seguir, são implementados para que haja a interação entre os componentes da rede WLAN com infra-estrutura. São eles:

- Distribuição: É utilizado pelas STAs para transmitir dados de uma STA em um BSS para outra STA em outro BSS. Observando a Figura 1. Para que a STA 2 envie dados para a STA 7, estes devem ser encaminhados para o AP (STA 1) que passa o dado para o DS que tem o trabalho de direcionar o dado para AP(STA 5). O AP(STA 5) recebe o dado e envia para a STA 7.

- Integração: É utilizado pelas STAs para transmitir dados de uma STA que pertence a uma arquitetura IEEE 802.11 para uma STA pertencente a uma arquitetura IEEE 802.x e vice versa. Essas duas arquiteturas estão interligadas fisicamente através do DS. Na Figura 1, o *Portal* está conectado de um lado em uma LAN cabeada e no outro lado em uma rede sem fio.

- Associação: Utilizado para registrar a STA em um AP. Para enviar *frame*, uma STA tem estar associada a um AP. O DS utiliza as informações da associação para determinar qual AP a STA está conectada. Uma STA pode estar associada somente em um AP. Na Figura 1, para a STA 2 enviar *frame* para o AP(STA 1), primeiramente tem solicitar um pedido de associação para o AP(STA 1).

- Dissociação: Esse serviço finaliza uma associação existente entre a STA e o AP. A dissociação é executado se a STA necessitar sair da WLAN ou migrar de AP. O serviço pode ser executado tanto pela STA como pelo AP.

- Reassociação : É o serviço que permite uma STA mover de um AP para outro AP. O AP nunca inicia o processo de reassociação. Essa função é sempre iniciada pela STA. Após a reassociação o DS atualiza o novo endereço da STA. Na FIgura 1, se a STA 2 necessitar se associar ao AP(STA 5), primeiro a STA 2 é desassociada do AP(STA 1) e terá que solicitar uma reassociação ao AP(STA 5).

- Autenticação: Autenticação é um requisito imprescindível para que somente os usuários autenticados pelo AP acessem a WLAN. Na Figura 1 o usuário da STA 6 tem de ser autenticado pelo AP(STA 5), para poder enviar utilizar a rede sem fio.

- Privacidade: Implementar serviço de segurança é fundamental para a confiabilidade das informações que circulam pela rede sem fio. A WLAN tem de fornecer serviços que dificultam a captação das informações por agentes não autorizados. O padrão 802.11 oferece serviços de segurança que dificultam o acesso indevido as informações. Os serviços de segurança serão discutidos detalhadamente mais adiante no Capítulo 3.

2.1 Camada física e MAC da WLAN

O ambiente de comunicação sem fio utiliza as tecnologias das camadas físicas e de enlace, em especial a sub camada MAC, que foram desenvolvidas para suportar o padrão 802.11. Primeiramente, duas faixas de freqüências de rádio (2,4 e 5,4 MHz) estão padronizadas, sendo que as de freqüências de rádio são as mais utilizadas devido principalmente, conforme relata Tanenbaum (2003), ao fato de não necessitarem de licenciamento, podendo atravessar pequenos obstáculos e permitindo a sua utilização em ambientes abertos e fechados.

O modelo OSI (*Open Systems Interconnection*) define as camadas de enlace e física. O IEEE diante das exigências de redes por difusão (cabo, wireless)

redefiniu a camada de enlace, constituindo-a por subcamada LLC (*Logic Link Control*) e MAC (*Medium Access Control*). Esta última se relaciona diretamente com a camada física como podemos observar na Figura 2, onde salienta o padrão 802.11.

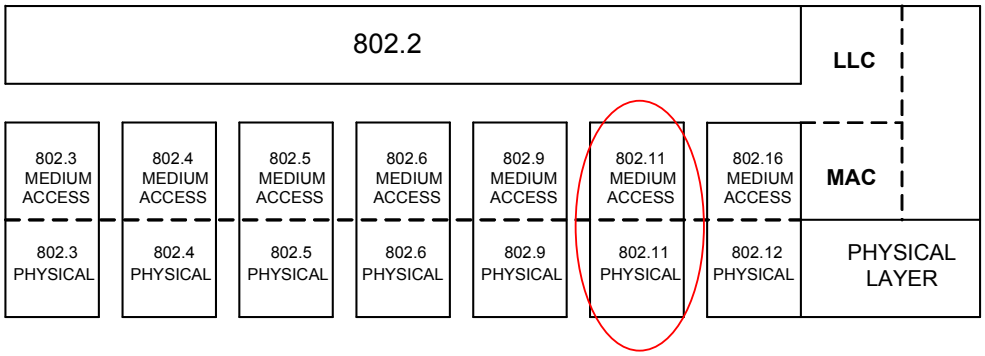


Figura 2 – Especificação das camadas física e MAC *Control* para WLAN
Fonte – IEEE802.11 (1999)

Conforme ilustra a Figura 2, a camada física “802.11 PHYSICAL” é a interface entre a MAC e a mídia, a qual transmite os *frames* para a rede sem fio, sendo que o objetivo da 802.11 especificamente é tratar a MAC e a camada física (PHYSICAL), tornando as camadas superiores independentes da camada física conforme está apresentado na Figura 3.

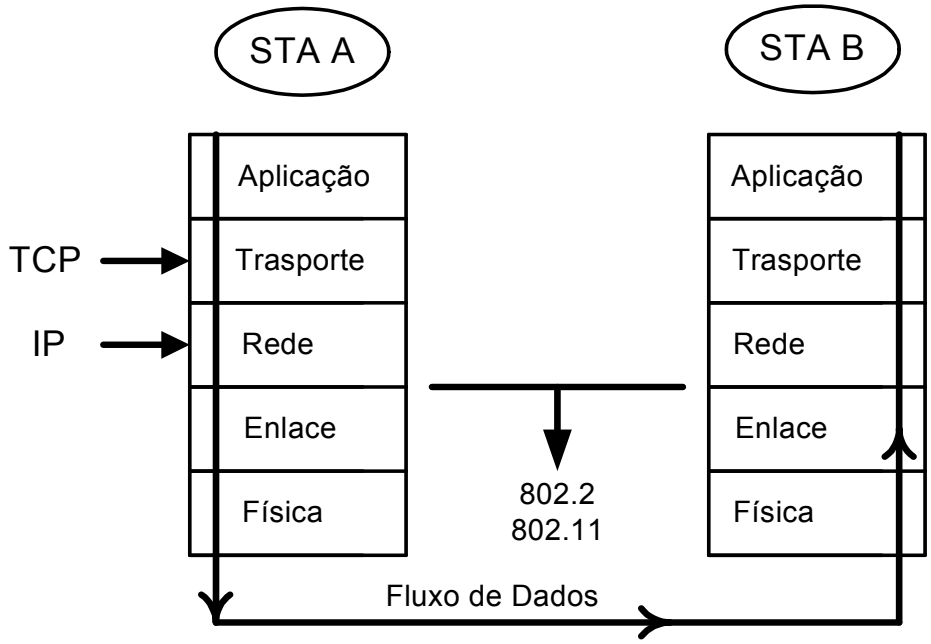


Figura 3 – Fluxo de dados na pilha TCP/IP

A Figura 3 mostra que interface 802.11 atende completamente a pilha do protocolo TCP/IP (*Transport Control Protocol* / *Internet Protocol*) sem a necessidade de qualquer adaptação para funcionar com aplicações que utilizam o protocolo TCP/IP. Ou seja, aplicações que utilizam o protocolo TCP/IP são independentes do tipo de interface da rede sem fio.

Na camada física o padrão 802.11 contempla duas tecnologias para a utilização de freqüência para a transmissão de dados entre os componentes da WLAN, o DSSS (*Direct Sequence Spread Spectrum*) e OFDM (*Orthogonal Frequency Division Multiplexing*)

2.2 Tecnologias utilizadas pela WLAN

2.2.1 DSSS (*Direct Sequence Spread Spectrum*)

O DSSS é suportado pelo padrão utilizando freqüência de 2,4 GHz divido em 14 canais conforme Tabela 1 abaixo.

Tabela 1 – Distribuição dos canais no DSSS nas regiões mundiais

Número Canal	Frequência GHz	EUA / Brasil	Europa	França	Espanha	Japão
01	2,412	**X**	X			
02	2,417	**X**	X			
03	2,422	**X**	X			
04	2,427	**X**	X			
05	2,432	**X**	X			
06	2,437	**X**	X			
07	2,442	**X**	X			
08	2,447	**X**	X			
09	2,452	**X**	X			
10	2,457	**X**	X	X	X	
11	2,462	**X**	X	X	X	
12	2,467		X	X		
13	2,472		X	X		
14	2,484					X

Fonte – O'Hara; Petrick (2001)

Na Tabela 1, nota-se que na América do Norte é permitido utilizar 11 canais entre 2,412 GHz e 2,462 GHz. São autorizados 13 canais na Europa, com exceção da Espanha e França, 1 canal no Japão, 2 canais na Espanha e 4 canais França.

De acordo com O'HAra; Petrick (2001), para que não haja interferência entre os canais, os mesmos têm de estar espaçados em freqüências de 25 MHz. Assim, no padrão da América do Norte, o mesmo utilizado no Brasil, permite a utilização de três canais independentes, na mesma faixa de freqüência de 2,4 GHz conforme Figura 4.

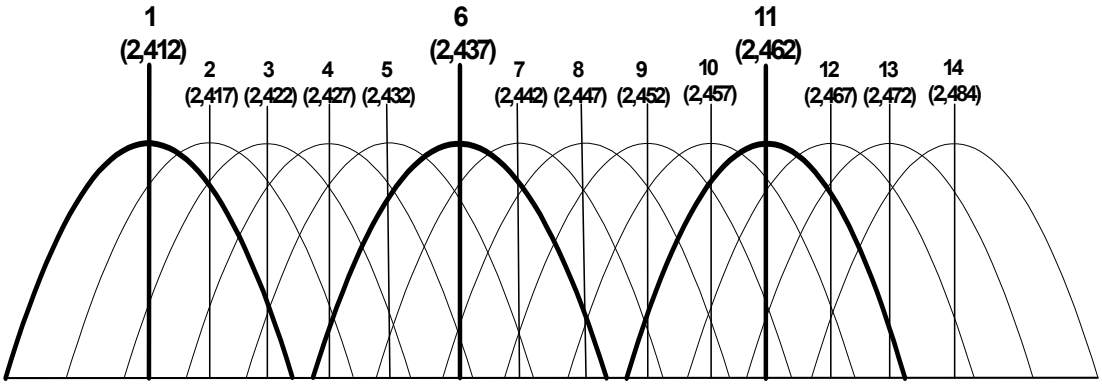


Figura 4 – Espaçamento mínimo entre os canais DSSS
Fonte – O'Hara; Petrick (2001)

A disposição dos canais ilustrado na Figura 4 permite a configuração de múltiplas redes para operar simultaneamente em uma mesma área. Ou seja, configura-se um AP para operar no canal 1, outro no canal 6 e um terceiro no canal 11. Em função da distância entre os APs, canais intermediários podem ser utilizados.

O DSSS utiliza as modulações DBPSK (*Differential Binary Phase Shift Keying*) e DQPSK(*Differential Quadrature Phase Shift Keying*) para fornecer taxas a 2 Mbps e 1 Mbps. Para fornecer taxas a 11 Mbps e 5,5 Mbps, o DSSS utiliza modulação HR-DSSS(*High Direct Rate Sequence Spread Spectrum*) com a técnica CCK(*Complementary Code Keing*).

2.2.2 OFDM (*Orthogonal Frequency Division Multiplexing*)

De acordo com (ROSHAN; LEARY, 2003, p. 125), "OFDM fragmenta o canal, em canais pequenos e independentes de transmissão ortogonal com menor taxa de transmissão utilizando menor banda". Ainda é importante salientar que essa tecnologia é utilizada em WLAN nos padrões 802.1a e 802.11g, permitindo que esses padrões utilizem velocidades na camada física de 54 Mbps.

> A técnica OFDM distribui os dados a serem transmitidos em partes menores, os quais são transmitidos simultaneamente sobre canais de múltipla freqüência que estão espacejados independentemente. Esse espacejamento proporciona a ortogonalidade que evita o demodulador de enxergar outras freqüências que não lhe pertence. Os benefícios do OFDM são a alta eficiência do espectro, o poder de recuperação da freqüência do radio e uma menor distorção dos múltiplos caminhos. (KHAN; KHWAJA, 2003, p.37-38).

O OFDM fornece taxas de transmissão que varia de 6 Mbps à 54 Mbps, dependendo das técnicas de modulação utilizada. As técnicas usadas são o BPSK (*Binary Phase Shift Keying*), QPSK (*Quadrature Phase Shift Keying*) e a QAM (*Quadrature Amplitude Modulation*) dependendo da taxa de transmissão utilizada.

2.3 Padrões 802.11

Conforme relata Duntemann's (2004), uma importante função do IEEE é desenvolver e estabelecer padrões tecnológicos. Padronizar é importante porque amplia o mercado e possibilita os diferentes fornecedores a produzir tecnologias que possam interagir e comunicar umas com as outras. Na WLAN existem vários padrões derivados do 802.11, cada um com suas características.

Para suportar a arquitetura de rede sem fio, o IEEE definiu o padrão IEEE 802.11. Depois definiu os padrões 802.11a, 802.11b, 802.11g e o padrão 802.11i, os quais estão sintetizados a seguir.

a) IEEE 802.11

Foi o primeiro padrão especificado pelos IEEE em 1997, o qual opera em uma freqüência de 2,4 GHz, utilizando o sistema DSSS para fornecer taxas de 1 ou 2 Mbps (IEEE802.11, 1999).

b) IEEE 802.11a

Esse padrão opera em freqüência de 5,4 GHz. Atuando nessa freqüência a interferência ou ruído é menor, pois não há compartilhamento do meio de transmissão com os telefones sem fio, fornos micro ondas e outros equipamentos que utiliza a freqüência de 2,4 GHz. Sua característica difere do padrão 802.11 principalmente na camada física de rede, pois utiliza freqüência e 5,4 GHZ. Portanto, a camada física teve que ser alterada para atender o padrão 802.11a (IEEE802.11a, 1999). De acordo com Rufino (2005), esse padrão utiliza o sistema OFDM, disponibilizando taxas até 54 Mbps, sendo essas taxas alocadas dinamicamente.

c) IEEE 802.11b

O padrão 802.11b opera em uma freqüência igual a do 802.11, utilizando o sistema DSSS. Conforme relata Roshan; Leary (2003), em 1997 o grupo de trabalho IEEE 802.11 definiu o padrão 802.11b com a utilização do DSSS com as técnicas DBPSK e DQPSK provendo taxas de 2 Mbps e 1 Mbps respectivamente e adicionou mais duas taxas de transmissão, uma de 5,5 Mbps e outra de 11 Mbps através da utilização do HR-DSSS com a técnica de propagação CCK.

d) IEEE 802.11g

Esse padrão foi liberado em 2003 disponibilizando as mesmas taxas de transmissão do padrão 802.11a, mas operando em uma freqüência igual do 802.11b. As interfaces 802.11g utilizam a melhor velocidade nominal, para trafegar os dados utilizando o OFDM com as taxas descritas na Tabela 2.

O padrão 802.11g é totalmente compatível com o padrão 802.11b. Ou seja, um AP operando no padrão 802.11g se comunica com uma STA operando no padrão 802.11b(IEEE802.11g, 2003).

As taxas em Mbps disponibilizadas no padrão 802.11a, 802.11b e 80.11g estão apresentadas na Tabela 2.

Tabela 2 – Taxas disponibilizadas no padrão 802.11

Especificação	Modulaçao	Taxa (Mbps)
802.11 / 80211b / 802.11g	DBPSK	1
802.11 / 80211b / 802.11g	DQPSK	2
80211b / 802.11g	CCK	5,5
80211a / 802.11g	BPSK	6
80211a / 802.11g	BPSK	9
80211b / 802.11g	CCK	11
80211a / 802.11g	QPSK	12
80211a / 802.11g	QPSK	18
80211a / 802.11g	QAM	36
80211a / 802.11g	QAM	36
80211a / 802.11g	QAM	48
80211a / 802.11g	QAM	54

Fonte – O'Hara; Petrick (2001)

e) IEEE 802.11i

Em março de 2001 o IEEE formou o grupo 802.11i com o intuito de desenvolver padrões para ampliar a segurança da WLAN. Em 2004 o grupo sancionou o padrão 802.11i que introduz o estabelecimento e gerenciamento de chave e amplia o algoritmo de criptografia e autenticação. Para aumentar a segurança em rede WLAN esse padrão utiliza o protocolo TKIP e também pode utilizar a tecnologia de autenticação do 802.1X (IEEE802.11i, 2004).

A seguir estão expostos os mecanismos de segurança em rede *wireless* incluindo os estabelecidos pelo padrão IEEE 802.11i.

3 SEGURANÇA EM WLAN

De acordo com Rufino (2005), em redes cabeadas a segurança física é um item de risco a ser considerado. Em rede sem fio esse componente é ainda maior, visto que, o controle de acesso a uma WLAN é muito menor que o controle de acesso a uma rede cabeada. Se antes para acessar uma rede precisava de um ponto de rede cabeada, com a tecnologia de rede sem fio o acesso a uma rede pode ser feito a dezenas ou centenas de metros ao redor e externamente a empresa.

Em rede com fio essa vulnerabilidade pode ser mitigada através de gerenciamento de controle de acesso a rede, permitindo que somente pessoas autorizadas se conectem na rede. Em rede sem fio, como os equipamentos não utilizam cabo e sim freqüência de radio para transmitir os dados, estranhos podem capturar os dados sem ser necessário conectar fisicamente na rede. Portanto, para prover segurança nas informações em WLAN é fundamental implementar processos de criptografias nas informações.

O intuito do processo de criptografia, no que tange a WLAN é prover a privacidade das informações que trafegam pela rede sem fio. Os dados cifrados devem ser decifrados somente pelos elementos autorizados a fazer essa operação.

Conforme citado por Khan; Khwaja (2003) criptografia é uma disciplina matemática utilizada para garantir a confidencialidade e a integridade das informações. Criptografia de dados é um processo onde os dados originais ou texto puro (*plaintext*) é transformado em dados ou texto cifrado (*ciphertex*t) através de operações denominadas de algoritmo de criptografia. Os caracteres utilizados para cifrar e decifrar os dados são chamados de chave para cifrar e decifrar os dados. Existem dois tipos de algoritmo de criptografia: simétrica e assimétrica. Simétrica utiliza a mesma chave para cifrar e decifrar os dados, enquanto o assimétrico utiliza chaves diferentes. O RC4 (*Ron's cipher 4*), o qual é

utilizado pelo WEP e pelo WPA/TKIP, utiliza o algoritmo simétrico para cifrar os dados.

Conforme relata Schneier (1996), o RC4 foi desenvolvido em 1987 por Ronald Rivest e até 1994 foi propriedade da RSA Data Security [1] sendo que detalhes do algoritmo somente era disponibilizado após assinar um termo de compromisso de não divulgar o algoritmo. Em setembro 1994 foi enviado, anonimamente, para uma lista de discussão na internet, um algoritmo igual ao desenvolvido por Ronald. Mesmo com a discordância da RSA Data Security, o RC4, que era mantido como segredo industrial se tornou público e passou a ser debatido e disseminado em congressos, cursos e grupos de discussões.

O RC4 é um gerador de *bytes* aleatório, através de uma chave de dados de tamanho variável que serão utilizados para cifrar as informações. No destino será executado o RC4 utilizando a mesma chave para gerar os *bytes* e decifrar as mensagens.

O WEP e o WPA/TKIP utilizam o RC4 para gerar *bytes* aleatórios em seus processos de criptografia conforme descrito a seguir. Além desses protocolos de criptografia é descrito a seguir o sistema de rede sem fio sem segurança ou aberto e também o sistema de segurança com compartilhamento de chave, o qual não possui nenhum processo de criptografia.

---

[1] RSA *Data Security* é uma empresa pública, sediada em Bedford, Massachusetts. Anteriormente era designada de Security Dynamics, que a adquiriu em 1996 e à DynaSoft AB em 1997. O nome *RSA* deriva dos seus fundadores, Ron **R**ivest, Adi **S**hamir e Len **A**dleman, três professores do Instituto MIT. Esta empresa dedica-se, sobretudo, à criptografia, e organiza, anualmente, a conferência RSA *Conference*.

3.1 Sistemas abertos

São os sistemas autenticação nula, onde as STAs acessam a WLAN sem qualquer algoritmo de autenticação (IEEE802.11, 1999). Todas as STAs comunicam entre si e com todos os APs sem nenhuma verificação de segurança.

Portanto, na rede de sistema aberto não devem transitar informações confidenciais.

3.2 Sistema de compartilhamento de chave

As STAs e os APs utilizam uma chave comum que será utilizada para autorizar a comunicação entre eles. A STA envia uma solicitação de acesso ao AP informando a sua chave, o AP compara a chave da STA com uma tabela chaves. Se a chave existir na tabela, o AP autoriza a STA a enviar as informações. O mais utilizado é configurar o AP informando os endereços MAC das STAs que poderão se comunicar com o AP. Quando o AP recebe uma solicitação de uma STA, o mesmo verifica se o endereço MAC da STA está contida em sua tabela para autorizar a comunicação.

3.3 Processo de segurança WEP

Na década 1990 quando o padrão 802.11 foi liberado com o intuito de prover maior confidencialidade para a WLAN, foi desenvolvido o mecanismo de segurança equivalente à transmissão por fio WEP((Wired Equivalent Privacy). Conforme afirma Duntemann's (2004), o objetivo do WEP é proteger a rede sem fio contra intrusos que tentarem acessar a WLAN. O WEP protege os dados que circulam pela WLAN criptografando os mesmos que passam entre os APs e as STAs. Porém, o WEP não é um mecanismo de criptografia *end-to-end*, não

distribui ou gerencia criptografia de chaves, não oculta o tráfego entre as STAs da rede, não autentica usuários, somente verifica chaves criptografadas. Na configuração do WEP é permitido definir quatro chaves a ser utilizada no processo de criptografia e para permitir que os equipamentos se conectem ao AP.

O protocolo WEP utiliza o gerador de número PRNG (*Pseudo Random Number Generator*) através do algoritmo RC4, para gerar uma chave que irá cifrar os dados através de um vetor de inicialização conhecido como IV e de outra chave que será utilizada para cifrar os dados.

Esses novos campos fazem parte do *frame* WEP conforme mostra a Figura 5 abaixo.

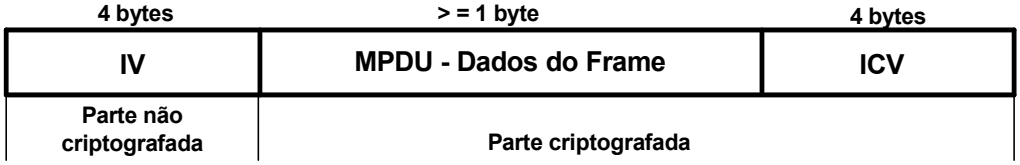


Figura 5 – *Frame* original expandido para o *frame* WEP
Fonte – IEEE802.11b (1999)

O WEP constrói um *frame* incluindo 4 *bytes* no início e 4 *bytes* no fim do *frame* original, sendo os 3 primeiros *bytes* do início utilizados para gerar o vetor de inicialização, permitindo a produção de 16 milhões de valores diferentes. O quarto *byte* contém o valor que define qual das quatros chaves será utilizada. O algoritmo WEP é um processo no qual um conjunto de informação não cifrado passa por várias etapas antes das informações serem enviadas pela rede *wireless*, conforme nota na Figura 6.

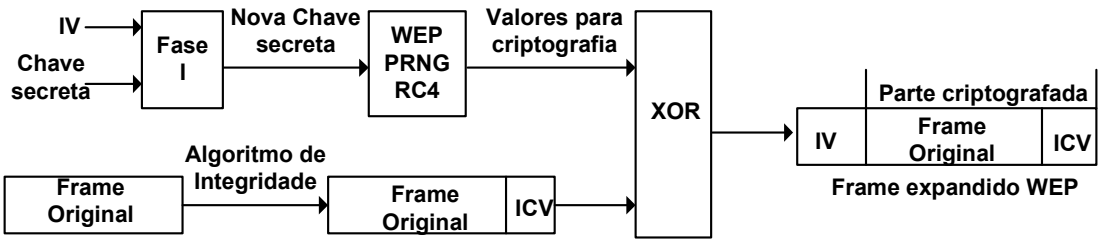


Figura 6 – Diagrama do processo para cifrar dados utilizando WEP

Conforme apresenta a Figura 6, na Fase I a chave secreta é concatenada com o vetor de inicialização (IV) resultando em uma nova chave secreta que será a entrada para o WEP PRNG, o qual gera os valores que serão utilizados para cifrar os dados de origem, através da técnica XOR (*Exclusive OR*). Através dos dados do *frame* original é calculado o ICV (*integrity Check Value*). O resultado é um *frame* expandido WEP com uma parte criptografadas e o vetor de inicialização (IV) que continua sem criptografia. Esse *frame* será enviado para o meio de transmissão sem fio.

No ponto de destino da informação, o processo é executado da maneira inversa, ilustrado na Figura 7 abaixo.

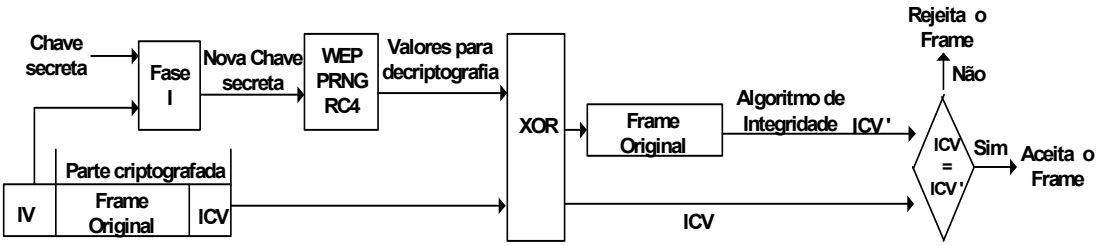


Figura 7 – Diagrama do processo para decifrar dados utilizando WEP

A Figura 7 ilustra o processo de decifragem WEP. O vetor de inicialização que chegou no *frame* em conjunto com a chave secreta irão gerar uma nova chave secreta, o qual será a entrada para o WEP PRNG que através do algoritmo RC4 irá gerar os valores para decifrar os dados do *frame*. No final do processo é calculado outro ICV que será comparado com o ICV gerado no equipamento que enviou o *frame*. Se forem diferentes o *frame* está com erro e será descartado, se forem iguais o *frame* está integro e será enviado para as camadas superiores para processamento.

Em 2001 os especialistas em criptografia Fluhrer; Mantin; Shamir (2001) publicaram um documento relatando um ataque teórico de como capturar a chave de criptografia em uma WLAN protegida pelo protocolo WEP. A partir dessa publicação, surgiram vários *softwares* livres na Internet para transgredir a

segurança WEP. A partir do momento que a fragilidade da tecnologia de segurança WEP tornou-se visível, o IEEE começou a estudar o desenvolvimento de um padrão de segurança que fosse mais confiável que o padrão WEP. Esse padrão é o IEEE 11i com a especificação do protocolo WPA.

3.4 Processo de segurança WPA / TKIP

Em 2003, foi apresentado o primeiro protocolo WPA apoiado nos padrões inicialmente estabelecidos pelo grupo do IEEE 802.11i. Nesse momento a finalidade do WPA foi aprimorar as duas maiores falhas do WEP que são a vulnerabilidade do protocolo e a ineficiência na metodologia de distribuição de chave (MASICA, 2007). Em 2004, o IEEE disponibilizou a tecnologia TKIP com o intuito de aumentar a segurança no padrão original WPA utilizando o mesmo algoritmo de criptografia RC4 que é usado pelo WEP, porém insere outros algoritmos e acrescenta mais campos no *frame*, conforme ilustrado na Figura 8.

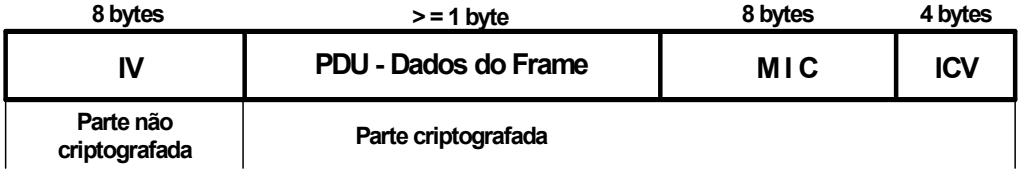


Figura 8 – *Frame* original expandido para o *frame* WPA/TKIP
Fonte – IEEE802.11i (2004)

Conforme mostra a Figura 8 o vetor de inicialização (IV) foi estendido de 3 para 6 *bytes* e foi incluído o campo MIC (*message integrity code*) após o campo de dados. O vetor de inicialização do TKIP é composto de 6 *bytes* subdivido em 6 campos TSC (TKIP *sequence counter*) apresentado na Figura 9.

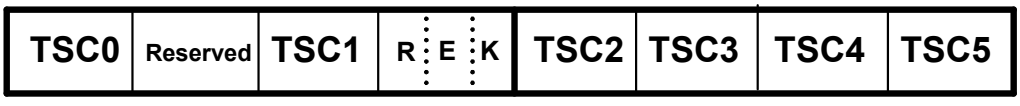


Figura 9 – Campo IV do *frame* WPA/TKIP
Fonte – IEEE802.11i (2004)

O campo “E” tem o tamanho de 1 *bit* e indica se os campos TSC2 , TSC3, TSC4 e TSC5 serão utilizados. Se o campo “E” for igual 1 deverão ser utilizados, se for 0 não serão utilizados. O campo “K” de 2 *bits* é o ID da chave, o campo “R” de 5 *bits* e o *byte* entre os campos TSC0 e TSC1 são reservados. Os campos TSC0 a TSC5 são utilizados no processo de criptografia apresentado na Figura 10 abaixo.

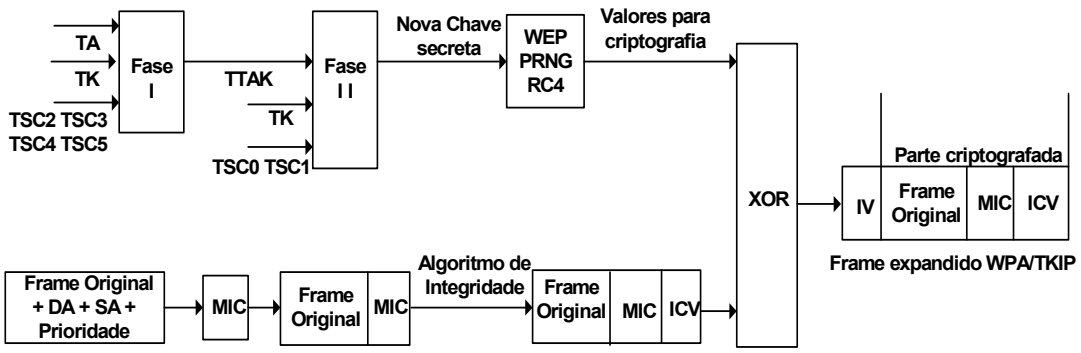


Figura 10 – Diagrama do processo de criptografia WPA/TKIP

A Figura 10 ilustra o processo de criptografia do WPA/TKIP. Em relação ao WEP o processo WPA/TKIP acrescenta outras funções, as quais serão descritas a seguir.

Antes de gerar a chave secreta utilizada para calcular os valores para criptografia, o processo passa por duas fases. Na Fase I os parâmetros de entrada são:

- TA (*Trasmiter Address*) – É composto pelo MAC *address* do transmissor do *frame*.

- TK (*Temporal Key*) – Dentre as novidades do WPA/TKIP é a possibilidade da preservação do segredo mediante a troca constante da *Temporal key* (RUFINO, 2005). Seu tamanho varia de 40 a 64 caracteres.

- TSC2, TSC3, TSC4 e TSC5 – Cada campo TSC possui 1 *byte* e são gerados dinamicamente.

Esses três campos passam na Fase I por um sistema de cálculo gerando o campo TTAK (*TKIP-mixed transmit address and key*) de 10 *bytes*. Esse campo será utilizado como entrada pela Fase II junto com o TK e TSC0 e TSC1. A saída será uma nova chave secreta de 16 *bytes* que será a entrada para o WEP PRNG. Como no processo de criptografia WEP, o PRNG/RC4, gera os valores que serão utilizados para cifrar os dados de origem e também o campo MIC, através da técnica XOR.

O WPA/TKIP adiciona o campo MIC (*message integrity code*) que visa detectar mensagens falsificadas e outras tentativas de violação nas transmissões que utilizam a WLAN. O MIC é composto de 8 *bytes* gerado a partir de um sistema de calculo que utiliza os campos do *frame* DA (*Destination Address*), SA (*Source Address*), *priority* e o dados de origem. O MIC será utilizado no processo de decifragem, descrito abaixo, para detectar possível tentativa de acesso não autorizado ao *frame* da WLAN.

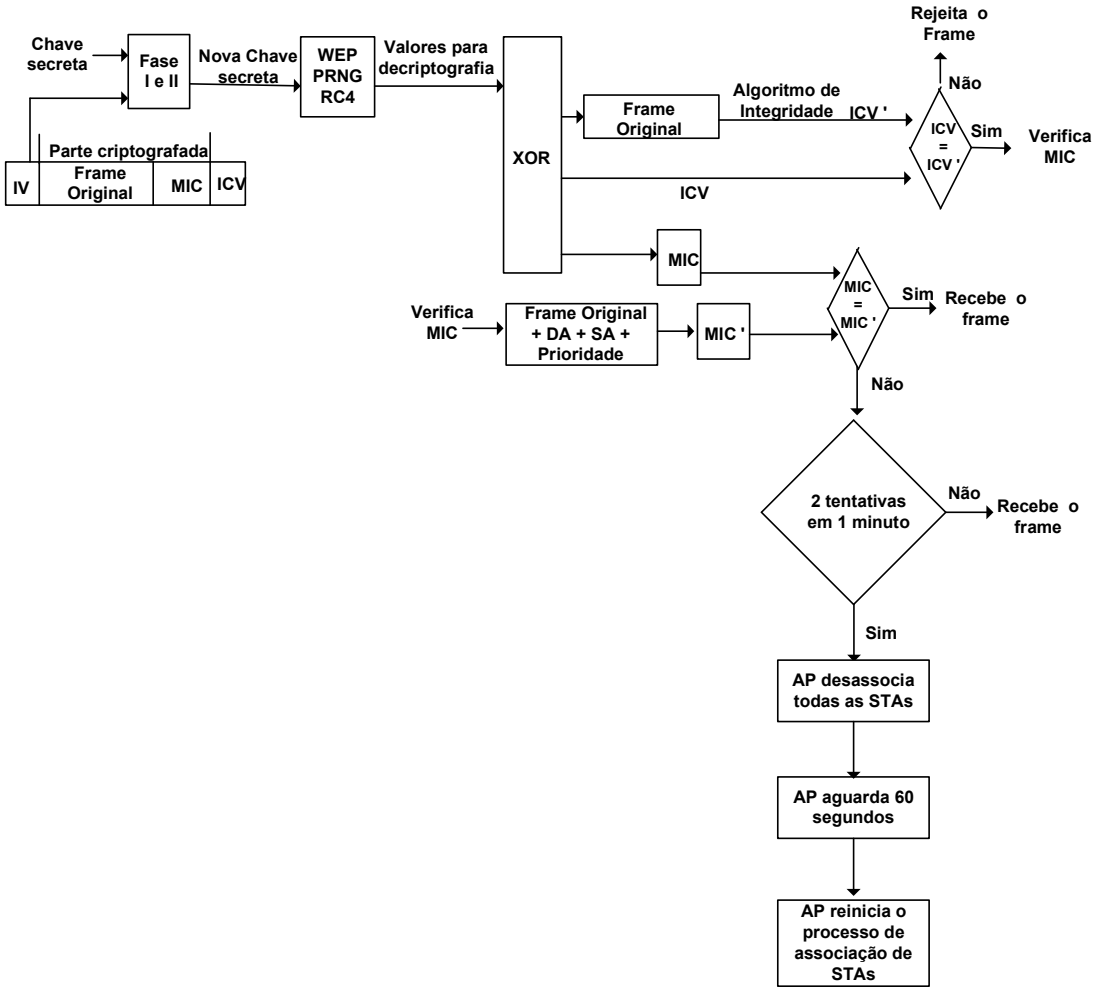


Figura 11 – Diagrama do processo para decifrar dados utilizando WPA/TKIP

Idêntico ao processo de cifragem, o processo de decifragem WPA passa por duas fases antes de gerar a nova chave secreta a ser utilizada pelo WEP PRNG. Na Figura 11, se observa que após a verificação do campo ICV, existe a verificação de integridade do campo MIC. Se o campo MIC que foi calculado na origem e enviado pela rede, for diferente do campo MIC calculado novamente no processo de decifragem do destino, o sistema considera que o campo MIC pode ter sido violado.

Um erro no recebimento do campo MIC, pode ser sinal de uma tentativa de violação na rede WLAN protegida pelo protocolo de segurança WPA/TKIP. Se ocorrerem dois erros no recebimento do campo MIC no período de um minuto o

WPA/TKIP desassocia todas as STAs conectadas no AP e o mesmo fica indisponível durante 60 segundos. Isso dificulta um invasor de enviar um grande numero de falsas tentativas em um curto período de tempo (IEEE802.11i, 2004).

Conforme descrito acima, os protocolos de segurança além de utilizar algoritmos e cálculos matemáticos adicionam informações nos pacotes a serem transmitidos, impactando no desempenho da rede sem fio.

3.5 Estimativa da degradação do desempenho da WLAN, com a implantação dos protocolos de segurança

Pode-se estimar o impacto no desempenho na WLAN, devido às informações incluídas no *frame*, as quais serão utilizadas no processo de segurança.

Conforme salienta Torres (2001), na cada camada do TCP/IP é incluído cabeçalho (*header)* com informações de controle usadas por cada uma das camadas do protocolo.

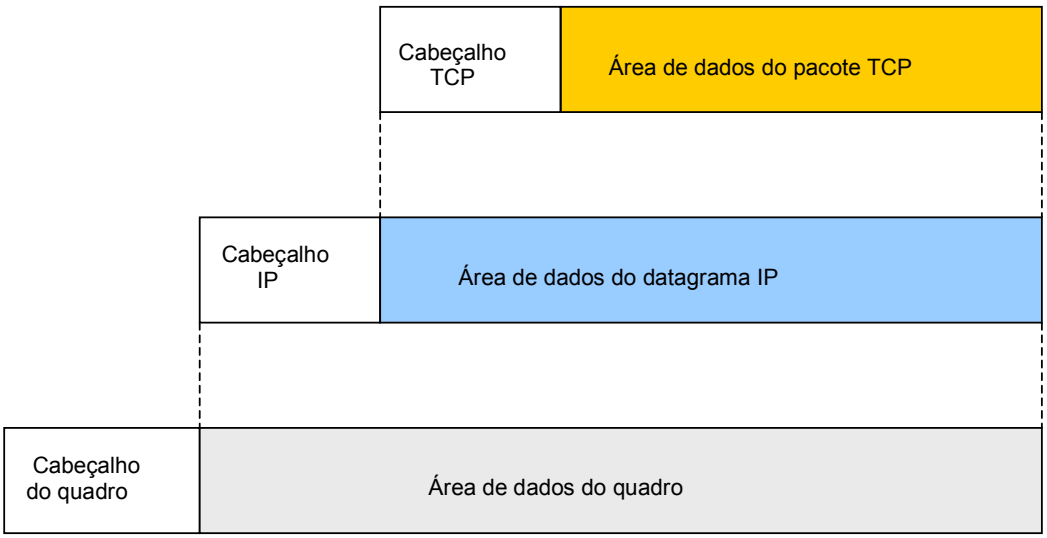


Figura 12 – Encapsulamento do protocolo de dados do TCP
Fonte – Torres (2001)

Na Figura 12 observa-se que na camada de transporte TCP, o protocolo inclui o cabeçalho (*header* TCP), a camada IP adiciona o cabeçalho (*header* IP) e a camada de interface de rede inclui o cabeçalho (*header*) do quadro (*frame*). Em uma WLAN são incluídas informações específicas do padrão 802.11, apresentada na Figura 13.

24 bytes	30 bytes	20 bytes	20 bytes	> = 1 byte	4 bytes
PCLP	MAC Cabeçalho	IP Cabeçalho	TCP Cabeçalho	Dados	FCS

Figura 13 – *Frame* específico da 802.11

Nota-se na Figura 13, o padrão 802.11 insere o cabeçalho denominado *preâmbulo* PLCP (*Physical Layer Convergence Protocol*) de 24 *bytes* no inicio do *frame* (IEEE802.11, 1999).

O protocolo de segurança WEP insere 8 *bytes* e o WPA/TKIP adiciona 20 *bytes* no *frame* apresentado nas Figuras 14 e 15 respectivamente.

24 bytes	30 bytes	8 bytes	20 bytes	20 bytes	> = 1 byte	4 bytes
PCLP	MAC Header	WEP	IP Header	TCP Header	Dados	FCS

Figura 14 – *Frame* especifico da 802.11 com o campo WEP

24 bytes	30 bytes	20 bytes	20 bytes	20 bytes	> = 1 byte	4 bytes
PCLP	MAC Header	WPA/ TKIP	IP Header	TCP Header	Dados	FCS

Figura 15 – *Frame* especifico da 802.11 com o campo WPA/TKIP

Com a inclusão dos campos WEP e WPA/TKIP é possível estimar o quanto essas informações degradam o desempenho da WLAN devido ao incremento no tamanho do *frame*. O processamento dos dados para cifrar/decifrar os dados e o efeito da atenuação os quais degradam o desempenho da WLAN não serão

estimados nessa seção. Esses fatores serão concluídos após a execução do experimento.

Conforme será descrito, em detalhe no Capitulo 4, os tamanhos dos pacotes variam em três conjuntos e pode-se estimar a degradação de desempenho em cada um deles.

No primeiro conjunto, os tamanhos dos pacotes variam entre 64 e 1460 *bytes*. Para a finalidade de estimativa, será considerado o tamanho médio dos pacotes entre 64 e 1460 igual a 762 *bytes.* Dessa maneira os tamanhos dos *frames* com os equipamentos configurados sem segurança, com o WEP e WPA/TKIP são os apresentados nas Figuras 16, 17 e 18.

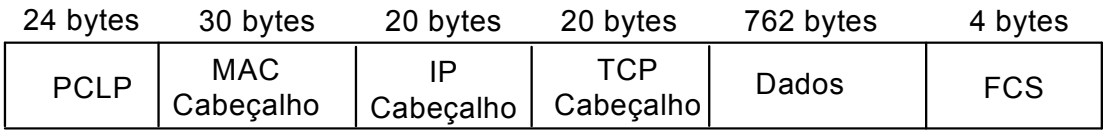


Figura 16 – *Frame* especifico da 802.11 sem segurança e tamanho do campo dados igual 762 *bytes*

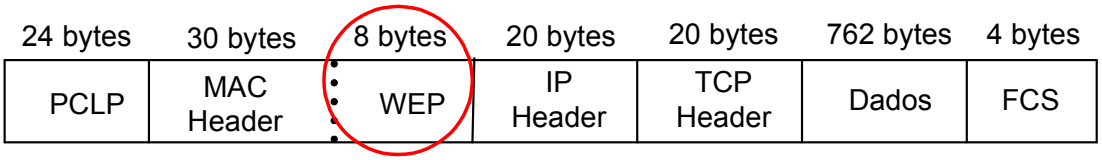


Figura 17 – *Frame* especifico da 802.11 com WEP e tamanho do campo dados igual 762 *bytes*

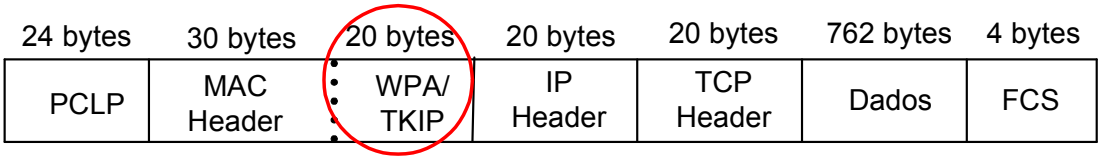


Figura 18 – *Frame* especifico da 802.11 com WPA/TKIP e tamanho do campo dados igual 762 *bytes*

De acordo com a Figura 16, o *frame* contém um total 860 *bytes*. Conforme mostra a Figura 17, quando no equipamento é configurado o WEP há um acréscimo de 8 *bytes* no *frame*, que acarreta uma sobrecarga de 1% em relação ao *frame* sem segurança. A Figura 18 apresenta o *frame* com o WPA/TKIP habilitado, ocorrendo um acréscimo de 20 *bytes* em relação ao *frame* sem segurança e 12 *bytes* em relação ao *frame* com o WEP, afetando a performance da WLAN em 2% em relação a sem segurança e 1,5% em relação ao protocolo WEP.

No segundo conjunto, os tamanhos dos pacotes variam entre 32 e 256 *bytes*. Da mesma maneira que na estimativa anterior, será considerado o tamanho médio dos pacotes entre 32 e 256 igual a 144 *bytes*. Assim, os *frames* com os equipamentos configurados sem segurança, com o WEP e WPA/TKIP são os apresentados nas Figuras 19, 20 e 21, onde nota-se na Figura 19 que o *frame* sem segurança possui o tamanho de 242 *bytes*.

24 bytes	30 bytes	20 bytes	20 bytes	144 bytes	4 bytes
PCLP	MAC Cabeçalho	IP Cabeçalho	TCP Cabeçalho	Dados	FCS

Figura 19 – *Frame* especifico da 802.11 sem segurança e tamanho do campo dados igual 144 *bytes*

24 bytes	30 bytes	8 bytes	20 bytes	20 bytes	144 bytes	4 bytes
PCLP	MAC Header	WEP	IP Header	TCP Header	Dados	FCS

Figura 20 – *Frame* especifico da 802.11 com WEP e tamanho do campo dados igual 144 *bytes*

		20 bytes				
PCLP	MAC Header	WPA/ TKIP	IP Header	TCP Header	Dados	FCS

Figura 21 – *Frame* especifico da 802.11 com WPA/TKIP e tamanho do campo dados igual 144 *bytes*

Observa-se nas Figuras 20 e 21 que com a adição dos campos WEP (8 *bytes*) e do WPA/TKIP (20 *bytes*) a estimativa na degradação do desempenho da WLAN com os pacotes de dados iguais a 144 *bytes* é de 3% quando os equipamentos estão habilitados com WEP em relação a sem segurança e 5% com os equipamentos configurados com WPA/TKIP em relação ao protocolo WEP. Para equipamentos configurados com WPA/TKIP em relação aos sem segurança estima-se que a degradação é de 8%.

Finalmente no terceiro conjunto, os tamanhos dos pacotes se mantiveram fixos em 1460 *bytes*. Portanto os tamanhos dos *frames* são os apresentados nas Figuras 22, 23 e 24.

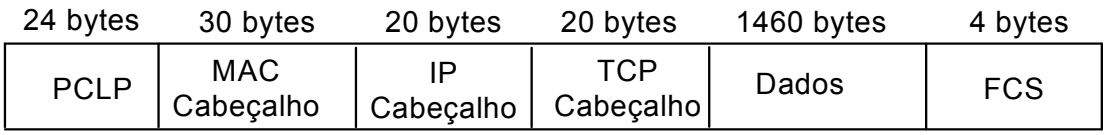


Figura 22 – *Frame* especifico da 802.11 sem segurança e tamanho do campo dados igual 1460 *bytes*

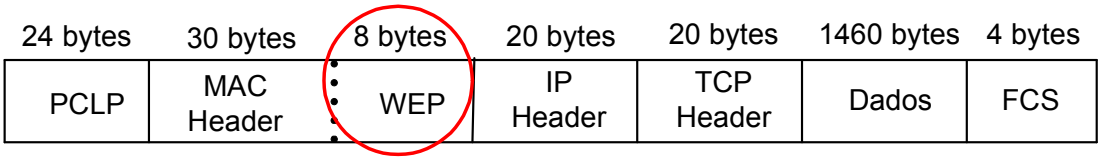


Figura 23 – *Frame* especifico da 802.11 com WEP e tamanho do campo dados igual 1460 *bytes*

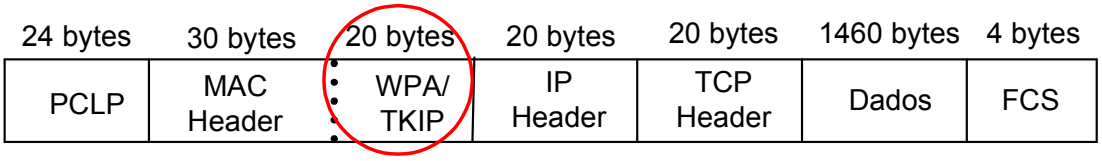


Figura 24 – *Frame* especifico da 802.11 com WPA/TKIP e tamanho do campo dados igual 1460 *bytes*

Conforme as Figuras 22, 23 e 24, os tamanhos dos *frames* são 1558 *bytes*, 1566 *bytes* e 1578 *bytes* respectivamente, o que ocasiona uma degradação do desempenho da WLAN de 0,5% do protocolo WEP em relação à sem segurança. A estimativa da degradação do protocolo WPA/TKIP em relação ao WEP é de 1% e 1,5 % do protocolo WPA/TKIP em relação a sem segurança.

4 METODOLOGIA DO EXPERIMENTO

O objetivo desse experimento é realizar emulações em laboratório de rede sem fio, implementando os protocolos de segurança para analisar o impacto destes na performance de WLAN, conforme será descrito a seguir.

Experimento em Laboratório: No laboratório de pesquisa em sistema de rádio da PUC Campinas, será efetuado os experimentos por meio de uma bancada montada para emulação de sinais de rádio freqüência, que possui um ambiente fechado *wireless* e utilizando o *software* LanTraffic™ para a geração de tráfego e coleta dos dados. Primeiramente, serão emulados no laboratório três cenários, em que as STAs estarão distantes entre si. No primeiro cenário as distância entre as STAs serão de 0 à 50 metros, depois de 50 à 100 metros e depois de 100 à 200 metros. Quando configurados os equipamento para emular uma distância acima de 200 metros a STA o perde a conexão com o AP.

Para cada um desses cenários os equipamentos serão configurados sem segurança, posteriormente com WEP habilitado e por fim com o WPA/TKIP configurado.

Finalmente dentro das combinações distância e protocolos de segurança configurados, serão enviados pacotes com tamanhos diferentes em três conjuntos. No primeiro os conjuntos de pacotes serão enviados variando o tamanho de 64 à 1460 *bytes*, no segundo os conjuntos irão variar de 32 à 256 *bytes* e no terceiro irão se manter fixo em 1460 bytes. Os pacotes serão enviados entre as STAs através de 15 conexões TCP. As 15 conexões TCP são estabelecidas utilizando o *software* LanTraffic™ conforme Figura 25.

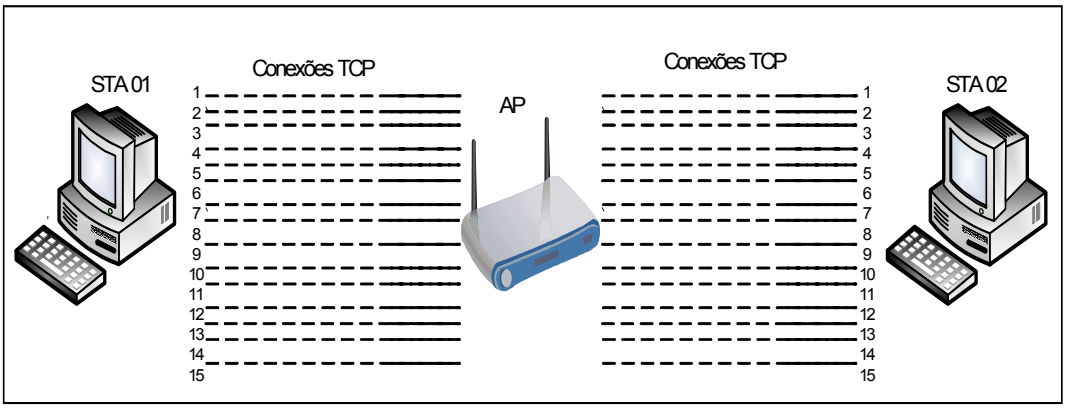


Figura 25 – Conexões TCP estabelecida entre os equipamentos da WLAN

Conforme ilustra a Figura 25, além da variação nos tamanhos dos pacotes foi configurado no software LanTraffic™, para estabelecer 15 sessões TCP entre as STA 01 e STA 02, com isso ocorrendo um maior fluxo de dados entre as STAs e o AP, emulando várias STAs trocando informações entre si e o AP.

Foi utilizado o TCP, pois o intuito do experimento é emular a utilização de WLAN em um ambiente de trabalho nas empresas, onde o TCP é utilizado devido principalmente a esse protocolo garantir a entrega dos pacotes e as aplicações a serem citadas no Item 4.5 utilizam o protocolo TPC/IP.

Durante os experimentos, os dados serão compilados e analisados, gerando os gráficos e tabelas, com o intuito de comprovar em laboratório a degradação da performance da WLAN com a implementação dos protocolos de segurança . Os dados são capturados na STA 02 e armazenado em um arquivo de texto com nome e local de armazenamento configurado no *software* LanTraffic™. Após os experimentos os dados serão compilados e analisados conforme detalhado no Capítulo 5.

Finalmente, os dados serão comparados e poderá ser verificado o impacto no desempenho da rede WLAN com a utilização dos protocolos de segurança, WEP e WPA/TKIP.

4.1 Cenário do experimento

Os experimentos serão realizados na bancada instalada no laboratório de pesquisa em sistema de rádio enlace da PUC Campinas cuja topologia física será apresentada na Figura 26.

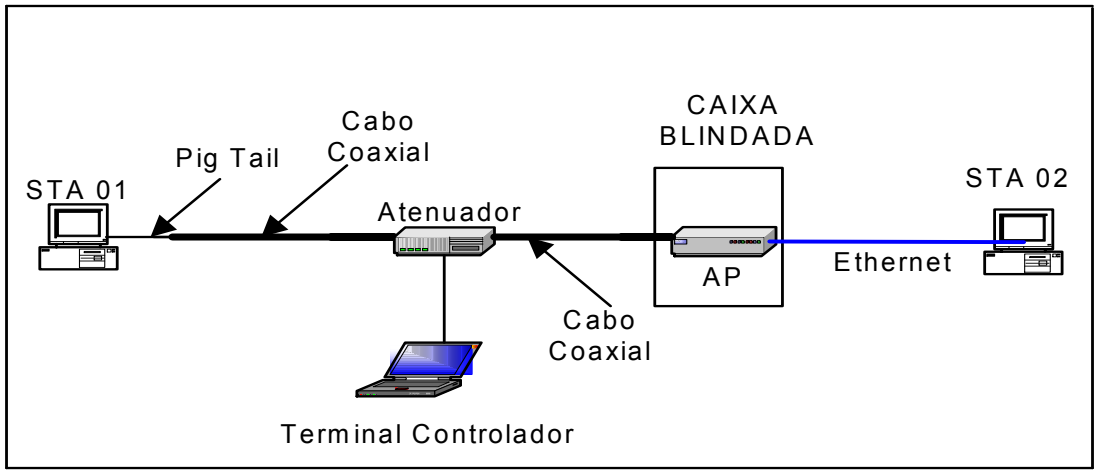


Figura 26 – Topologia física da WLAN no laboratório da PUC Campinas

Salientamos o cuidado em se manter o ambiente, visto na Figura 26 sob controle por meio das conexões entre os equipamentos da WLAN, os quais são efetuados através de cabo coaxial e com isso eliminando interferências na transmissão dos sinais emitidos pelos equipamentos.

A STA 01 utiliza o Pig Tail para conectar a placa wireless com o cabo coaxial. Pig tail ou cabo proprietário é um pequeno fio flexível e fino com conectores apropriados nas duas extremidades. Sua função é conectar uma antena externa ao rádio ou placa wireless.

Essa bancada foi construída no laboratório de pesquisa em sistema de rádio da PUC Campinas para o desenvolvimento de outra pesquisa e tem como intuito de confinar o sinal de uma rede sem fio em cabo coaxial, para que outras pesquisas possam ser desenvolvidas. (GOES; BRANQUINHO; REGGIANI, 2006).

Entre a STA 01 e o AP existe um circuito atenuador, que possibilita controlar potência Rx da STA 01, emulando dessa maneira a distância da STA 01 em relação ao AP. O circuito atenuador é composto por duas chaves, controladas por duas fontes de tensão que variam de 0 a 5V, ligadas em série a um atenuador variável, que é acessado por um terminal controlador através de um conversor digital analógico conectado na porta paralela. Na saída do circuito atenuador encontra-se um divisor de sinal, o qual envia o sinal de rádio freqüência (RF) para a STA 01.

A descrição detalhada da bancada está contida no Anexo A dessa dissertação. Verifica-se que através de calibrações consegue-se emular o ambiente de maneira estável e segura, conforme descrito no Item 4.4.

4.2 *Hardwares* utilizados

Os *hardwares* utilizados para a execução dos experimentos são os descritos abaixo:

- STA 01 e STA 02 : Micro computador HP Compaq com 256 Mega de memória, com 4 processadores Pentium III de 2.4 GHz.

- AP : Modelo Air Live 802.11 a/b/g Wireless AP WL-5460AP

Figura 27 – AP utilizado nos experimentos

- Placa PCI *wireless* EW7128G *Chipset* RTL8185 instalada na STA 02.
  - Compatível com os protocolos 802.11b e 802.11g.
  - Criptografias WEP e WPA/TKIP.

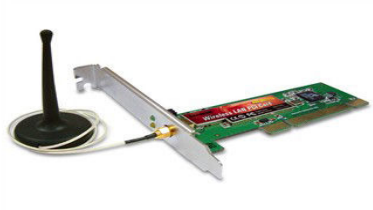


Figura 28 – Placa instalada na STA 02

4.3 *Softwares* utilizados

Os Softwares utilizados para a execução dos experimentos são os descritos abaixo:

- STA 01 : Sistema operacional Windows XP service pack 2. É utilizado o Windows, pois o intuito do experimento é analisar a degradação de performance na rede WLAN devido à implementação dos protocolos de segurança. Portanto, o sistema operacional não será considerado no experimento.

  LanTraffic™ V.2

- STA 02 : Sistema operacional Windows XP service pack 2.

  LanTraffic™ V.2

4.4 Procedimentos do experimento

Foi utilizado o *software* LanTraffic™ para configurar a geração de tráfego na rede e também para capturar a taxa de transmissão em Kbps entre a STA 01 e STA 02. Utilizada a mesma configuração de geração de tráfego para todos os cenários usados no experimento.

Na STA 02 foi utilizado também o LanTraffic™ para capturar a taxa de transmissão em Kbps trafegados na rede e armazenado em arquivo de *log*.

Para a execução dos experimentos foram parametrizados três cenários apresentados na Tabela 3 abaixo. Os parâmetros presentes na tabela foram medidos na STA 01.

Tabela 3 – Parâmetros utilizados nos três cenários

Parâmetros	Cenário 01	Cenário 02	Cenário 03
Potência Rx (dBm)	-57 à -61	-65 à -69	-73 à -77
Taxa nominal (Mbps)	54-36-24	24-18-12-11	12-11-6-2-1
Distância simulada (metros)	0 à 50	50 à 100	100 à 200

Através dos valores das potências medidas na STA 01 pode-se calcular a distância entre a STA 01 e o AP.

Conforme Rappaport (2002), o modelo de propagação de sinal em espaço, no qual não ocorre atenuações no sinal recebido pelo equipamento receptor, representa um ambiente ideal. Porém, na realidade a potência de recepção em uma determinada distância é uma variável randômica devido a variação e perda na potência dos sinais de transmissão no trajeto do sinal entre dois equipamentos. Portanto, de acordo com Rappaport (2002), o modelo mais adequado e utilizado mundialmente em transmissão de sinal de rádio é chamado de modelo de sombreamento.

O modelo de sombreamento consiste de duas partes. A primeira parte é conhecida como modelo de perda da potência no trajeto do sinal, a qual degrada a potência recebida a uma distância d, indicada por Pr(d) e utiliza d_0 como uma distância próxima do rádio. A segunda parte reflete a variação da potência recebida a uma distância, através de uma variável randômica em logaritmo, denominada distribuição gaussiana se medida em dB. Assim, as distâncias emuladas podem ser obtidas, de acordo com Rappaport (2002), através das Equações 1, 2 e 3.

$$PL(d_0) = 10 \log \left[(4 * \pi * d_0 / \lambda)^2 \right] \quad \textbf{(1)}$$

$$P_{rx}(d_0) = P_{tx} + G_{tx} + G_{rx} - PL(d_0) \quad \textbf{(2)}$$

$$P_{rx}(d) = P_{rx}(d_0) - 10 * \beta * \log[(d)/d_0] \quad \textbf{(3)}$$

Onde:

d_0 :Distância de referência, sendo considerado 1 metro para ambientes internos.

$\lambda = C / f$:Comprimento de onda. Onde *C* é a velocidade da luz e *f* é a freqüência de operação do rádio.

d:Distância da STA em relação ao AP.

P:Potência, sendo rx de recepção e tx de transmissão.

G_{tx} e G_{rx}:Ganho das antenas potência, sendo considerado ganho nulo.

β:Expoente de perda na trajetória (*path loss exponent*). Conforme relata Rappaport (2002), o valor *β* igual 2,0 representa um espaço livre o que não ocorrem em WLAN, pois sempre ocorre atenuações nos sinais transmitido entre os equipamentos. Medidas efetuadas por Rajesh (2003) revelaram que em ambiente aberto (*outdoor*) sem obstrução, *β* varia de 2,2 à 3. Portanto, nesse experimento foi considerado o valor de 2,5 o qual está dentro dos valores citado acima.

Utilizando os recursos existentes na bancada Figura 26, pode-se ajustar a sensibilidade do sinal na STA 01. Através da potência e dos parâmetros da

Tabela 3 e utilizando as Equações (1), (2) e (3), emula-se a distância da STA 01 em relação ao AP. Ajustando a potencia na STA 01, a distância emulada também varia, conforme a Figura 29 abaixo.

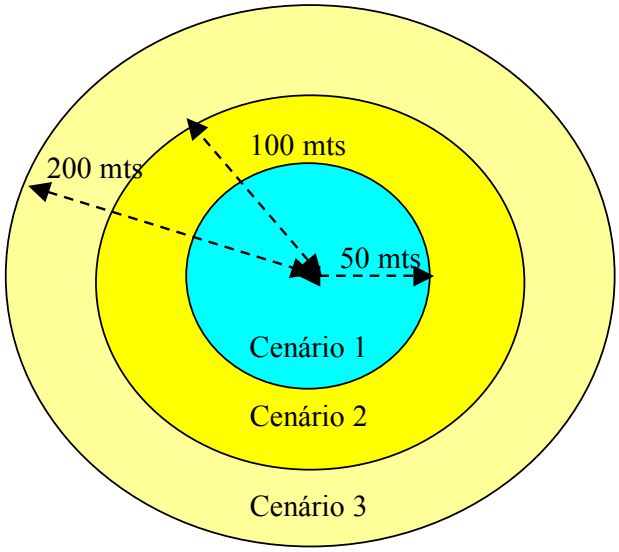


Figura 29 – Distância emulada para os três cenários

A medida que um usuário se afasta do *Access Point*, os dispositivos baseados no 802.11g reduzem a taxa de transmissão passando a utilizar as técnicas de modulação CCK, DQPSK e DBPSK para fornecer taxas de 11/5,5 Mbps, 2 Mbps e 1 Mbps respectivamente.

Para cada cenário foi gerado tráfego de pacotes da STA 01 para a STA 02 com os equipamentos configurados sem segurança, com os protocolos de segurança WEP e WPA/TKIP.

Detalhes da configuração do AP e da STA estão contidos no Anexo B desta dissertação.

4.5 Gerações dos pacotes na rede WLAN

Para cada cenário descrito no Item 4.4, foi feita a geração dos pacotes na rede com variação de tamanho. A parametrização no *software* LanTraffic^{TM}, que possibilita gerar pacotes na WLAN de tamanhos variados e isso foi feito, conforme descrito a seguir:

- Primeiro. Os três cenários tiveram tamanhos dos pacotes variando de 64 *bytes* até 1460 *bytes*. Essas variações no tamanho dos pacotes emulam um perfil de usuário que utiliza várias aplicações em sua STA.

- Segundo. Nos três cenários os tamanhos dos pacotes variaram de 32 *bytes* até 256 *bytes*. Esse experimento emula aplicações transacionais cuja característica é a transferências de pequenos dados entre dois equipamentos. Exemplo: Apontamento de produção, ERPs (*Enterprise Resource Planning*), pequenos e-mails, etc.

- Terceiro. O tamanho dos pacotes se mantiveram fixos em 1460 bytes nos três cenários. Esse experimento emula aplicação como o FTP (*File Transfer Protocol*), acesso a arquivo no *file server*, HTTP (*Hyper Text Transfer Protocol*), etc.

As gerações dos tráfegos de pacotes duraram 180 minutos no total para cada cenário conforme apresentado nas Tabelas 4, 5 e 6.

Tabela 4 – Execução dos experimentos: Cenário 01

Experimento	Protocolo de segurança	Tamanhos dos pacotes	Duração (minutos)
01	SEM	32 à 256	20
02	SEM	64 à 1460	20
03	SEM	1460	20
04	WEP	32 à 256	20
05	WEP	64 à 1460	20
06	WEP	1460	20
07	WPA/TKIP	32 à 256	20
08	WPA/TKIP	64 à 1460	20
09	WPA/TKIP	1460	20
TOTAL CENÁRIO 01			**180**

Tabela 5 – Execução dos experimentos: Cenário 02

Experimento	Protocolo de segurança	Tamanhos dos pacotes	Duração (minutos)
10	SEM	32 à 256	20
11	SEM	64 à 1460	20
12	SEM	1460	20
13	WEP	32 à 256	20
14	WEP	64 à 1460	20
15	WEP	1460	20
16	WPA/TKIP	32 à 256	20
17	WPA/TKIP	64 à 1460	20
18	WPA/TKIP	1460	20
TOTAL CENÁRIO 02			**180**

Tabela 6 – Execução dos experimentos: Cenário 03

Experimento	Protocolo de segurança	Tamanhos dos pacotes	Duração (minutos)
19	SEM	32 à 256	20
20	SEM	64 à 1460	20
21	SEM	1460	20
22	WEP	32 à 256	20
23	WEP	64 à 1460	20
24	WEP	1460	20
25	WPA/TKIP	32 à 256	20
26	WPA/TKIP	64 à 1460	20
27	WPA/TKIP	1460	20
TOTAL CENÁRIO 03			**180**

Os resultados obtidos são os apresentados a seguir. Os experimentos foram repetidos duas vezes e os dados mantiveram os mesmos resultados.

5 RESULTADOS

Utilizando os métodos para a transmissão e captura dos dados descritos no Capítulo 4, se obteve a taxa de transmissão em Kbps entre os equipamentos da WLAN. As medidas da taxa de transmissão foram coletadas conforme descrito no Item 4.4.

Para a geração das médias mencionadas nas tabelas a seguir foi utilizada, conforme Barradas (1982, p.195) a Equação 4 para cálculo da média.

$$\mu = \sum_{i=1}^{N} x_i \left(\frac{f_i}{\sum_{i=1}^{N} f_i} \right) \qquad \textbf{(4)}$$

Onde:

μ: Média, da taxa em Kbps trafegado pela rede

x_i : Valor da taxa coletada.

f_i :Freqüência ou a quantidade de vezes que um determinado valor se repetiu durante o experimento.

Portanto, o valor médio é igual à soma dos produtos dos valores individuais pelas suas freqüências relativas de ocorrências.

Essa média é obtida utilizando planilha do Excel, através da opção de análise de dados.

Os resultados serão apresentados nas Tabelas 7, 8 e 9. Os histogramas das medidas estão contidos no Anexo C desta dissertação.

5.1 Demonstrativo dos resultados

Na Tabela 7 estão apresentadas as médias dos resultados dos experimentos efetuados no laboratório, onde os tamanhos dos pacotes variaram de 64 *bytes* até 1460 *bytes.*

Tabela 7 – Taxa de transmissão em Kbps trafegado na WLAN com os tamanhos dos pacotes variando de 64 a 1460 *bytes*

Configuração	Cenário 01 Média	Cenário 02 Média	Cenário 03 Média
Sem Segurança	15.915	8.410	4.905
WEP	15.615	8.145	4.705
WPA/TKIP	15.140	7.670	4.320

O Gráfico 1 ilustra um comparativo da média taxa de transmissão, através dos valores contidos na Tabela 7.

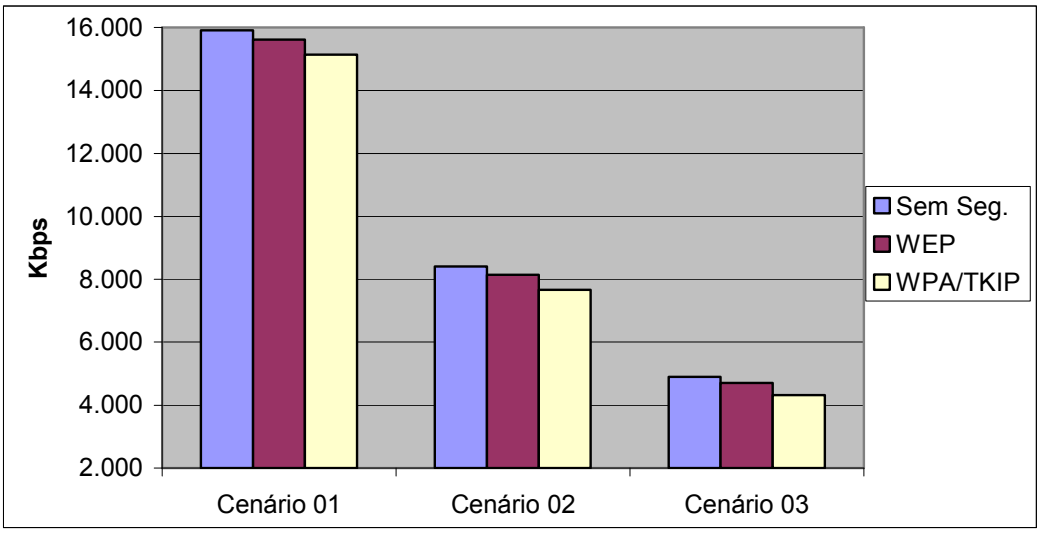


Gráfico 1 – Comparativo da Taxa da transmissão em Kbps trafegada na WLAN com pacotes variando de 64 a 1460 *bytes*

Na Tabela 8 estão apresentadas as médias dos resultados dos experimentos efetuados no laboratório, onde os tamanhos dos pacotes variaram de 32 *bytes* até 256 *bytes.*

Tabela 8 – Taxa de transmissão em Kbps trafegado na WLAN com os tamanhos dos pacotes variando de 32 a 256 *bytes*

Configuração	Cenário 01 Média	Cenário 02 Média	Cenário 03 Média
Sem Segurança	14.740	7.920	4.405
WEP	14.325	7.565	4.135
WPA/TKIP	13.605	6.950	3.710

O Gráfico 2 ilustra um comparativo da média da taxa de transmissão, através dos valores contidos na Tabela 8.

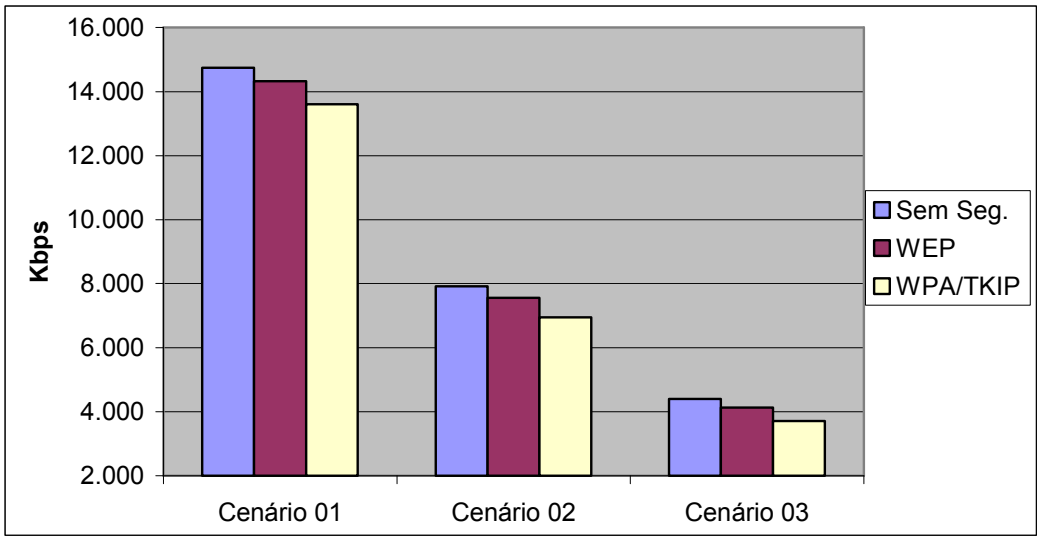


Gráfico 2 – Comparativo da Taxa da transmissão em Kbps trafegada na WLAN com pacotes variando de 32 a 256 *bytes*

Na Tabela 9 estão apresentadas as médias dos resultados dos experimentos efetuados no laboratório, onde o tamanho dos pacotes se manteve fixo em 1460 *bytes*.

Tabela 9 – Taxa de transmissão em Kbps trafegado na WLAN com os tamanhos dos pacotes mantendo fixo em 1460 *bytes*

Configuração	Cenário 01 Média	Cenário 02 Média	Cenário 03 Média
Sem Segurança	20.935	9.240	5.395
WEP	20.695	9.020	5.235
WPA/TKIP	20.260	8.545	4.930

O Gráfico 3 ilustra um comparativo da média da taxa de transmissão, através dos valores contidos na Tabela 9.

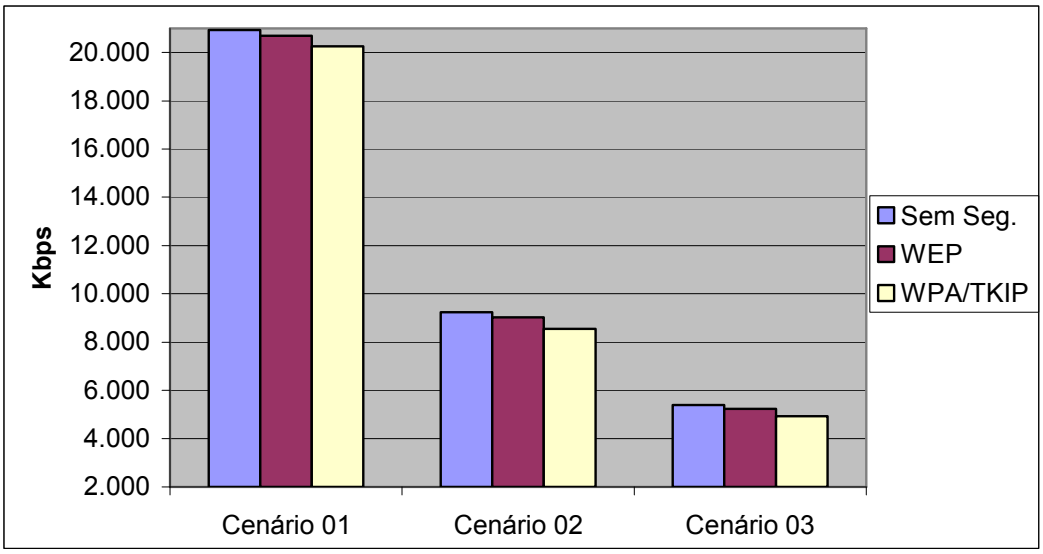


Gráfico 3 – Comparativo da Taxa da transmissão em Kbps trafegada na WLAN com pacotes mantendo fixo em 1460 *bytes*

Os *Throughputs (vasões)* obtido por conexão estão de acordo com WP802.11g (2003), onde em WLAN com TCP, o *throughput* máximo esperado por cada conexão TCP utilizando interfaces 802.11g em relação à distância (em metros) são os ilustrados na Tabela 10.

Tabela 10 – *Throughput* máximo esperado para ambientes IEEE 802.11g

Distância Metros	15,2	30,5	49,0	61,0	76,0	91,0
Throughput Mbps	24,7	19,8	12,4	4,9	1,6	0,9

Fonte – WP802.11g (2003)

5.2 Avaliação e análise dos resultados

Para a análise dos resultados foram geradas as Tabelas 11, 12 e 13, apresentando em porcentagem, a degradação do desempenho com a implementação dos protocolos de segurança e com a variação dos tamanhos dos pacotes.

Tabela 11 – Comparativo de desempenho entre os protocolos de segurança com pacotes de 64 a 1460 *bytes*

Diferenças	Cenário 01 Média	Cenário 02 Média	Cenário 03 Média
WEP em relação a sem segurança	2%	3%	4%
WPA/TKIP em relação a WEP	3%	6%	8%
WPA/TKIP em relação a sem segurança	5%	9%	12%

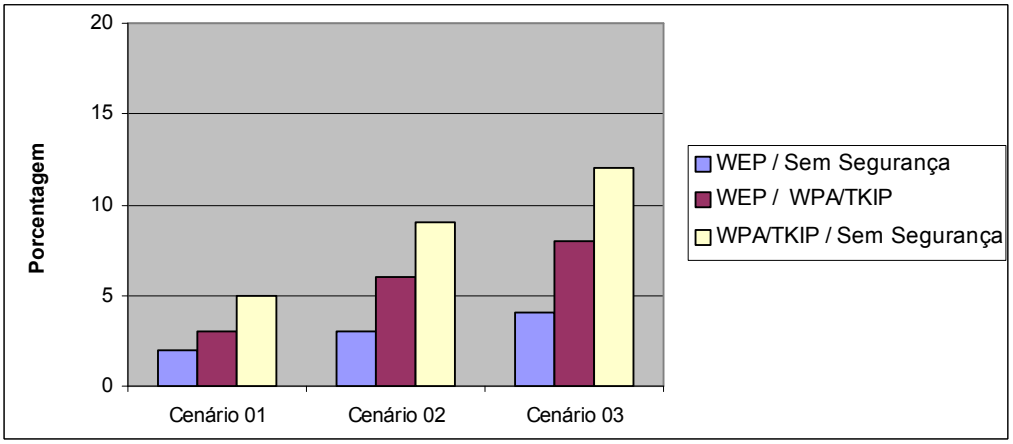


Gráfico 4 – Comparativo de desempenho entre os protocolos de segurança com pacotes de 64 a 1460 *bytes*

Tabela 12 – Comparativo de desempenho entre os protocolos de segurança com pacotes de 32 a 256 *bytes*

Diferenças	Cenário 01 Média	Cenário 02 Média	Cenário 03 Média
WEP em relação a sem segurança	3%	4%	6%
WPA/TKIP em relação a WEP	5%	8%	10%
WPA/TKIP em relação a sem segurança	8%	12%	16%

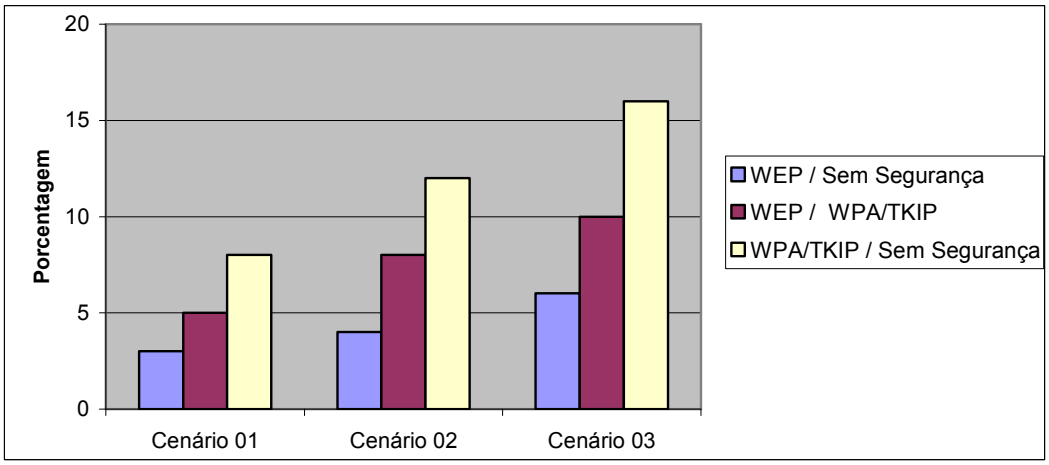


Gráfico 5 – Comparativo de desempenho entre os protocolos de segurança com pacotes de 32 a 256 *bytes*

Tabela 13 – Comparativo de desempenho entre os protocolos de segurança com pacotes de 1460 *bytes*

Diferenças	Cenário 01 Média	Cenário 02 Média	Cenário 03 Média
WEP em relação a sem segurança	1%	2%	3%
WPA/TKIP em relação a WEP	2%	5%	6%
WPA/TKIP em relação a sem segurança	3%	7%	9%

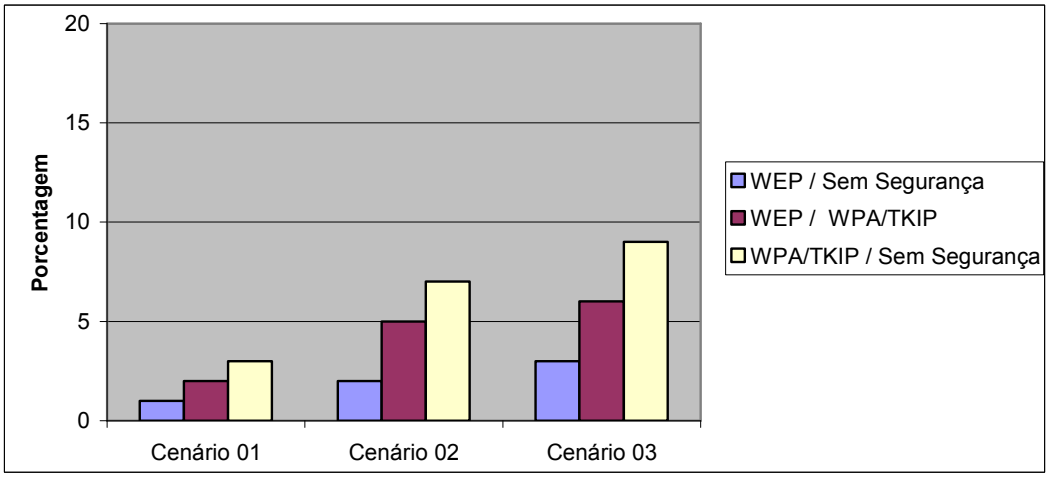


Gráfico 6 – Comparativo de desempenho entre os protocolos de segurança com pacotes de 1460 *bytes*

Analisando os dados das Tabelas 11, 12 e 13 com o intuito de comparar o desempenho entre os equipamentoss configuradas sem segurança com as mesmas configuradas com WEP e WPA/TKIP, verifica-se que há uma degradação da performance quando os protocolos de segurança são implementados.

A menor degradação está na Tabela 13, na qual nota-se que o protocolo WEP degrada o desempenho em relação ao equipamento configurado sem segurança em 1% no Cenário 01, 2% no Cenário 02 e 3% no Cenário 03. O protocolo WPA/TKIP degrada o desempenho em relação ao WEP em 2% no Cenário 01, 5% no Cenário 02 e 6% no Cenário 03. Comparando o uso do protocolo WPA/TKIP em relação com a implementação sem segurança, pode-se constatar que no Cenário 01 há variação de 3%, para o Cenário 02 ocorre variação de 7% e no Cenário 03 a variação e de 9%.

A maior degradação de performance está apresentada na Tabela 12, na qual verifica-se que o protocolo WEP degrada a performance em relação ao equipamento configurado sem segurança em 3% no Cenário 01, 4% no Cenário 02 e 6% no Cenário 03. O protocolo WPA/TKIP degrada a performance em relação ao WEP em 5% no Cenário 01, 8% no Cenário 02 e 10% no Cenário 03. Comparando o uso do protocolo WPA/TKIP em relação com a implementação sem segurança, pode-se constatar que no Cenário 01 há variação de 8%, para o Cenário 02 existe variação de 12% e no Cenário 03 a variação percebida é de 16%.

A Tabela 11 ilustra a degradação de desempenho quando os pacotes variam de 64 a 1460 bytes. O protocolo WEP degrada o desempenho em relação ao equipamento parametrizado sem segurança em 2% no Cenário 01, 3% no Cenário 02 e 4% no Cenário 03.O protocolo WPA/TKIP degrada o desempenho em relação ao WEP em 3% no Cenário 01, 6% no Cenário 02 e 8% no Cenário 03. Comparando o uso do protocolo WPA/TKIP em relação com a implementação sem segurança, pode-se constatar que no Cenário 01 houve variação de 5%, para o Cenário 02 a variação foi de 9% e no Cenário 03 a variação constatada foi de 12%. Experimento semelhante ao especificado na Tabela 11, feito por Barka e Boulmalf (2007), em que concluíram que a sobrecarga do protocolo WPA em relação a redes sem segurança é de 13 %, sendo que eles mantiveram as distâncias entre os equipamentos em 5 metros e os equipamentos não estavam conectados por meio de cabo e sim em ambiente aberto.

6 CONCLUSÃO

Neste trabalho foi estudado o impacto que ocorre na performance de uma rede WLAN com a implementação dos protocolos de segurança WEP e WPA/TKIP em três cenários distintos e variando o tamanho do pacotes. Os estudos iniciais mostram que esses protocolos incluem informações nos cabeçalhos dos pacotes de dados e com isso há o aumento do processamento devido ao processo de criptografia dos dados. Assim verificou-se através dos resultados do experimento que a degradação do desempenho é maior quando o tamanho dos pacotes é menor.

É possível observar o impacto da atenuação do meio no desempenho da rede, refletindo também na implementação dos níveis de segurança. Ou seja, quanto mais distante se posicionaram os equipamentos maior foi a degradação do desempenho com a implementação dos protocolos de segurança, conforme observados nas Tabelas 11, 12 e 13.

A análise dos resultados nos leva a acreditar que o processo de criptografia do WPA/TKIP é bem mais robusto que o WEP, portanto logicamente provê mais segurança. Contudo decorrente disto, o mesmo consome mais recursos da WLAN.

O protocolo WEP utiliza um vetor de inicialização de 3 *bytes* e a chave de autenticação de 13 bytes e no protocolo WPA/TKIP o vetor de inicialização tem 6 *bytes* e a chave de autenticação possui 64 bytes. Quanto aos processos e algoritmos para gerar a nova chave que será a entrada para o algoritmo de criptografia PRNG/RC4, o WEP passa por uma única fase enquanto o WPA/TKIP utiliza duas fases. O protocolo WPA/TKIP inclui o algoritmo de criação do campo MIC, o qual será utilizado no processo de decifragem, enquanto o WEP não possui a técnica de geração e verificação do MIC. Em relação à adição de informação no cabeçalho do frame, o protocolo WEP adiciona 8 *bytes* e o WPA/TKIP inclui 20 *bytes*. Dessa maneira, constatou-se, em todos os cenários

estudados, que o WPA/TKIP consome mais recursos em relação ao WEP e esse por sua vez consome mais que uma WLAN sem segurança. Portanto, à medida que aumenta o nível de segurança decresce a taxa de transmissão da rede sem fio.

Sendo esse campo de alto interesse para as empresas, visto a grande utilização dessa solução atualmente, consideramos como trabalhos futuros, repetir o experimento com a implementação da técnica de segurança AES(*Advanced Encryption Standard*) e RADIUS(*Remote Authentication Dial In User Service*).

Também outro ponto importante neste contexto seria analisar o impacto do MIC no desempenho quando ocorre atenuação na rede ocasionando maior perda de pacotes.

7 REFERÊNCIAS

BARKA, Ezedin; BOULMALF, Mohammed. On The Impact of Security on the Performance of WLANs, *Journal of Communications*, Vol.2, N^{o}. 4, June 2007.

DUNTEMANN'S, Jeff. *Wi-FI Guide*, Arizona (EUA), Paraglyph Press, 2nd Edition, 2004.

FLUHRER, Scott; MANTIN Itsik; SHAMIR Adi. *Weaknesses in the Key Scheduling Algorithm of RC4*, 2001. FMS

GAST, Matthew S; *802.11 Wireless Networks: The Definitive Guide*, O'Reilly Publisher, 2002.

GOES, Adriano; BRANQUINHO Omar C.,; REGGIANI, Norma. *Emulação de flat fading para teste de redes WLAN em 2,4 GHz.* Disponível na intranet via URL: http://goes.adriano.googlepages.com/MOMAG2006-FLATFADINGV6.PDF.
Arquivo capturado em 29/03/2008.

IEEE802.11. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,* ANSI/IEEE Std 802.11, Information technology , 1999 Edition.

IEEE802.11a. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band*, ANSI/IEEE Std 802.11, Information technology, 1999.

IEEE802.11b. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band,* ANSI/IEEE Std 802.11, Information technology, 1999.

IEEE802.11g. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band*, ANSI/IEEE Std 802.11, Information technology, 2003.

IEEE802.11i. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 6: Medium Access Control (MAC) Security Enhancements,* ANSI/IEEE Std 802.11, Information technology, 2004.

KARKOTLI , Gilson Rihan - *Importância da Responsabilidade Social Para Implementação do Marketing Social nas Organizações*, 2002. Disponível na Internet via URL: http://teses.eps.ufsc.br/defesa/pdf/10772.pdf. Arquivo capturado em 16/09/2007.

KHAN, Jahanzeb; KHWAJA, Anis. *802.11 Building Secure Wireless Networks with 802.11*, New Jersey (EUA),Wiley Publishing, 2003.

MASICA, Ken. *Security WLANs using 802.11i Draft*, Lawrence Livermore National Laboratory, 2007.

O'HARA, Bob; PETRICK Al. *The IEEE 802.11 Handbook A Designer's Companion*, New York (EUA), IEEE Press, 1st Edition, 2001.

RAJESH, Gandhi; R. Gandhi. *Empirical Path Loss Models for 802.11b Links. Master's thesis*, Indian Institute of Technology, Kanpur, 2003.

RAPPAPORT, Theodore S. *Wireless Communications Principles and Practice*, New Jersey (EUA), Prentice Hall PTR, Second Edition, 2002.

BARRADAS, O.; RIBEIRO, MARCELLO P. *Telecomunicações - Sistemas Analógicos Digitais*, Rio de Janeiro, Livros Técnicos e Científicos Editora S.A, 1980.

ROSHAN, Pejman; LEARY Jonathan. *802.11 Wireless LAN Fundamentals*, Cisco Press, 2003.

RUFINO, Nelson Murilo de O. *Segurança em Redes Sem Fio Aprenda a Poroteger Suas Informações em Ambientes Wi-Fi e Bluetooth*, São Paulo, Novatec Editora, 2ª Edição, 2005.

SCHNEIER Bruce. *Applied Cryptography, Protocols, Algorthms, and Source Code in C (cloth)*, New Jersey (EUA), Wiley Publishing, 1996.

STALLINGS William. *Data and Computer Communications Computer Networking*, New Jersey (EUA), Pearson Education, 7th Edition, 2003.

SOARES, Luiz F. Gomes; LEMOS Guido; COLCHER Sérgio. *Redes de Computadores Das LANs MANs e WANs às Redes ATM, Curso Completo*, Rio de Janeiro, Editora Campus, 3ª Edição, 2000.

TANENBAUM, Andrew S. *Redes de Computadores*, Rio de Janeiro, Editora Campus, 3ª Edição, 2003.

TORRES, Gabriel. *Redes de Computadores Curso Completo*, Rio de Janeiro, Axcel Books do Brasil Editora, 1ª Edição, 2001.

WI-FI ALLIANCE. *WI-FI Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks*, 2003.

WALKER Jesse. *IEEE 802.11i Standard Improves Wireless LAN Security*, Communications Technology Lab Intel Corpotation, 2005.

WP802.11g. *Broadcom Corporation. "The New Mainstream Wireless LAN Standard" White Paper 802.11g*, 2003. Disponível na Internet via URL:

http://www.dell.com/downloads/global/shared/broadcom_802_11_g.pdf. Arquivo capturado em 16/09/2007.

ANEXOS

ANEXO A - DESCRIÇÃO DO FUNCIONAMENTO DA BANCADA EDIFICADA NO LABORATÓRIO DE PESQUISA DE SISTEMA DE RADIO (LP-SiRa) DA PUC CAMPINAS

Este documento foi elaborado pelos alunos da Engenharia Elétrica da PUC Campinas : Eduardo Coco e Karyna Silveira Cardoso e seu objetivo é descrever o funcionamento da bancada de emulação de sinais de rádio freqüência, na qual a atenuação é feita através de um atenuador variável e duas chaves de RF. É apresentado o funcionamento da bancada, e todos os componentes são caracterizados com maiores detalhes.

A bancada tem como objetivo emular um ambiente de rede sem fio, utilizando um atenuador variável e duas chaves de RF. Isto possibilita fazer testes de serviços e aplicativos rodando em uma rede sem fio, porém em um ambiente cabeado com comportamento estável e controlado.

1 DESCRIÇÃO DA BANCADA

Os equipamentos estão organizados dentro de um *rack*, para evitar modificações na configuração, e assim alterar o mínimo possível nos resultados dos testes.

Dentro de uma caixa blindada tem-se um *acess point* (AP), na qual entram três cabos.

Um está ligado em uma fonte de tensão de 110V, o outro é o cabo de rede que vai para o *hub* e o último está conectado ao circuito atenuador.

O circuito atenuador é composto por duas chaves, controladas por duas fontes de tensão que variam de 0 a 5V, ligadas em série a um atenuador variável, controlado por um computador (PC1) através de um conversor digital analógico conectado na porta paralela do PC1.

Na saída do circuito atenuador encontra-se um divisor de sinal, o qual envia o sinal de rádio freqüência (RF) para um computador de medida PC2, o qual recebe o sinal através de uma placa.

Podemos melhor entender a bancada através do diagrama em blocos na Figura 1.

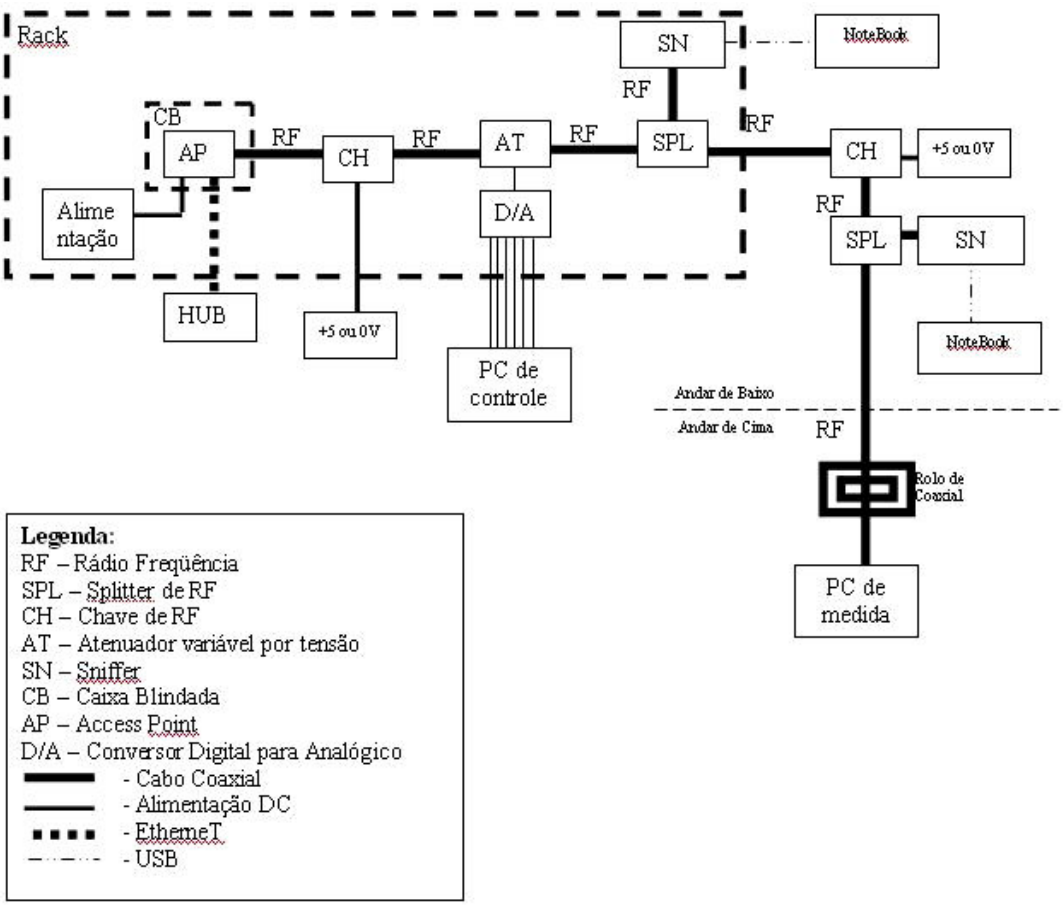


Figure 1: Diagrama em blocos da bancada de emulação.

2 COMPONENTES DA BANCADA

2.1 ATENUADOR VARIÁVEL

Este atenuador variável é caracterizado como um RVA-2500, que possui um sistema equivalente como apresentado na Figura 2, abaixo.

Possui uma fonte de alimentação de 5V constante e uma controlada com variação de 0 à 16V , sendo calibrada manualmente na fonte.

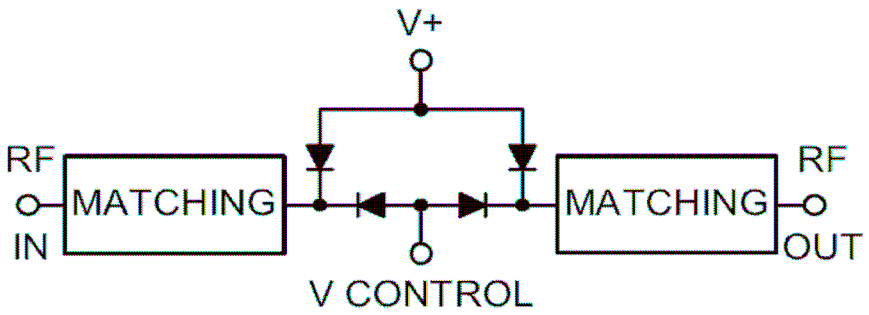


Figura 2: Circuito de atenuador variável

2.2 CHAVE DE RF

Têm-se na bancada duas chaves de RF, do mesmo modelo, mas possuem comportamento diferente. Caracteriza-se como uma chave ZMSW-1111 com freqüência de operação de 10 a 3000 MHz e impedância de 50Ω. Possui uma única fonte de alimentação na qual variamos manualmente, através de uma fonte, de 0 a 5 V. Temos melhor exemplificada a chave através do seu *datasheet* na Fig 3.

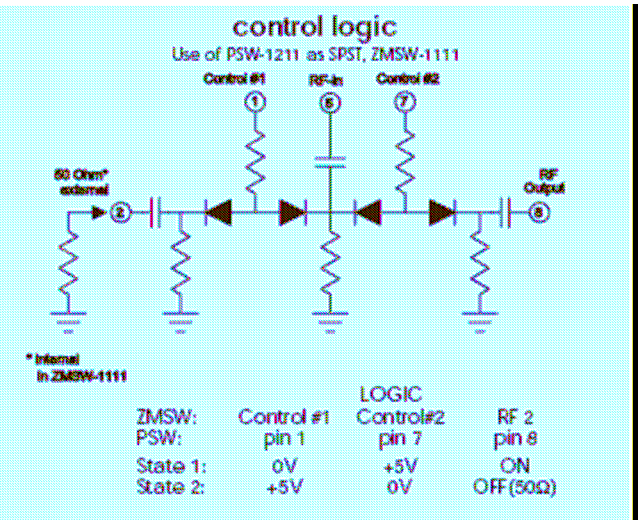


Figura 3: Circuito da chave de RF.

3 CALIBRAÇÃO

O processo de calibração consistiu em vários testes para que pudéssemos ter confiabilidade.

Primeiramente determinamos o *offset* na caixa preta em (mínimo,médio e máximo). Configuramos os valores decimais de 0 a 255 no PC1 através de um *software*, o qual emula Flat Fading em Java, lê a primeira coluna de um arquivo feito no Excel e salva como *.csv. Além de carregar o arquivo indicamos o tempo entre uma célula e outra que determinou também o intervalo de tempo para mudar o valor do decimal, que enviará um sinal para o conversor digital / analógico.

Figura 4: Software de controle da interface paralela.

Podemos ver no multímetro o valor da tensão correspondente. Esse sinal percorrerá todo o sistema (passando pelos atenuadores que controlaram o sinal) e irá chegar até o PC2 através do cabo rj 45 que está conectado a uma placa no PC2 onde poderemos ver através do software *Netstumbler* o valor da potência do sinal, relação sinal ruído.

Assim descrevemos as curvas de comportamento de sinal RF através do *NetStumbler*, para medir a intensidade final do sinal gerado pela bancada de emulação. Pois teremos mais dados do comportamento geral da bancada em relação ao atenuador variável, possibilitando uma melhor análise dos fenômenos obtidos.

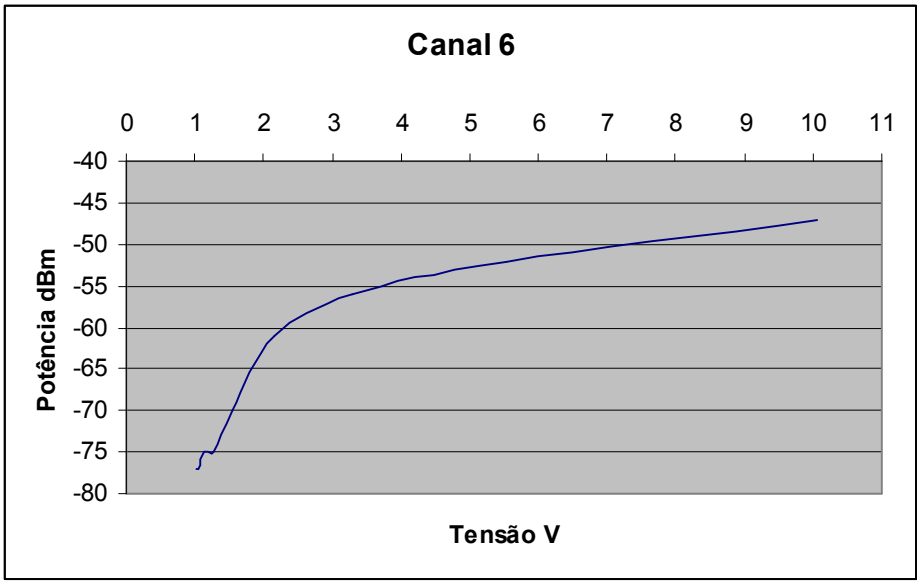


Figura 5: Curva de atenuação da bancada.

3.1 ATENUADOR VARIÁVEL

É controlado por um computador (PC1) através de um conversor digital analógico conectado na porta paralela do (PC1).

Para termos dados sobre o comportamento do atenuador variável na bancada e assim podermos comparar estes dados com o gráfico especificado pelo fabricante tivemos que realizar vários testes até que sentíssemos estabilidade e constância nestes valores.

Foi utilizado um analisador de espectro no modo *transmission measurement*, o qual está representado na Figura 4, ligamos no atenuador variável, na entrada e saída, no mesmo sentido que o sinal da bancada passa através do atenuador. Mantivemos uma fonte de alimentação de 5V constante e uma controlada com variação de 1 à 10V, devido a regulagem da bancada , sendo calibrada manualmente na fonte.

Figura 6: Analisador de Espectro

A freqüência foi variada para 2.412 GHz (canal 1), 2.437 GHz (canal 6) e para 2.462 GHz (canal 11). Percebe-se através da análise dos resultados na tabela ou mesmo através das próprias curvas dos gráficos que estão nas Figuras 8, 9 e 10 que, no canal 6 o atenuador variável apresentou maior atenuação que nos outros canais.

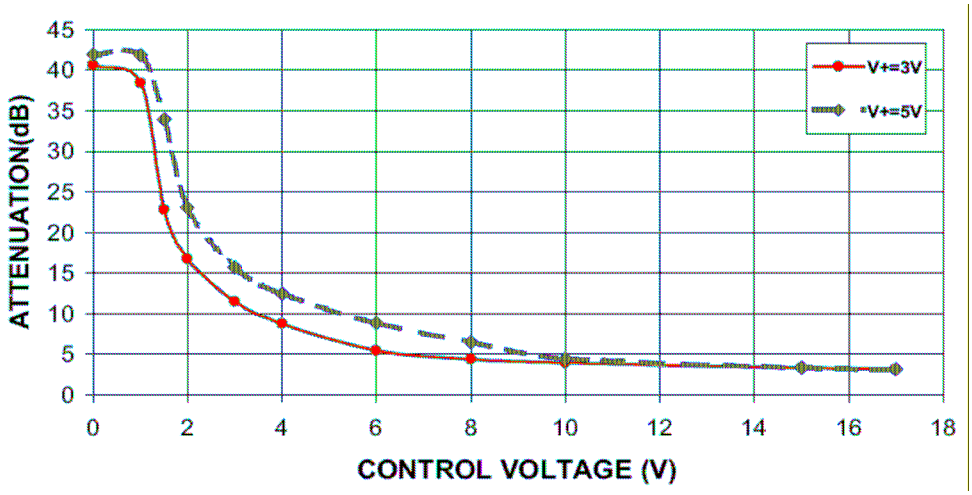


Figura 7: Resposta especificada pelo fabricante.

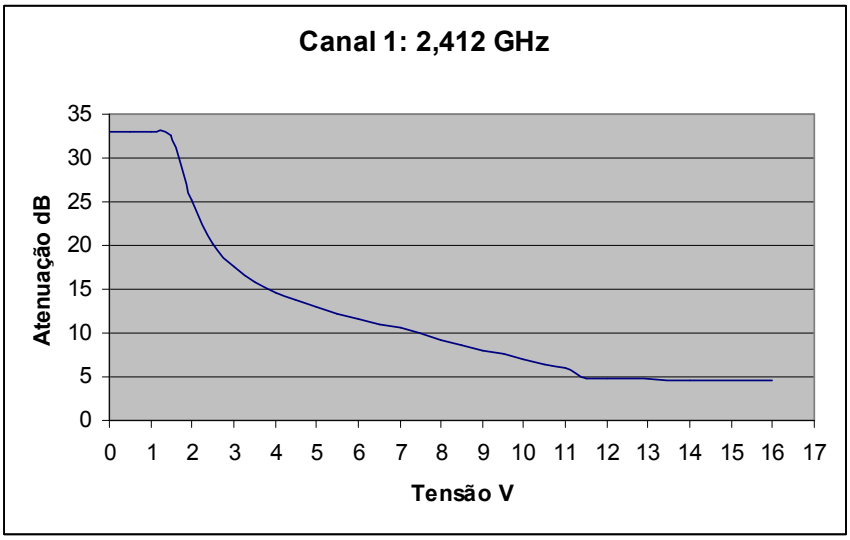


Figura 8: Curva do atenuador variável para o canal 1.

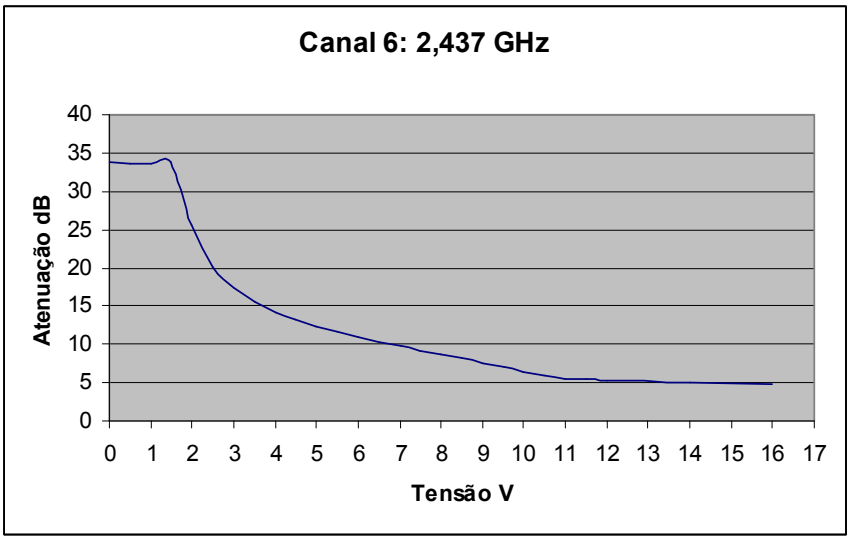


Figura 9: Curva do atenuador variável para o canal 6.

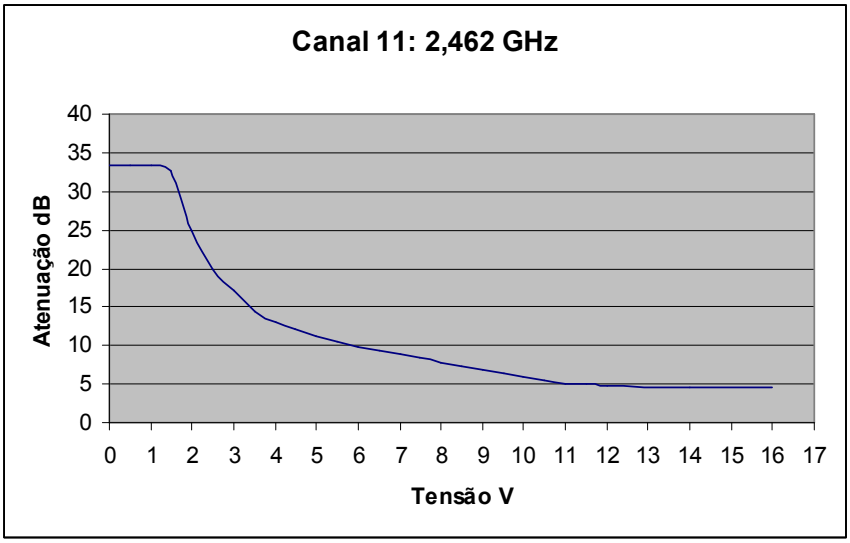


Figura 10: Curva do atenuador variável para o canal 11.

Ao analisarmos a resposta especificada pelo fabricante, como observado na Figura 7, percebe-se que os gráficos que obtivemos está bem próximo do desejado, sendo que a pequena diferença entre eles , deve-se ao fato de o fabricante ter considerado a freqüência de 1 GHz, enquanto nossos testes foram para freqüência de 2.412 à 2.462 GHz. Este fato pode justificar a pequena discrepância entre os gráficos obtidos e o especificado pelo fabricante.

3.2 CHAVE DE RF

Para obtermos dados sobre o comportamento das chaves de RF, testamos cada uma delas, separadamente. Liga-se o analisador de espectro no modo *transmission measurement* na chave, o qual é variado o valor da freqüência de 2,412 a 2,462 GHz, ou seja, para os canais 1, 6 e 11, e também uma fonte de tensão a qual varia-se manualmente de 0 à 5 V.

Logo para a chave 1 obteve-se os valores conforme os gráficos nas Figuras 11,12 e 13.

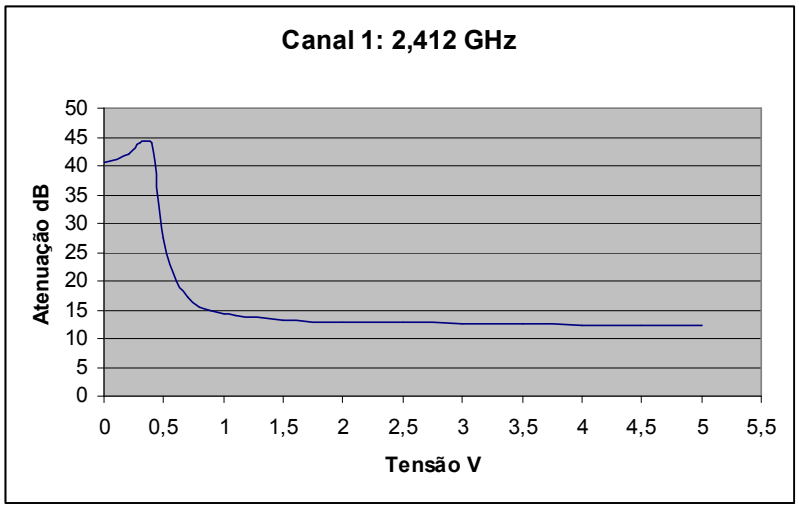


Figura 11: Atenuação da chave 1 no canal 1.

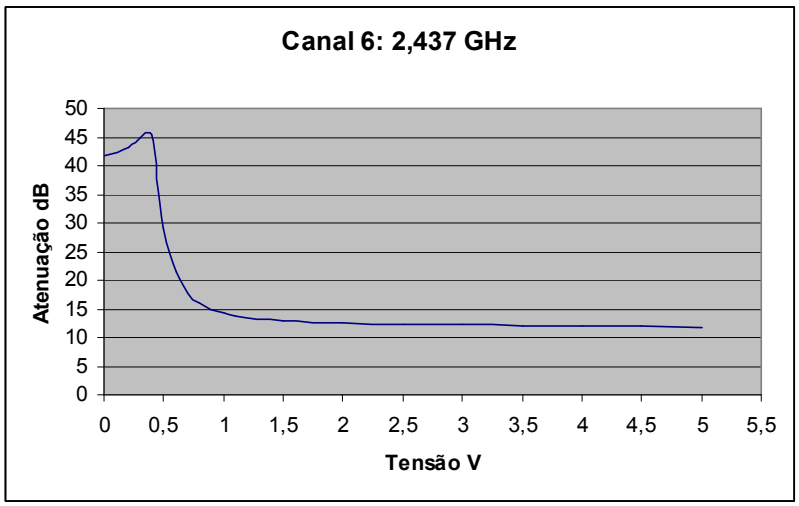


Figura 12: Atenuação da chave 1 no canal 6.

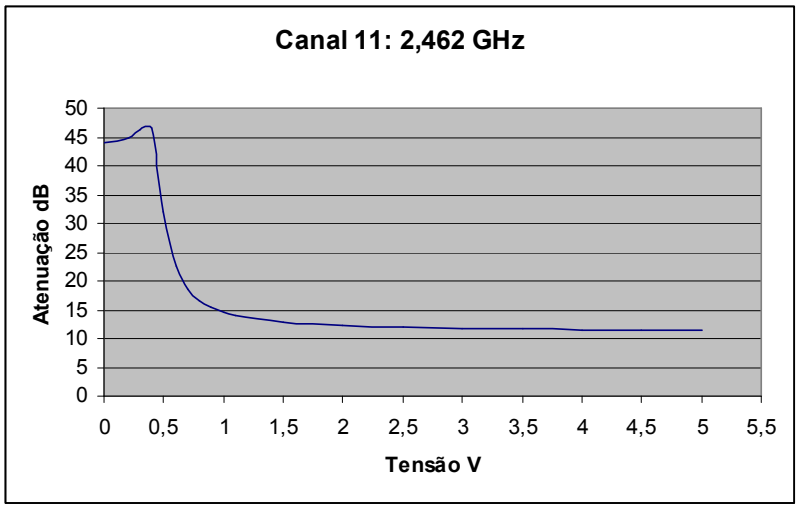


Figura 13: Atenuação da chave 1 no canal 11.

Para a chave 2 obteve-se os gráficos conforme mostrados nas Figuras 14,15 e 16.

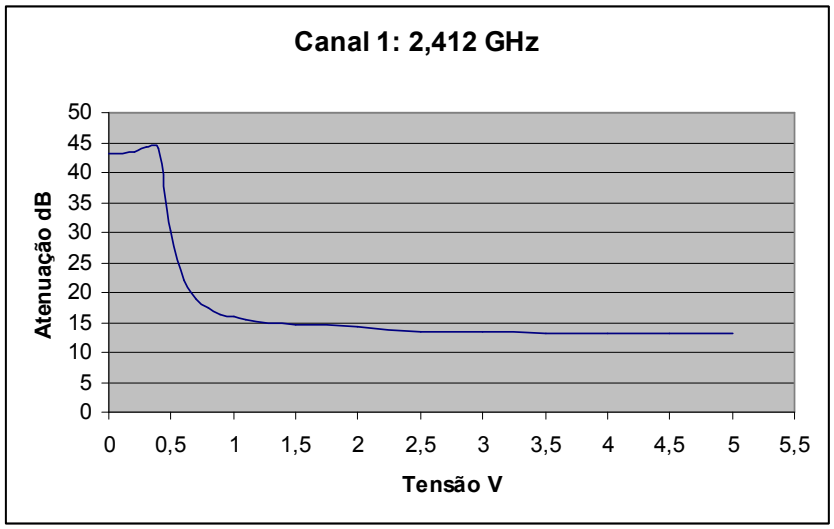


Figura 14: Atenuação da chave 2 no canal 1.

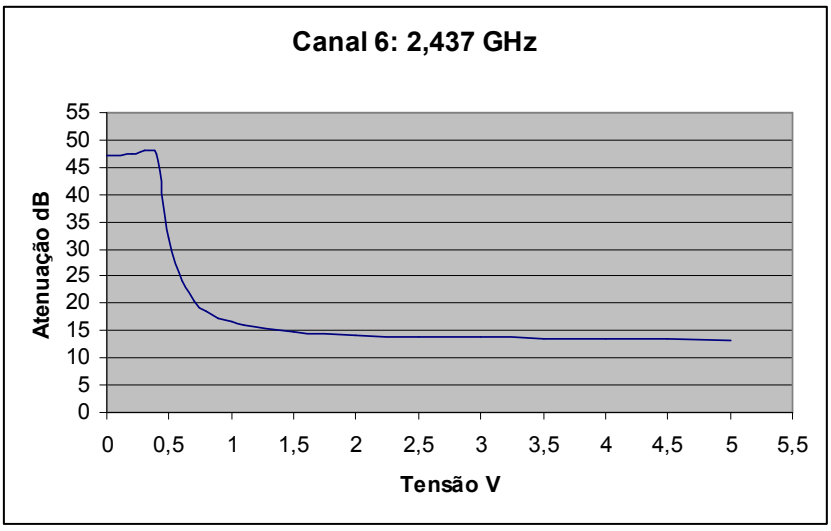


Figura 15: Atenuação da chave 2 no canal 6.

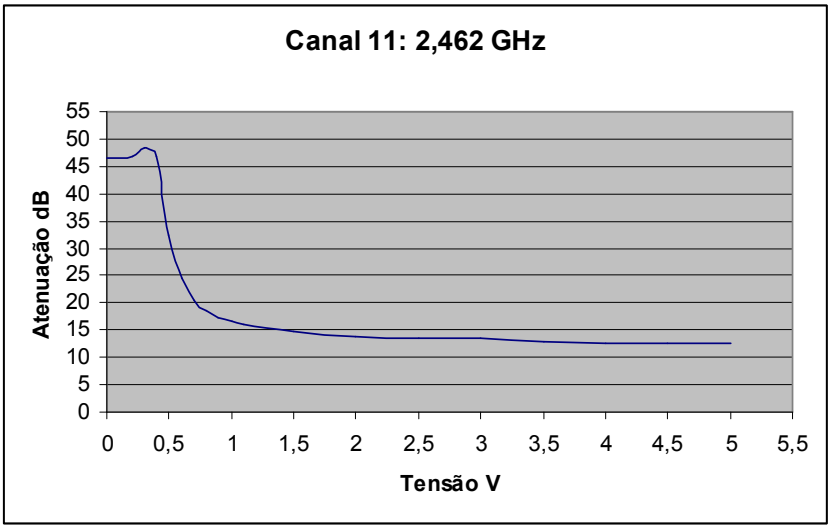


Figura 16: Atenuação da chave 2 no canal 11.

Através dos dados coletados verifica-se que a sensibilidade da chave é considerável quando a tensão varia de 0 a 1 V, sendo que para os valores de 1 a 5V apresenta-se uma atenuação praticamente constante, mas relevante em torno de 10 dB.

4 CONCLUSÃO QUANTO AO FUNCIONAMENTO DA BANCADA

Analisando o comportamento da bancada, percebe-se que ela consegue emular o ambiente *wireless* de uma forma estável, podendo assim proporcionar testes que provem serviços e aplicativos. Alcançando assim o seu objetivo.

ANEXO B - CONFIGURAÇÃO DE SEGURANÇA NO AP E NA STA 01

Os equipamentos de segurança foram configurados com os protocolos de segurança conforme apresentados nas figuras abaixo.

1 CONFIGURAÇÃO SEM SEGURANÇA

Configuração dos equipamentos AP e a STA 01 sem os protocolos de segurança.

Figura 01 - Configuração do AP sem segurança

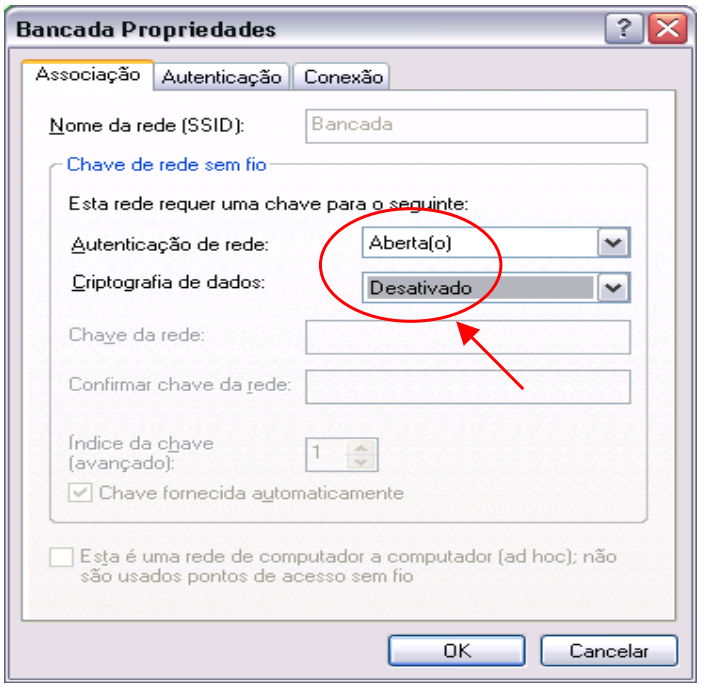


Figura 02 - Configuração da STA 01 sem segurança

2 CONFIGURAÇÃO WEP

Nesse experimento os equipamentos estão configurados com o protocolo WEP 16 *bytes*, sendo informado chave de 26 caracteres hexadecimais ou 13 *bytes*.

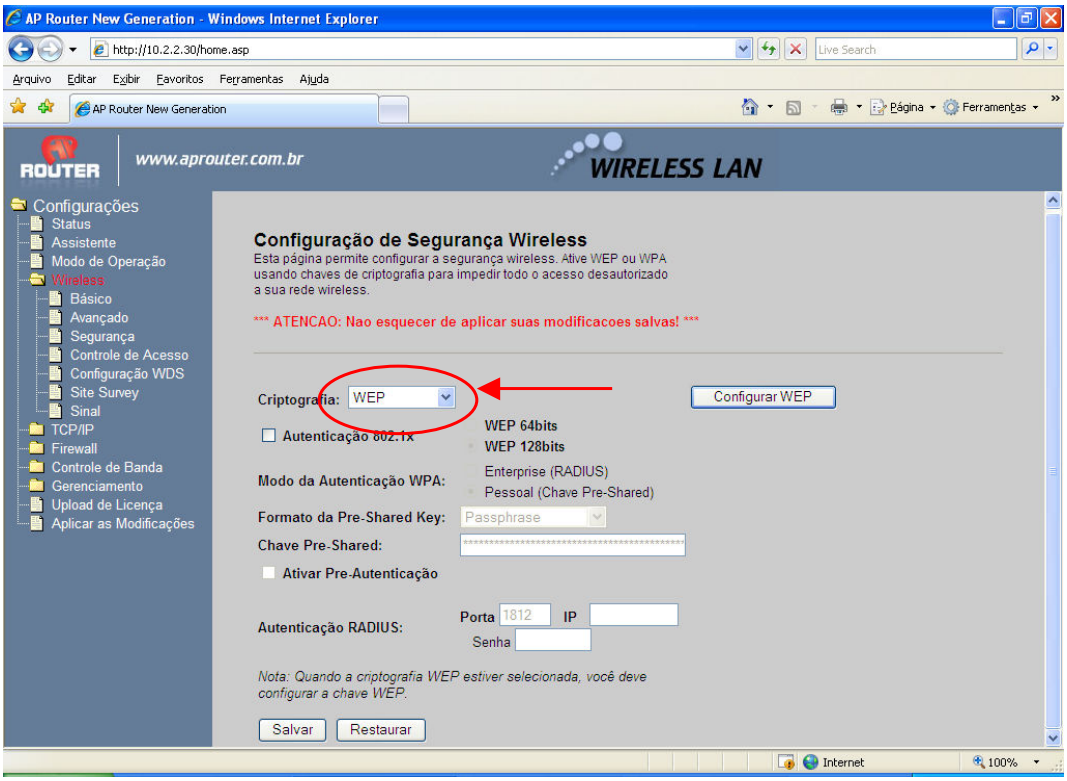


Figura 03 - Configuração do AP com protocolo WEP habilitado

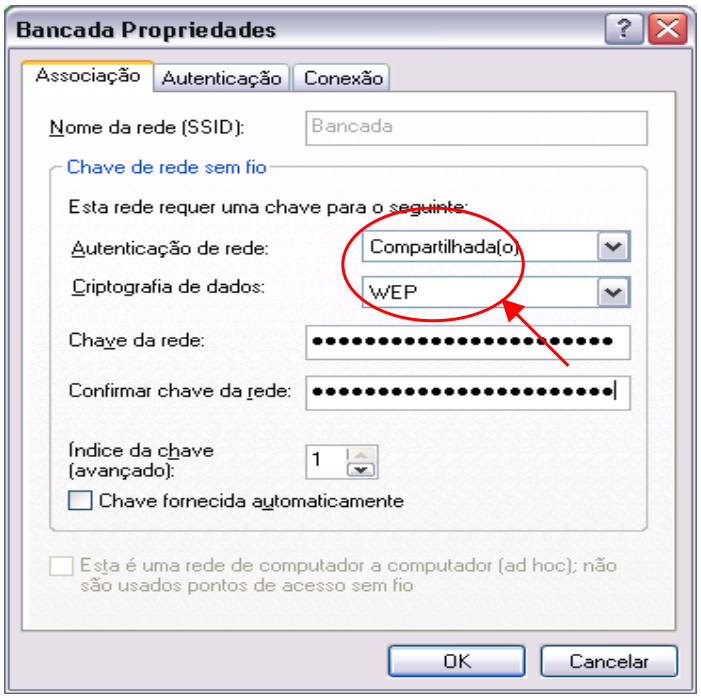


Figura 04 - Configuração da STA 01 com WEP habilitado

3 CONFIGURAÇÃO WPA/TKIP

Os equipamentos foram configurados com o protocolo WPA/TKIP, sendo configurada chave de 64 caracteres hexadecimais ou 32 *bytes*.

Figura 05 - Configuração do AP com protocolo WPA/TKIP habilitado

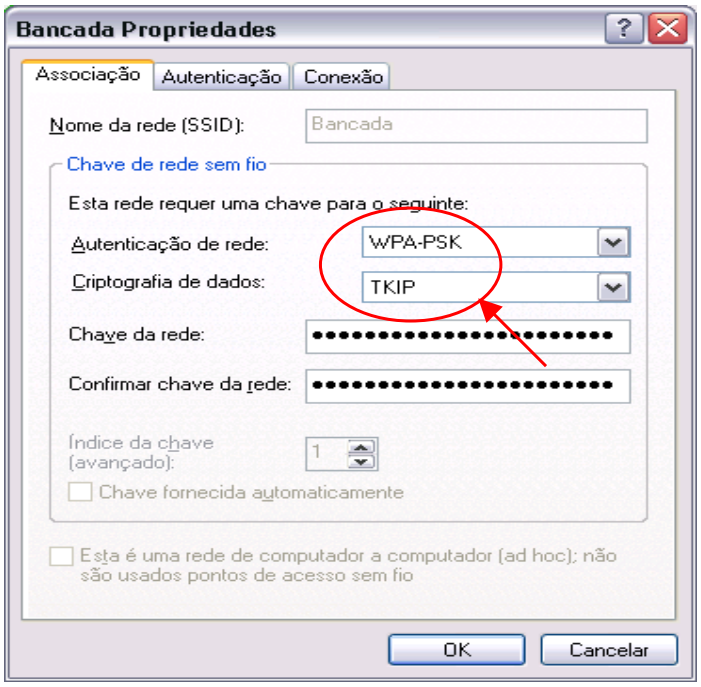


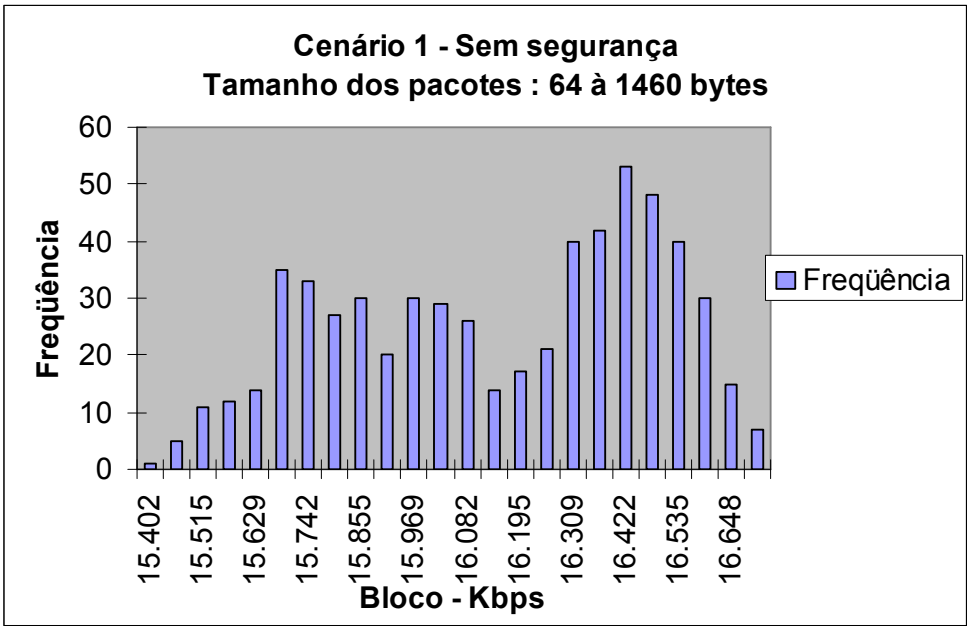
Figura 06 - Configuração da STA 01 com WPA/TKIP habilitado

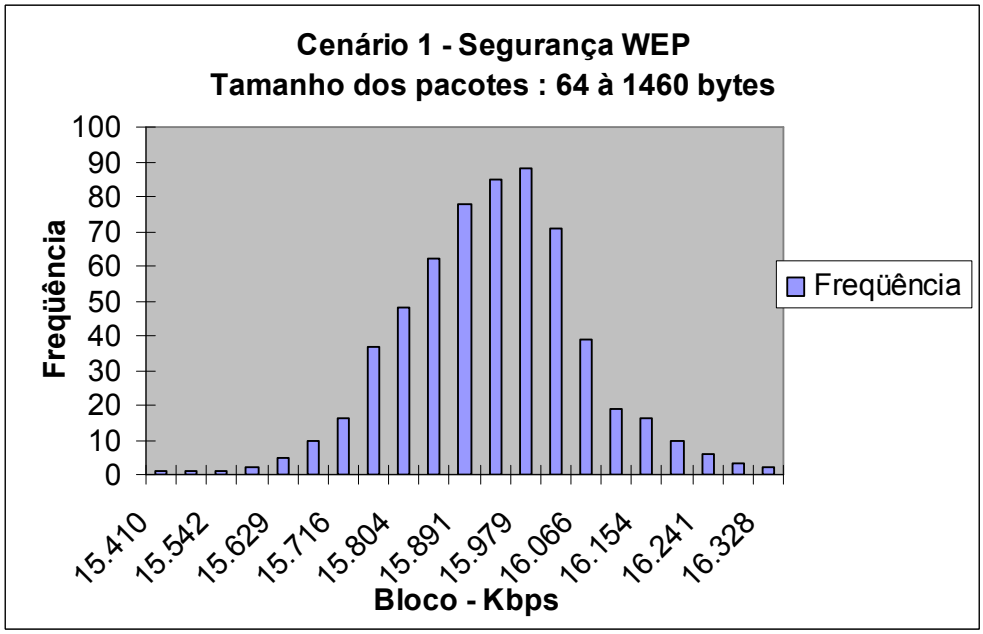
ANEXO C - HISTOGRAMA DAS MEDIDAS

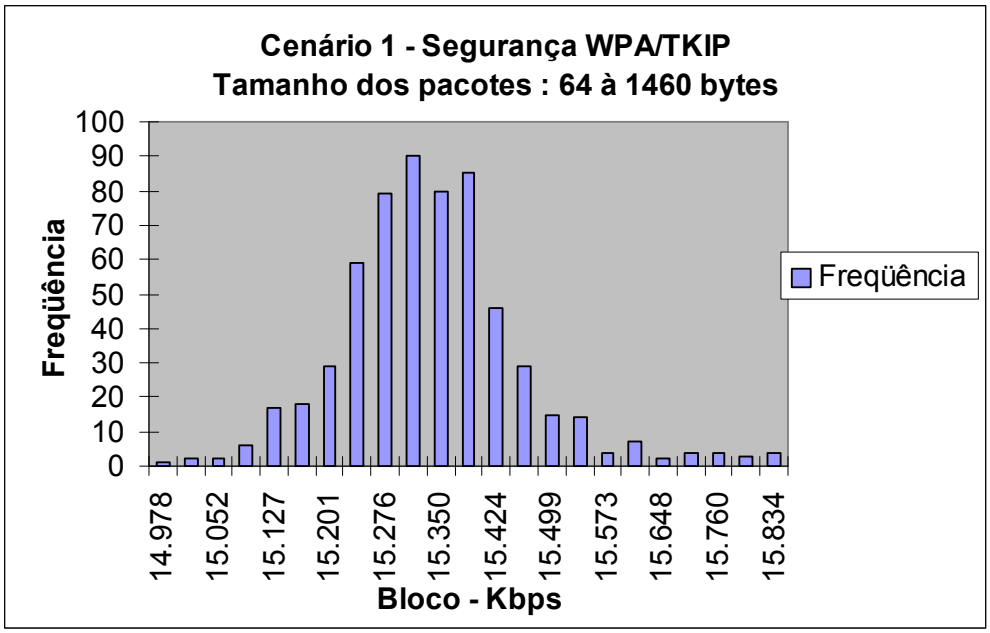
Abaixo estão apresentados os histogramas referente às medidas contidas nas Tabelas 4, 5 e 6.

1 HISTOGRAMAS REFERENTES ÀS MEDIDAS DA TABELA 7

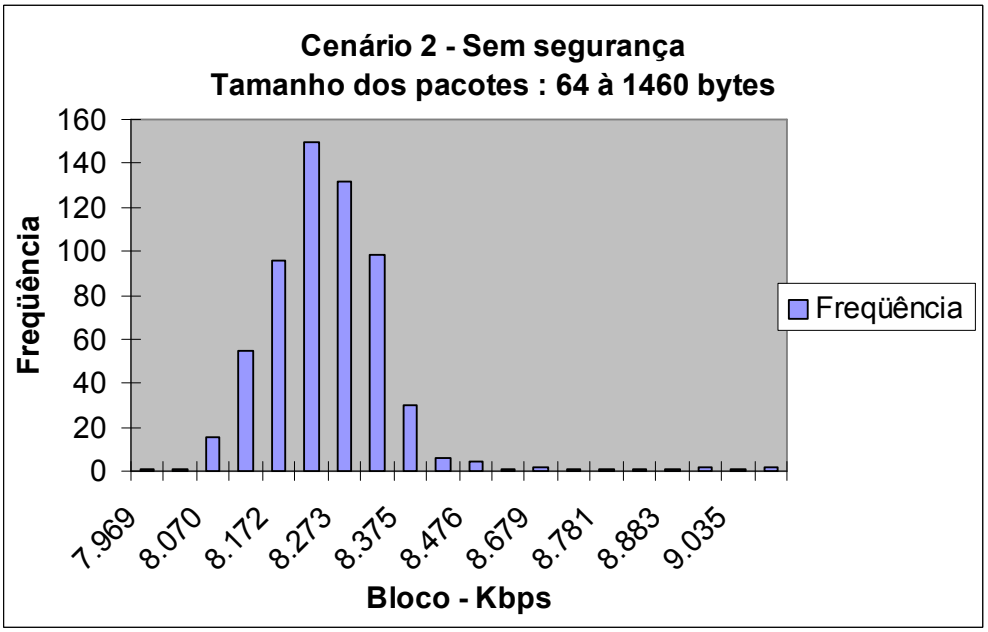
1.1 Cenário 1

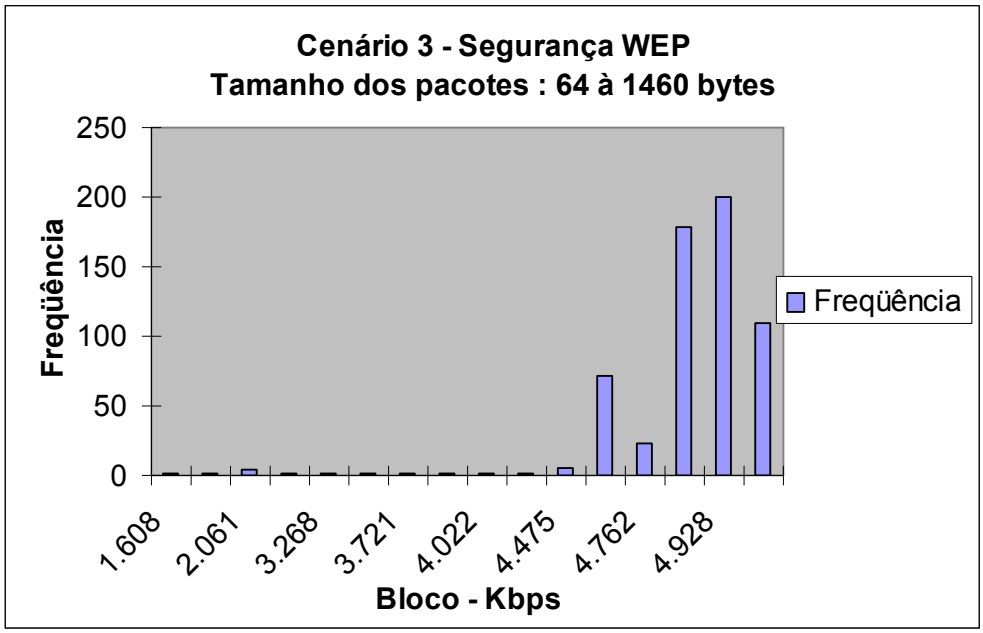


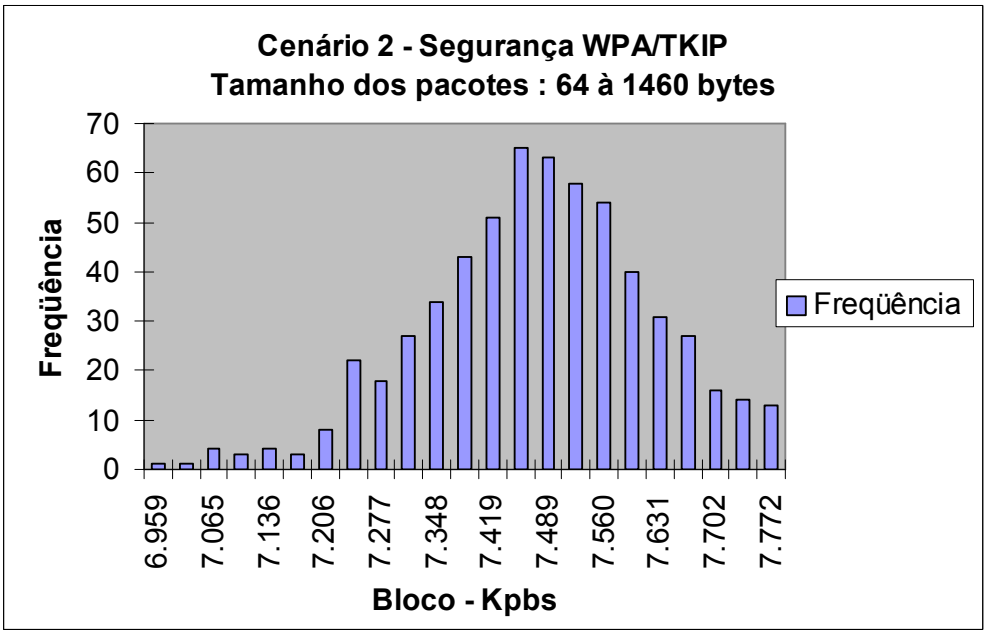



Cenário 1 - Segurança WPA/TKIP
Tamanho dos pacotes : 64 à 1460 bytes
Freqüência
100
90
80
70
60
50
40
30
20
10
0
14.978
15.052
15.127
15.201
15.276
15.350
15.424
15.499
15.573
15.648
15.760
15.834
Bloco - Kbps
Freqüência

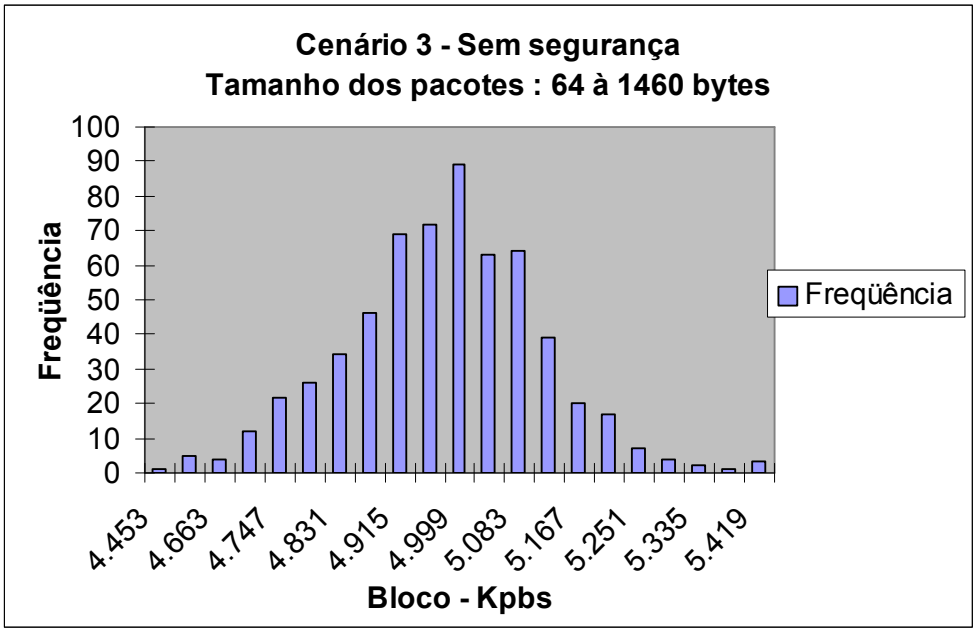
1.2 Cenário 2

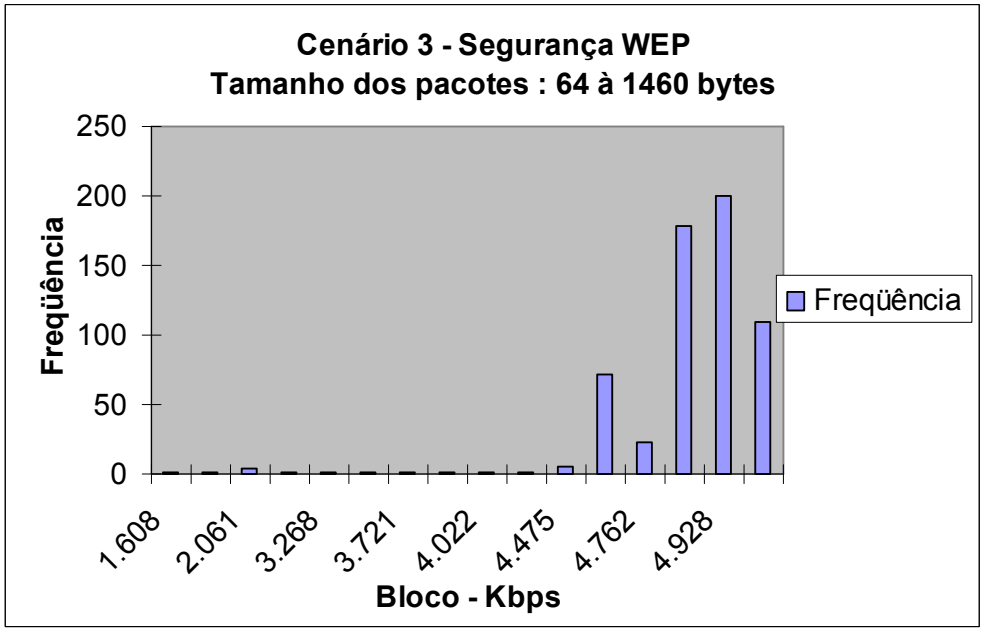

Cenário 2 - Sem segurança
Tamanho dos pacotes : 64 à 1460 bytes
Freqüência
160
140
120
100
80
60
40
20
0
7.969
8.070
8.172
8.273
8.375
8.476
8.679
8.781
8.883
9.035
Bloco - Kbps
Freqüência

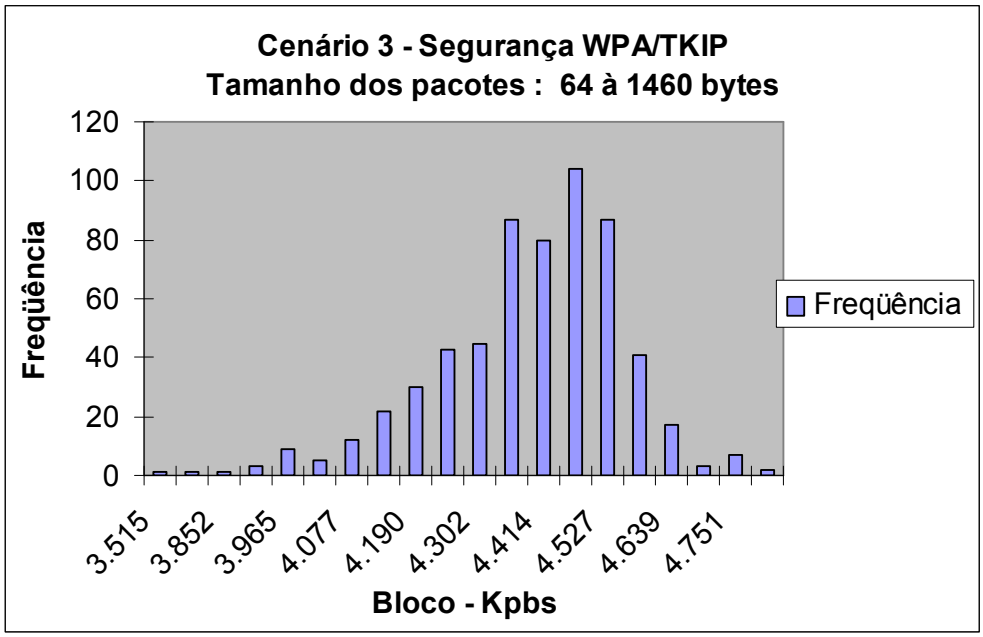

Cenário 3 - Segurança WEP
Tamanho dos pacotes : 64 à 1460 bytes
Freqüência
250
200
150
100
50
0
1.608
2.061
3.268
3.721
4.022
4.475
4.762
4.928
Bloco - Kbps
Freqüência


Cenário 2 - Segurança WPA/TKIP
Tamanho dos pacotes : 64 à 1460 bytes
Freqüência
70
60
50
40
30
20
10
0
6.959
7.065
7.136
7.206
7.277
7.348
7.419
7.489
7.560
7.631
7.702
7.772
Bloco - Kpbs
Freqüência

1.3 Cenário 3

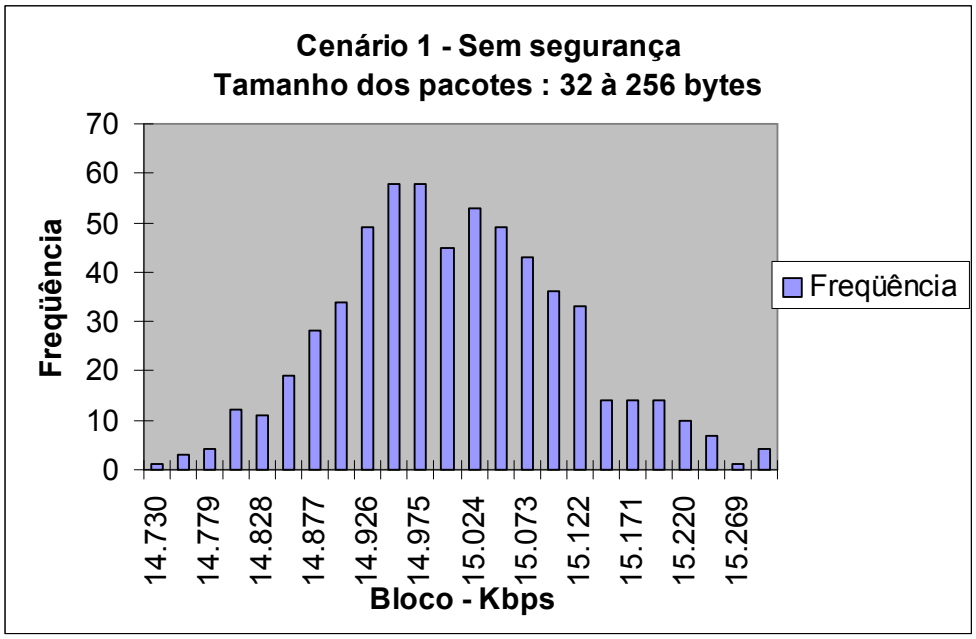

Cenário 3 - Sem segurança
Tamanho dos pacotes : 64 à 1460 bytes
Freqüência
100
90
80
70
60
50
40
30
20
10
0
4.453
4.663
4.747
4.831
4.915
4.999
5.083
5.167
5.251
5.335
5.419
Bloco - Kpbs
Freqüência

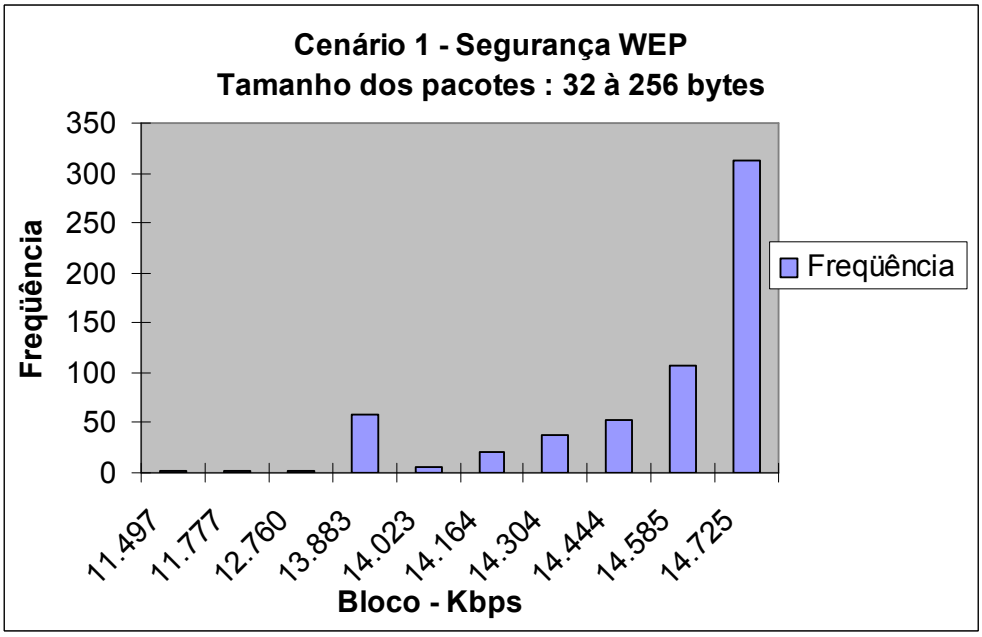

Cenário 3 - Segurança WEP
Tamanho dos pacotes : 64 à 1460 bytes
Freqüência
250
200
150
100
50
0
1.608
2.061
3.268
3.721
4.022
4.475
4.762
4.928
Bloco - Kbps
Freqüência

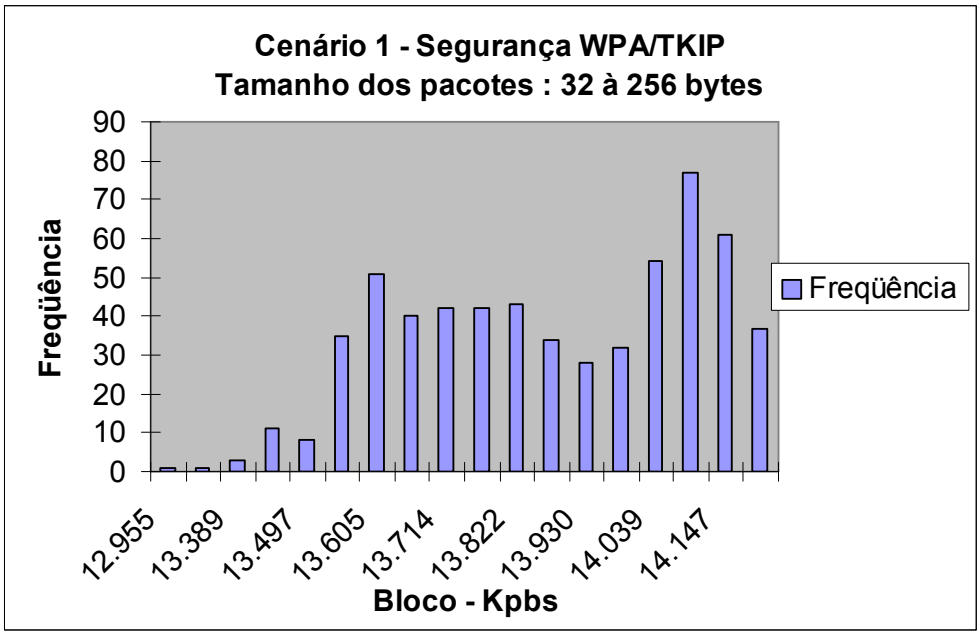

Cenário 3 - Segurança WPA/TKIP
Tamanho dos pacotes : 64 à 1460 bytes
Freqüência
120
100
80
60
40
20
0
3.515
3.852
3.965
4.077
4.190
4.302
4.414
4.527
4.639
4.751
Bloco - Kpbs
Freqüência

2 HISTOGRAMAS REFERENTES ÀS MEDIDAS DA TABELA 8

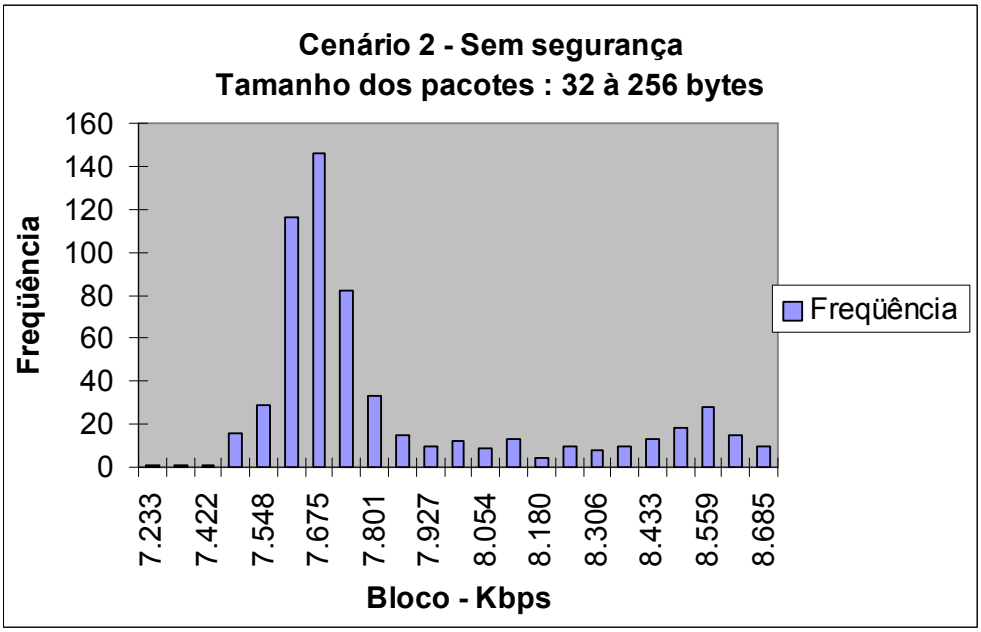
2.1 Cenário 1

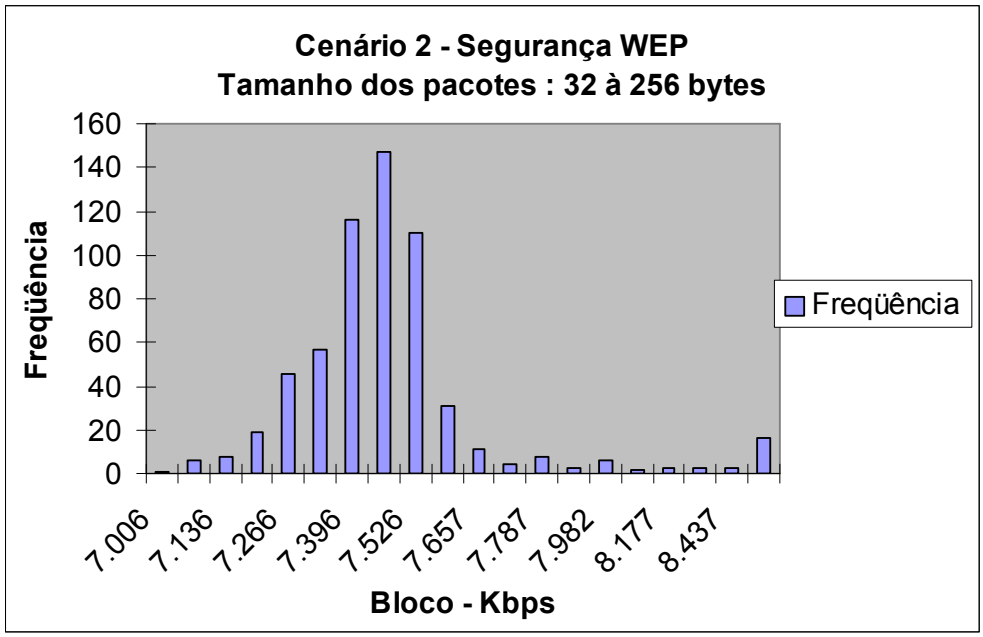


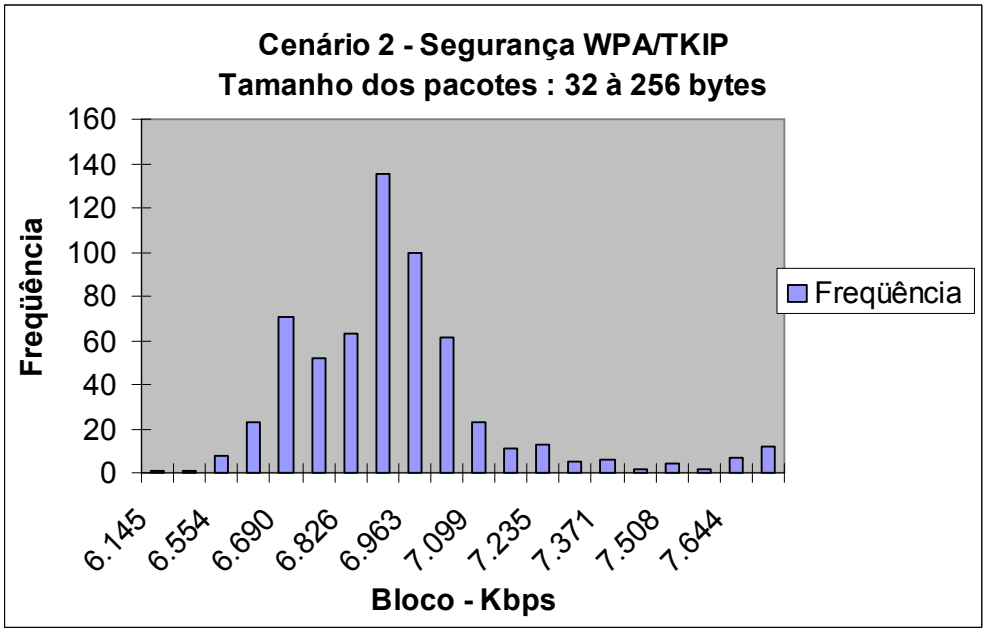



Cenário 1 - Segurança WPA/TKIP
Tamanho dos pacotes : 32 à 256 bytes
Freqüência
90
80
70
60
50
40
30
20
10
0
12.955
13.389
13.497
13.605
13.714
13.822
13.930
14.039
14.147
Bloco - Kpbs
Freqüência

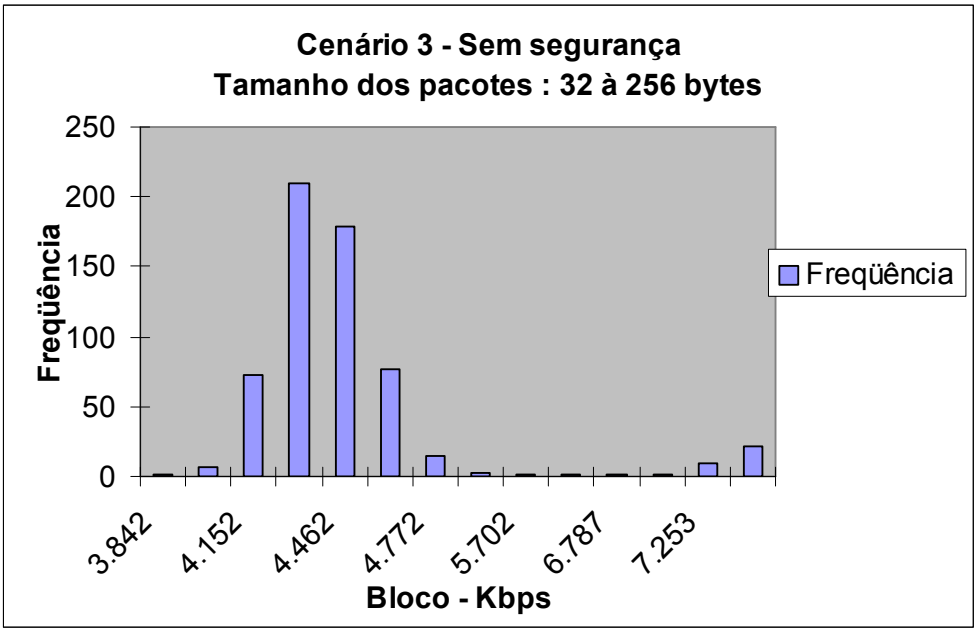
2.2 Cenário 2

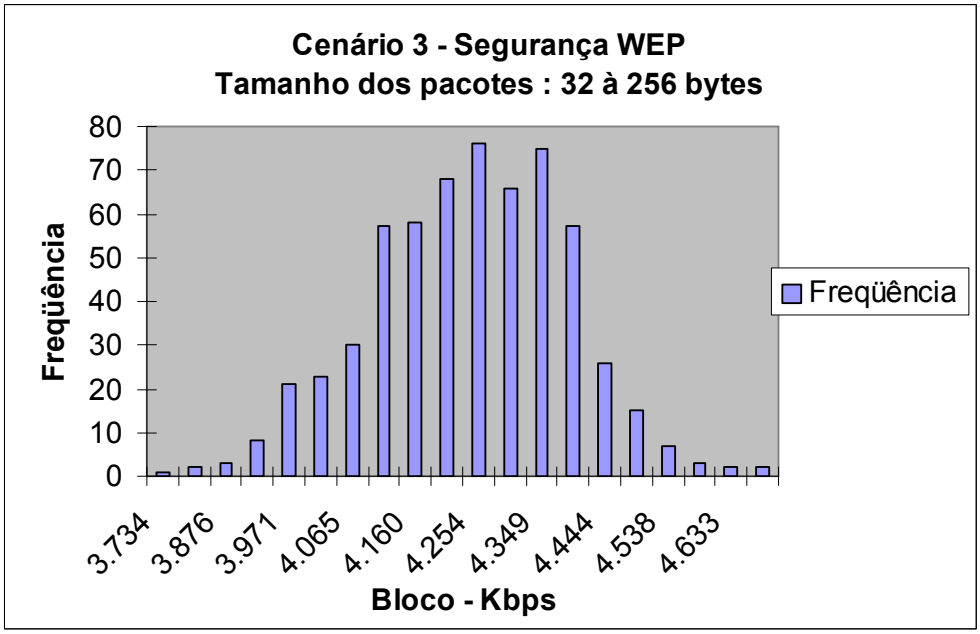

Cenário 2 - Sem segurança
Tamanho dos pacotes : 32 à 256 bytes
Freqüência
160
140
120
100
80
60
40
20
0
7.233
7.422
7.548
7.675
7.801
7.927
8.054
8.180
8.306
8.433
8.559
8.685
Bloco - Kbps
Freqüência

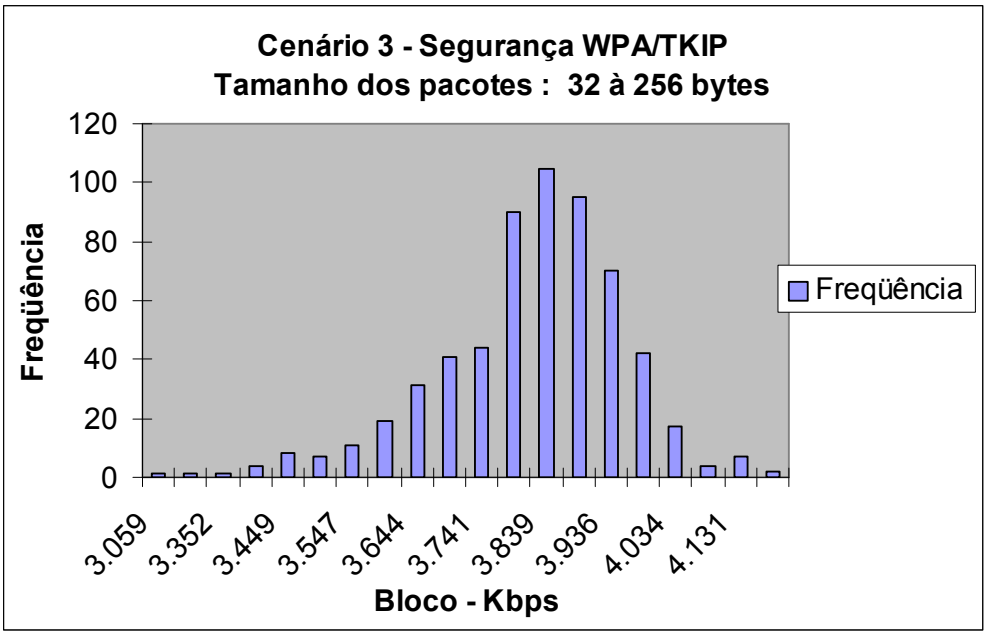

Cenário 2 - Segurança WEP
Tamanho dos pacotes : 32 à 256 bytes
Freqüência
160
140
120
100
80
60
40
20
0
7.006
7.136
7.266
7.396
7.526
7.657
7.787
7.982
8.177
8.437
Bloco - Kbps
Freqüência


Cenário 2 - Segurança WPA/TKIP
Tamanho dos pacotes : 32 à 256 bytes
Freqüência
160
140
120
100
80
60
40
20
0
6.145
6.554
6.690
6.826
6.963
7.099
7.235
7.371
7.508
7.644
Bloco - Kbps
Freqüência

2.3 Cenário 3

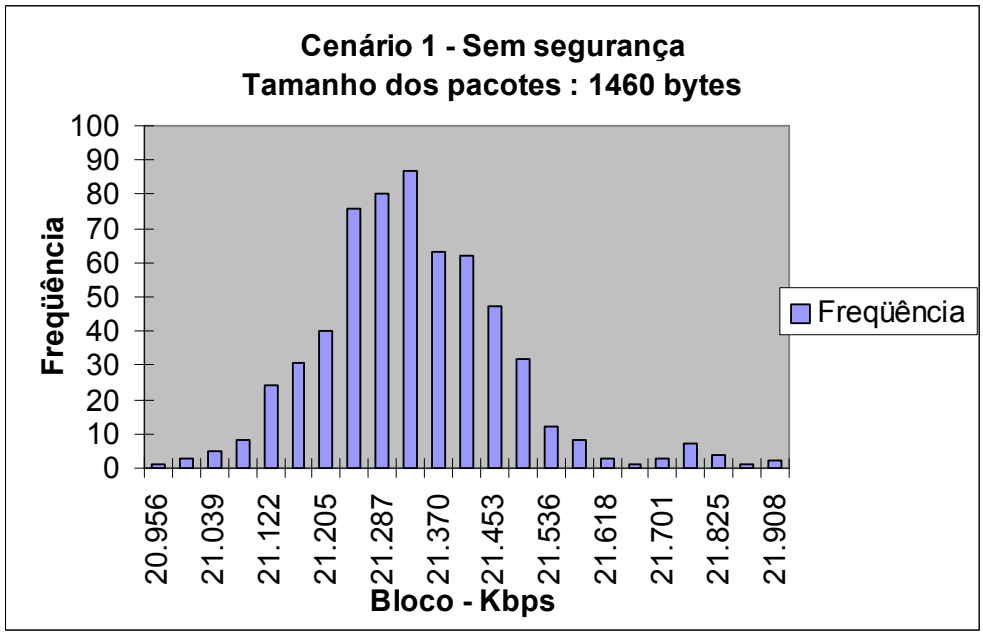

Cenário 3 - Sem segurança
Tamanho dos pacotes : 32 à 256 bytes
250
200
150
100
50
0
Freqüência
3.842
4.152
4.462
4.772
5.702
6.787
7.253
Bloco - Kbps
Freqüência

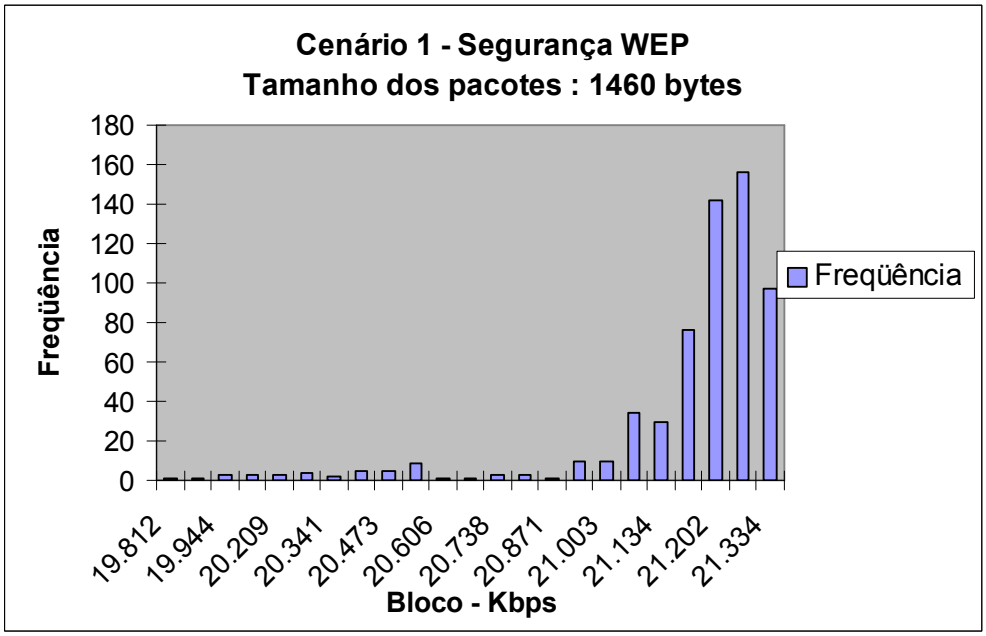

Cenário 3 - Segurança WEP
Tamanho dos pacotes : 32 à 256 bytes
80
70
60
50
40
30
20
10
0
Freqüência
3.734
3.876
3.971
4.065
4.160
4.254
4.349
4.444
4.538
4.633
Bloco - Kbps
Freqüência

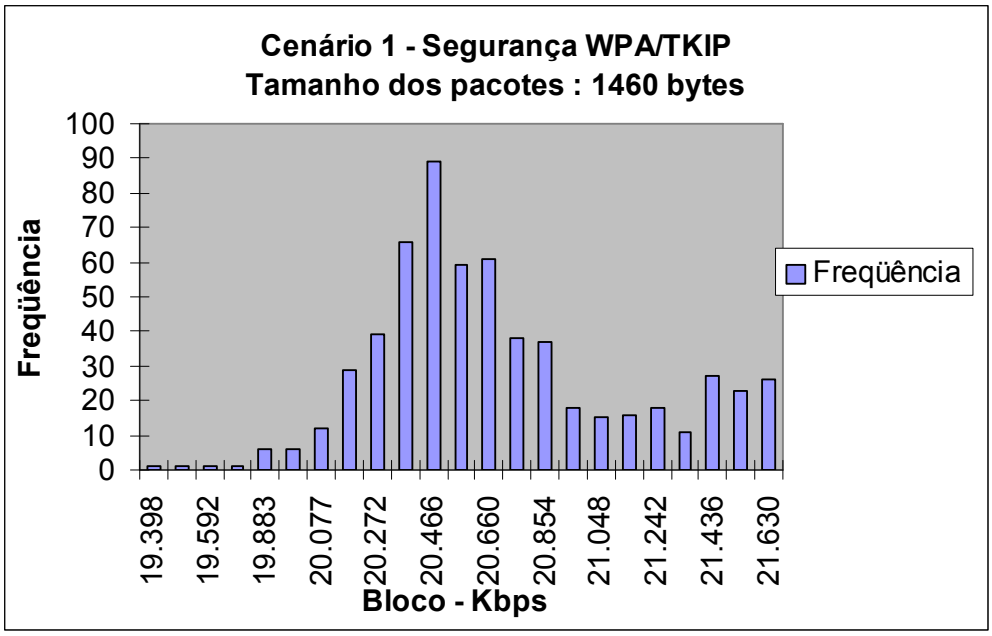

Cenário 3 - Segurança WPA/TKIP
Tamanho dos pacotes : 32 à 256 bytes
Freqüência
120
100
80
60
40
20
0
3.059
3.352
3.449
3.547
3.644
3.741
3.839
3.936
4.034
4.131
Bloco - Kbps
Freqüência

3 HISTOGRAMAS REFERENTES ÀS MEDIDAS DA TABELA 9

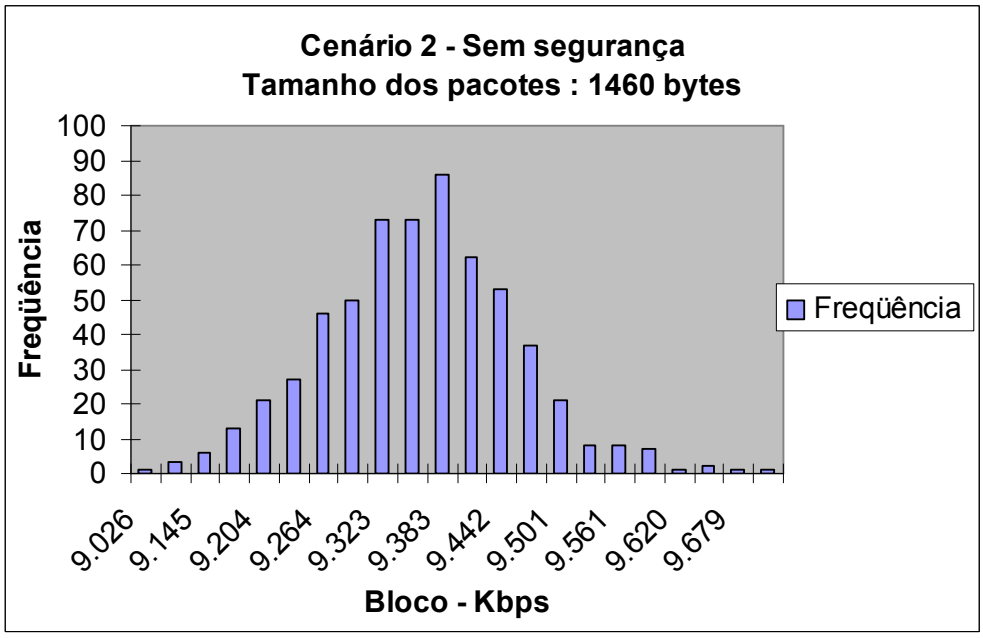
3.1 Cenário 1

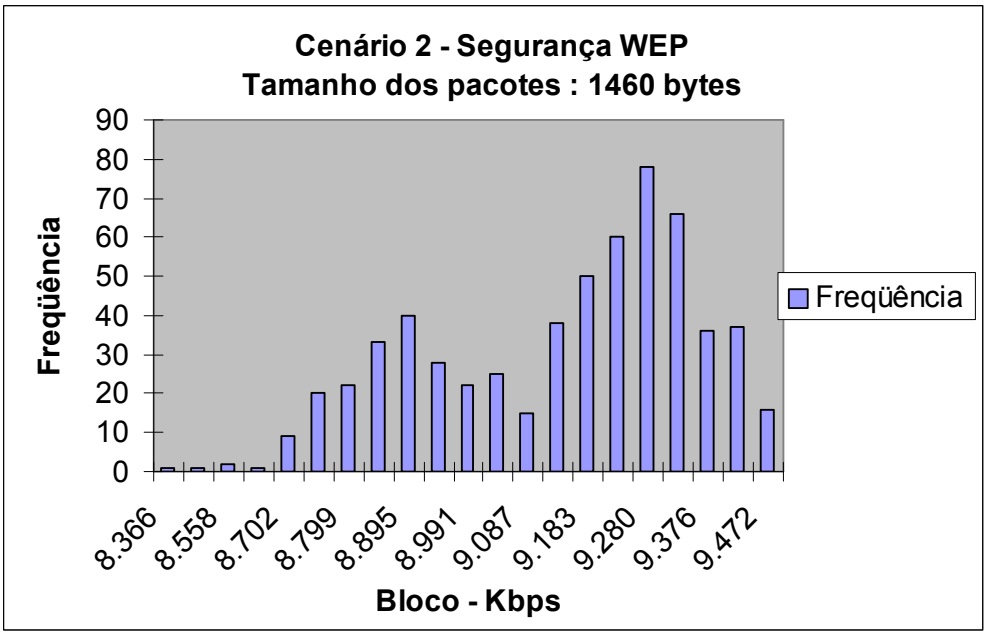


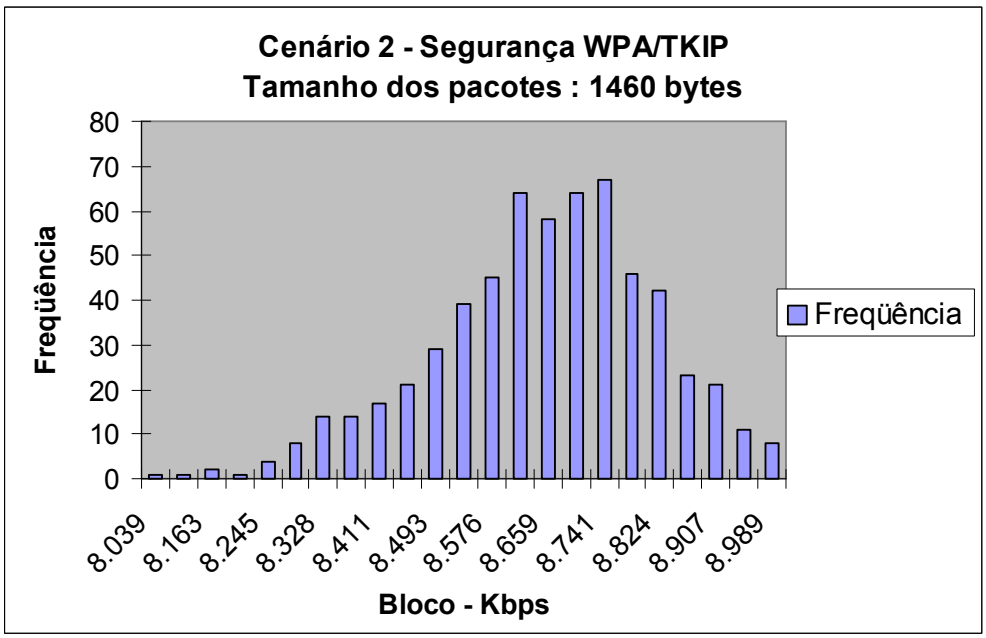



Cenário 1 - Segurança WPA/TKIP
Tamanho dos pacotes : 1460 bytes
Freqüência
100
90
80
70
60
50
40
30
20
10
0
19.398
19.592
19.883
20.077
20.272
20.466
20.660
20.854
21.048
21.242
21.436
21.630
Bloco - Kbps
Freqüência

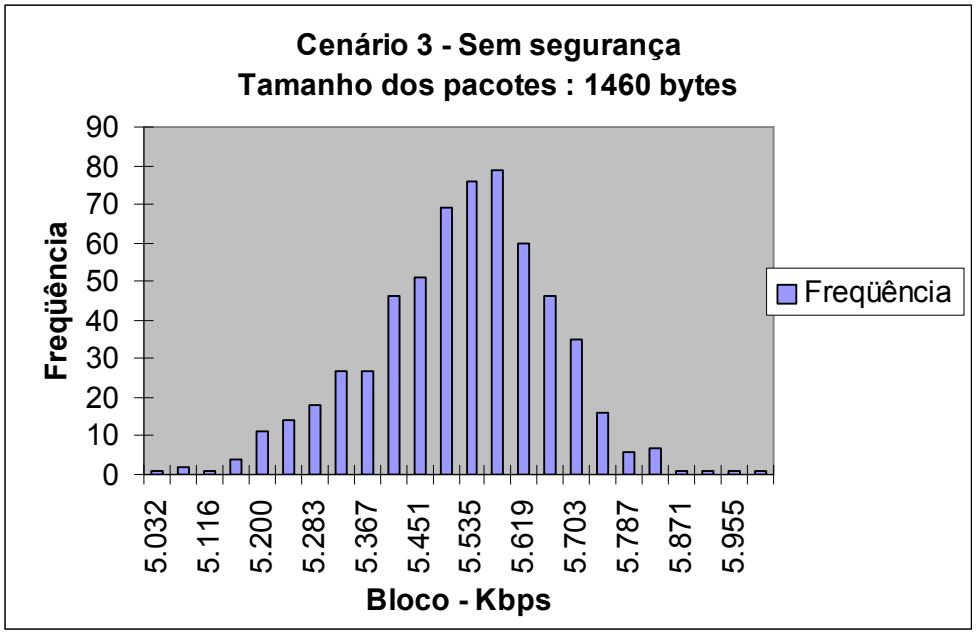
3.2 Cenário 2

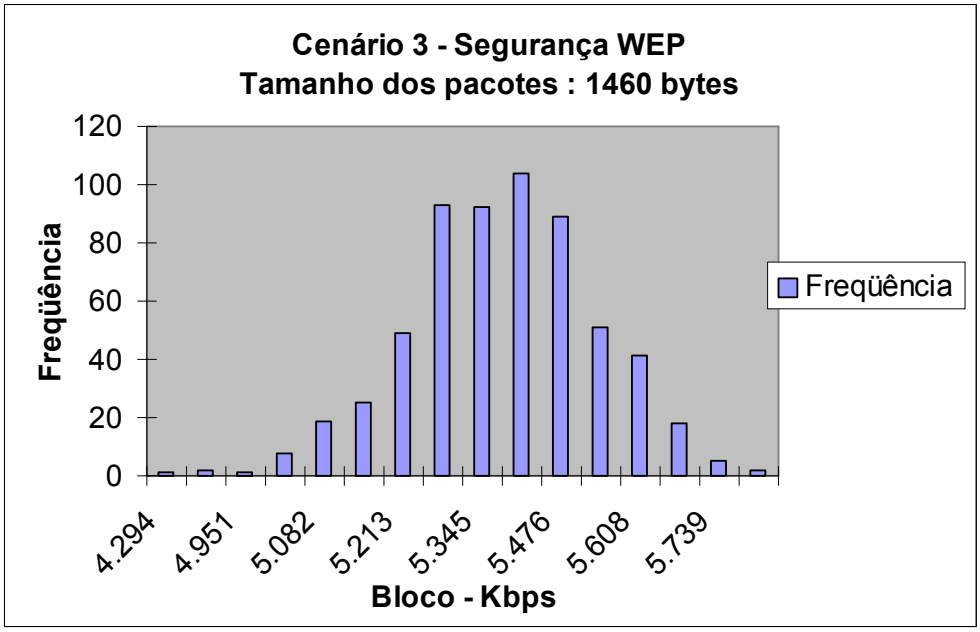

Cenário 2 - Sem segurança
Tamanho dos pacotes : 1460 bytes
Freqüência
100
90
80
70
60
50
40
30
20
10
0
9.026
9.145
9.204
9.264
9.323
9.383
9.442
9.501
9.561
9.620
9.679
Bloco - Kbps
Freqüência

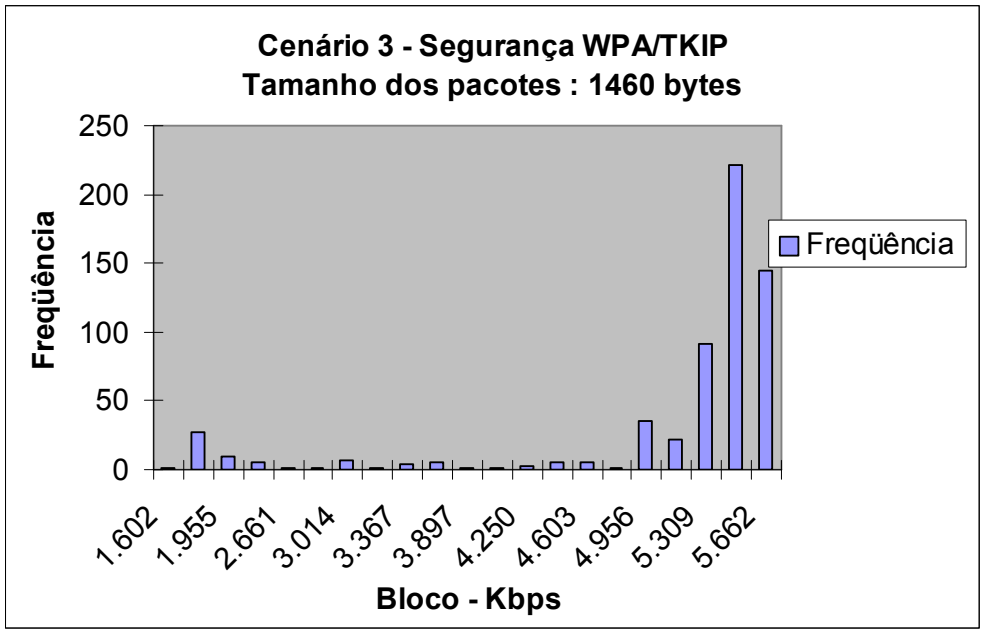

Cenário 2 - Segurança WEP
Tamanho dos pacotes : 1460 bytes
Freqüência
90
80
70
60
50
40
30
20
10
0
8.366
8.558
8.702
8.799
8.895
8.991
9.087
9.183
9.280
9.376
9.472
Bloco - Kbps
Freqüência


Cenário 2 - Segurança WPA/TKIP
Tamanho dos pacotes : 1460 bytes
Freqüência
80
70
60
50
40
30
20
10
0
8.039
8.163
8.245
8.328
8.411
8.493
8.576
8.659
8.741
8.824
8.907
8.989
Bloco - Kbps
Freqüência

3.3 Cenário 3


Cenário 3 - Sem segurança
Tamanho dos pacotes : 1460 bytes
Freqüência
90
80
70
60
50
40
30
20
10
0
5.032
5.116
5.200
5.283
5.367
5.451
5.535
5.619
5.703
5.787
5.871
5.955
Bloco - Kbps
Freqüência


Cenário 3 - Segurança WEP
Tamanho dos pacotes : 1460 bytes
Freqüência
120
100
80
60
40
20
0
4.294
4.951
5.082
5.213
5.345
5.476
5.608
5.739
Bloco - Kbps
Freqüência


Cenário 3 - Segurança WPA/TKIP
Tamanho dos pacotes : 1460 bytes
Freqüência
250
200
150
100
50
0
1.602
1.955
2.661
3.014
3.367
3.897
4.250
4.603
4.956
5.309
5.662
Bloco - Kbps
Freqüência