UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

ANÁLISE DE DESEMPENHO DE REDES SEM FIO COM DIFERENTES PROTOCOLOS DE CRIPTOGRAFIA: UM ESTUDO DE CASO

TRABALHO DE CONCLUSÃO DE CURSO

Douglas Pegoraro Stangarlin

Santa Maria, RS, Brasil

2012

ANÁLISE DE DESEMPENHO DE REDES SEM FIO COM DIFERENTES PROTOCOLOS DE CRIPTOGRAFIA: UM ESTUDO DE CASO

Douglas Pegoraro Stangarlin

Trabalho de Conclusão de Curso (TCC) do Curso Superior de Tecnologia em Redes de Computadores, da Universidade Federal de Santa Maria (UFSM,RS), como requisito parcial para obtenção do grau de
Tecnólogo em Redes de Computadores

Orientador: Prof. Ms. Walter Priesnitz Filho

Santa Maria, RS, Brasil

2012

UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

A Comissão Examinadora, abaixo assinada, aprova o Trabalho de Conclusão de Curso

ANÁLISE DE DESEMPENHO DE REDES SEM FIO COM DIFERENTES PROTOCOLOS DE CRIPTOGRAFIA: UM ESTUDO DE CASO

elaborado por
Douglas Pegoraro Stangarlin

COMISSÃO EXAMINADORA

Walter Priesnitz Filho, Ms.
(Presidente/Orientador)

Rogério Correa Turchetti, Ms. (UFSM)

Tiago Antonio Rizzetti, Ms. (UFSM)

Santa Maria, 06 de julho de 2012.

RESUMO

TRABALHO DE CONCLUSÃO DE CURSO
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES
UNIVERSIDADE FEDERAL DE SANTA MARIA

ANÁLISE DE DESEMPENHO DE REDES SEM FIO COM DIFERENTES PROTOCOLOS DE CRIPTOGRAFIA: UM ESTUDO DE CASO

AUTOR: DOUGLAS PEGORARO STANGARLIN
ORIENTADOR: WALTER PRIESNITZ FILHO
Data e Local da Defesa: Santa Maria, 06 de julho de 2012.

Este trabalho apresenta o estudo e desenvolvimento de uma análise de desempenho de redes sem fio IEEE 802.11, também conhecida como *Wireless* ou WiFi, levando em consideração os diferentes padrões de segurança existentes comercialmente para esta tecnologia.

O trabalho é desenvolvido em um ambiente controlado, em uma rede de infraestrutura, considerando à análise dos padrões de segurança em diferentes tempos de testes, sobre o protocolo de transporte UDP, a fim de comparar o desempenho conforme os diferentes padrões de segurança são utilizados.

Palavras-Chave: IEEE 802.11. DESEMPENHO. SEGURANÇA.

ABSTRACT

COMPLETION OF COURSE WORK
SUPERIOR OF TECHNOLOGY COURSE IN COMPUTER NETWORKS
FEDERAL UNIVERSITY OF SANTA MARIA

PERFORMANCE ANALYSIS OF WIRELESS NETWORKS WITH DIFFERENT ENCRYPTION PROTOCOLS: A CASE STUDY
AUTHOR: DOUGLAS PEGORARO STANGARLIN
ADVISER: WALTER PRIESNITZ FILHO
Defense Place and Date: Santa Maria, July 6th, 2012.

This work presents the study and development of a performance analysis of IEEE 802.11 wireless networks, also known as Wireless or WiFi, taking into account the different security standards for this technology commercially existing.

The work is developed in a controlled environment, in an infrastructure network, consider the analysis of security standards at different times of testing on the UDP transport protocol, in order to compare the performance according to different security standards are used.

Keywords: IEEE 802.11. PERFORMANCE. SECURITY.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AES	-	*Advanced Encription Standard*
AP	-	*Access Point*
TDMA	-	*Time Division Multiple Access*
BSS	-	*Basic Service Set*
MAC	-	Camada de acesso ao meio
PHY	-	Camada física
CERT.br	-	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
RC6	-	Cifra de bloco baseada no RC5
RC5	-	Cifra de bloco parametrizada projetada por Ronald Rivest
RC4	-	Cifra de fluxo projetada por Ronald Rivest
CBC-MAC	-	*Cipher Block Chaining Message Authentication Code*
CTR	-	*Counter Mode*
CCMP	-	*Counter-Mode/CBC-MAC Protocol*
DES	-	*Data Encription Standard*
DFS	-	*Dynamic Frequency Selection*
EAP-MD5	-	*EAP Message Digest 5*
EAP-TLS	-	*EAP Transport Layer Security*
EAP-TTLS	-	*EAP Tunneled TLS*
ECC	-	*Elliptic Curve Cryptography*
ESN	-	*Enhanced Security Network*
EAP	-	*Extensible Authentication Protocol*
HR-DSSS	-	*High Rate Direct Sequence Spread Spectrum*
IBSS	-	*Independent Basic Service Set*
IEEE	-	*Institute of Electrical and Electronics Engineers*
ICV	-	*Integrity Check Value*
ITU	-	*International Telecommunication Union*
IAPP	-	*Internet Access Point Protocol*
LEAP	-	*Lighweight Extensible Authentication Protocol*
LAN	-	*Local Area Network*
MD4	-	*Message Digest 4*
MD5	-	*Message Digest 5*
MIC	-	*Message Integrity Code*
MIMO	-	*Multiple-Input Multiple-Output*
NIST	-	*National Institute of Standards and Technology*
NSA	-	*National Security Agency*
NTP	-	*Network Time Protocol*
OSI	-	*Open Systems Interconnection*
OFDM	-	*Orthogonal Frequency Division Multiplexing*
PSK	-	*Pre-Shared Key*
PEAP	-	*Protected EAP*

QoS	-	Qualidade de Serviço (*quality of service*)
RF	-	Radio Frequência
WLANs	-	Redes locais sem fio (*Wireless Local Area Network*)
RADIUS	-	*Remote Authentication Dial In User Service*
RSA	-	*Rivest-Shamir-Adleman*
RSN	-	*Robust Security Network*
SHA-1	-	*Secure Hash Algorithm 1*
SHA-2	-	*Secure Hash Algorithm 2*
SSL/TLS	-	*Secure Sockets Layer/Transport Layer Security*
SSID	-	*Service Set IDentifier*
TKIP	-	*Temporal Key Integrity Protocol*
TPC	-	*Transmit Power Control*
UDP	-	*User Datagram Protocol*
IV	-	vetor de inicialização (*initialization vector*)
VOIP	-	*Voice over Internet Protocol*
WPA	-	*WiFi Protect Access*
WPA2	-	*WiFi Protect Access 2*
WEP	-	*Wired Equivalent Privacy*
WAVE	-	*Wireless Access in Vehicular Environments*
Wi-Fi	-	*Wireless Fidelity*
WNM	-	*Wireless Network Management*

SUMÁRIO

1 INTRODUÇÃO

Com o aumento de disponibilidade e serviços das redes sem fio, cada vez mais equipamentos destinados a este fim surgem no mercado. Para que este crescimento continue, o aumento da segurança e do desempenho destas redes tornam-se fundamentais, visto que estes dados trafegam por meio não guiado.

As questões de desempenho e segurança são vitais em redes de computadores. Em se tratando de redes sem fio esta questão é ainda mais importante, pois esta deve ter um alto nível de segurança sem apresentar perdas significativas no seu desempenho.

Redes sem fio são mais fáceis de ser interceptadas do que as comunicações com fio. Visto que, para ter acesso ao sinal irradiado da rede basta estar no alcance deste sinal com um dispositivo compatível, já em uma rede com fio é necessário ter um ponto de acesso para esta rede, como enfatizado por Nakamura e Geus (2007).

> Basta o usuário ligar seu equipamento sem fio ou notebook com placa *wireless* para que passe a ter acesso à internet. Isso, porém depende da configuração dos equipamentos; no entanto, do mesmo modo que o acesso é facilitado para usuários legítimos, ele é facilitado também para possíveis *hackers*. (Nakamura e Geus, 2007, p. 139-140).

Para tentar solucionar esta fragilidade é necessário o uso de mecanismos de segurança como cifragem e criptografia. A cifragem é "O uso de algoritmos matemáticos para transformar os dados em um formato que não seja prontamente decifrável. A transformação e subsequente recuperação dos dados dependem de um algoritmo e zero ou mais chaves de criptografia." (Stallings, 2008, p. 11). A criptografia é "a ferramenta automatizada mais importante para a segurança da rede e das comunicações." (Stallings, 2008, p. 15).

A criptografia em uma rede de computadores requer utilização da largura de banda da mesma e processamento extra, como Stallings (2008) descreve, o modelo genérico de criptografia consiste em gerar um pacote, criptografar o mesmo e só depois enviá-lo para o destinatário, este por sua vez executa a decriptografia do pacote e só após deste processo que o pacote é considerado transmitido com sucesso. Quanto mais complexo o algoritmo do protocolo de criptografia maior será o processamento necessário para os processos de criptografia e decriptografia.

"Algoritmos criptográficos basicamente objetivam "esconder" informações sigilosas de qualquer pessoa desautorizada a lê-las, isto é, qualquer pessoa que não conheça a chave

secreta de criptografia.” (Terada, 2008, p. 18). Para que isto seja verdade e, outra pessoa não consiga decifrar a chave da mensagem, o algoritmo de criptografia precisa ser complexo de maneira que um intruso não consiga decifrá-la ou, pelo menos, não em tempo hábil. Nakamura e Geus (2007) enfatizam que novos protocolos de criptografia surgem para solucionar as falhas dos anteriores, mais complexos e, consequentemente com maior tempo de processamento e maior utilização da largura de banda em uma rede de computadores. Nakamura e Geus (2007) também analisam que uma deficiência de segurança em redes de computadores são senhas fracas configuradas pelos usuários.

Neste trabalho são apresentados quanto os protocolos de criptografia interferem no desempenho de uma rede sem fio, apresentando estudos sobre o desempenho com os diferentes protocolos de criptografia disponíveis comercialmente na atualidade.

Este trabalho está organizado em seções, na seção 2 são apresentadas as redes sem fio e os padrões 802.11 presentes e os futuros padrões em desenvolvimento. Na seção 3 são apresentados conceitos de segurança, bem como o cenário atual de incidentes de segurança reportados ao CERT.br no Brasil. A seção 4 traz uma apresentação sobre criptografia, conceitos, aplicações e principais sistemas criptográficos. A seção 5 está destinada a segurança em redes sem fio, apresentando os padrões de segurança existentes atualmente. Na seção 6 são apresentados os parâmetros de desempenho em redes de computadores. A seção 7 traz o ambiente dos testes, bem como os testes realizados. A seção 8 é destinada a análise dos resultados. Apresentando na seção 9 as considerações finais.

2 REDES SEM FIO

2.1 Apresentação

Redes sem fio foram projetadas para suprir as necessidades não atendidas pelas redes cabeadas, surgiram nos anos 90 juntamente com o surgimento de equipamentos móveis, como *notebooks*. Segundo Tanenbaum (2003) nesta época, muitas pessoas sonhavam com o momento em que poderiam chegar a qualquer lugar e estar conectada a Internet, a partir dessas necessidades, vários grupos começaram a trabalhar para chegar nesse objetivo. Primeiramente foram equipados locais e *notebooks* com transmissores e receptores de ondas de rádio para permitir a comunicação entre eles, levando a utilização de redes sem fio de diferentes empresas sem um padrão definido. Consequentemente era difícil encontrar compatibilidade entre os diferentes fabricantes de equipamentos de rede sem fio, impossibilitando a comunicação entre eles.

Com o problema de comunicação entre diferentes equipamentos fabricados viu-se a necessidade de padronização para redes sem fio, a fim de possibilitar a comunicação independente do fabricante. Com isso foi criado um comitê no IEEE (*Institute of Electrical and Electronics Engineers)* que recebeu a tarefa de criar um padrão para LANs (*Local Area Network*) sem fio, o qual recebeu o nome de 802.11, também denominado *Wireless*, ou Wi-Fi (*Wireless Fidelity).*

O 802.11 foi elaborado para funcionar de duas maneiras: com um ponto de acesso, *Access Point* (AP), onde todas as comunicações deveriam passar pela estação-base, este tipo de rede também é conhecido como rede de infraestrutura; ou como *ad hoc* onde os computadores transmitem uns para os outros sem a necessidade de um AP. Tanenbaum (2003) enfatiza que para o primeiro padrão ser elaborado e aprovado, surgiram no mercado alguns desafios, os quais deveriam ser enfrentados, como descobrir uma banda de frequências disponível no mundo todo, manter a privacidade dos usuários, e construir um sistema economicamente viável.

O padrão 802.11 especifica as funções da camada física (PHY) e da camada de acesso ao meio (MAC), o que pode ser observado na Figura 1, de acordo com Stallings (2005).

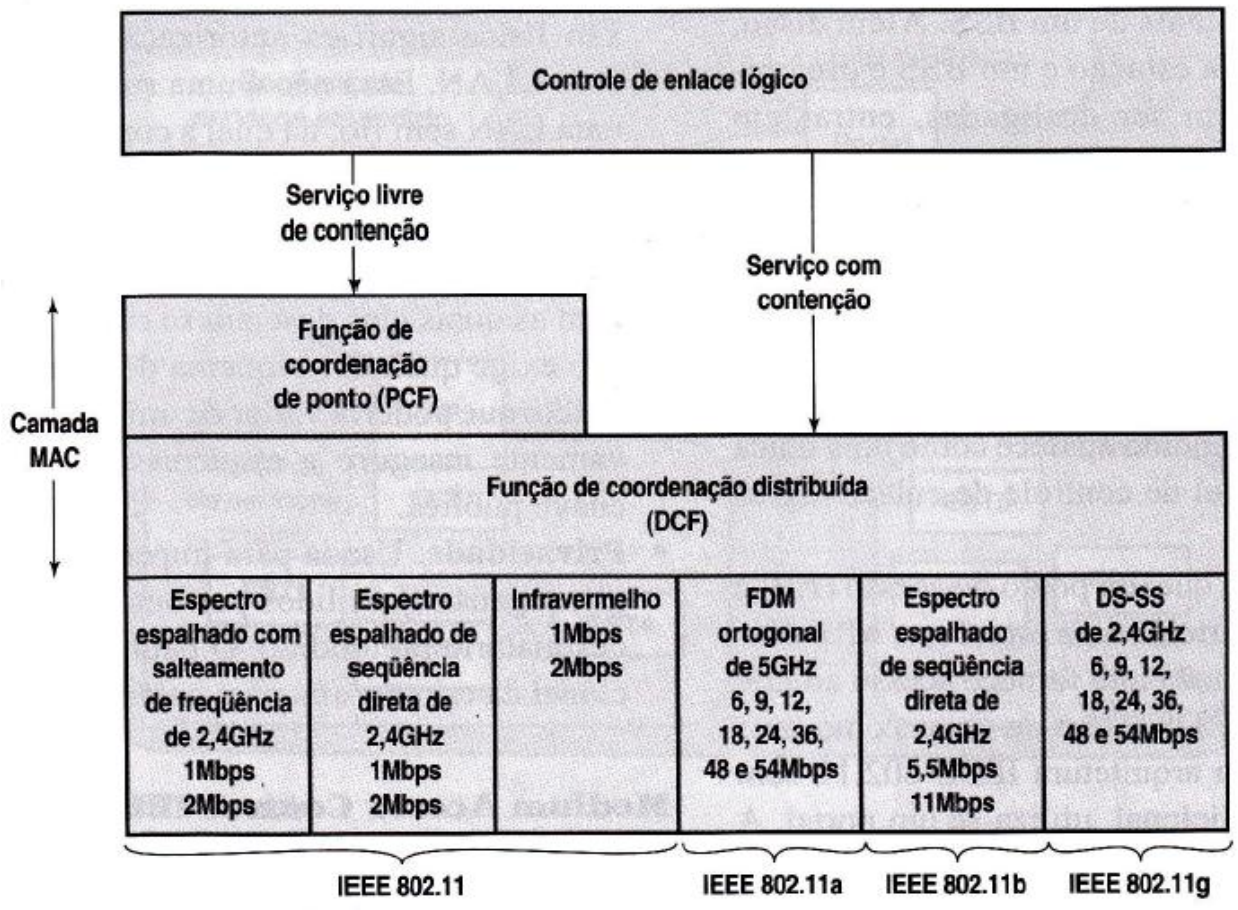


Figura 1 - Arquitetura do padrão 802.11, camada física e camada MAC.
Fonte: Stallings (2005, p. 236).

Nas redes 802.11 para a frequência de 2.4 GHz foram especificados 14 canais de transmissão, porém em alguns países 3 deles não podem ser usados devido a questões de legalização. Os canais disponíveis numerados de 1 a 11 englobando as frequências de 2,426 GHz a 2,462 GHz, com intervalos de 5 MHz entre eles e largura de banda de 22 MHz. Devido à largura de banda ser maior que os intervalos entre os canais e devido a proximidade entre os canais, estes interferem uns nos outros. Apenas 3 canais entre os 11 usualmente disponíveis não sofrem interferências uns dos outros se usados próximos, os quais são os canais 1 (2.412 GHz), 6 (2.437 GHz) e 11 (2.462 GHz).

A seguir podemos observar o

Quadro 1 com todos os canais disponíveis e suas respectivas frequências.

Canal	Frequência Central
1	2.412 GHz
2	2.417 GHz
3	2.422 GHz
4	2.427 GHz
5	2.432 GHz
6	2.437 GHz
7	2.442 GHz
8	2.447 GHz
9	2.452 GHz
10	2.457 GHz
11	2.462 GHz
12	2.467 GHz
13	2.472 GHz
14	2.484 GHz

Quadro 1 - Canais 802.11 disponíveis na banda de 2.4 GHz com respectivas frequências.
Fonte: Adaptado de *Moonblink Communications 2012*.

Em alguns países, como o caso do Brasil, os canais 12 e 13 também são liberados, porém a maioria dos equipamentos não vem com estes canais disponíveis. Como exemplo de equipamento com estes canais disponíveis pode-se observar a Figura 2, que representa os canais do D-Link DSL-2640B.

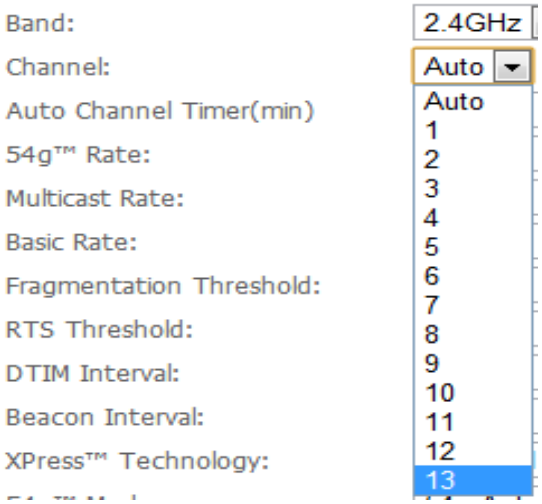


Figura 2 - Canais disponíveis no D-Link DSL-2640B.

O canal 14 é liberado no Japão. Pode-se observar a Figura 3 para visualizar a frequência de todos os canais disponíveis, assim como os canais que não interferem uns aos outros.

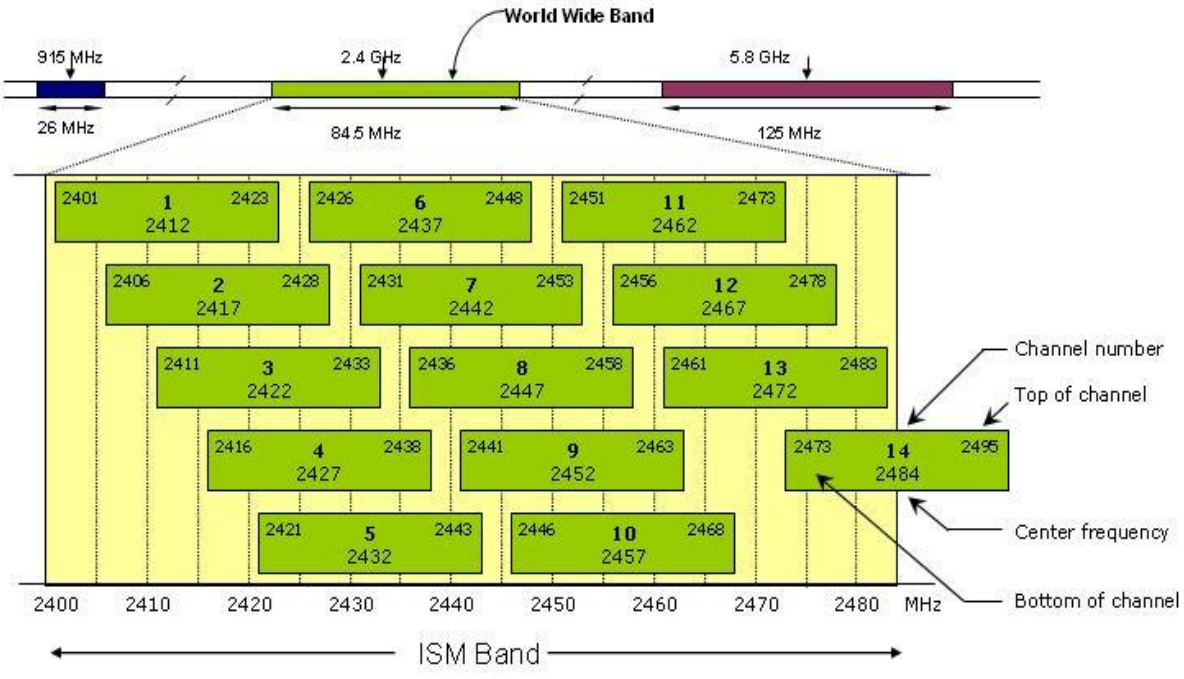


Figura 3 - Canais disponíveis e respectivas larguras de banda.
Fonte: *Moonblink Communications 2012*.

"As redes *wireless* ou redes sem fio são um sistema de comunicação de dados extremamente flexível, que pode ser usado como uma extensão, ou uma alternativa a redes locais (LANs cabeadas)" (Moraes, 2010, p. 174). Tendo como características mobilidade e conectividade de dados através de radio frequência (RF).

Segundo Moraes (2010) usuários precisam de mobilidade e a tecnologia *wireless* vai ao encontro dessas necessidades, pois é crescente o aumento de utilização de equipamentos móveis, como nos Estados Unidos cerca de um terço dos trabalhadores ficam 20% do tempo longe do escritório.

2.2 Padrões de Redes Sem Fio

O IEEE trabalhou para combater os desafios para este tipo de rede poder ser usado no mundo inteiro, e vem trabalhando nas melhorias para este padrão conforme vem surgindo novos desafios. Em 1997 o IEEE apresentou um padrão onde a LAN sem fio funcionava a 1 Mbps ou 2 Mbps, e assim começou o trabalho para padrões mais rápidos.

Em 1999 dois padrões foram publicados. O padrão 802.11a funcionando a velocidades de 54 Mbps e o padrão 802.11b com velocidades de 11 Mbps. A seguir serão apresentados os padrões para redes 802.11 já existentes, elaborados pelo IEEE em seus diferentes grupos de pesquisa, de acordo com Suzin (2007), Nakamura e Geus (2007), Moraes (2010), Vaughan-Nichols (2010), Netgear (2011) e IEEE (2012).

2.2.1 Padrão 802.11a

O padrão 802.11a foi concluído em 1999, e especifica que pode alcançar taxas de transmissão de até 54 Mbps, operando na frequência de 5 GHz em 8 canais de radio, com taxa máxima de transmissão de 54 Mbps por canal. Maior número de canais traz um controle maior com interferências entre APs vizinhos. Este padrão pode operar a taxas de transmissão de 6, 9, 12, 18, 24, 36, 48 e 54 Mbps. "Os produtos começaram a ser comercializados em 2002" (Nakamura e Geus, 2007, p. 165).

O padrão 802.11a utiliza *Orthogonal Frequency Division Multiplexing* (OFDM), esta utiliza múltiplos sinais em diferentes frequências, são usadas 52 diferentes frequências, sendo que 48 para dados e 4 para sincronização. Com as transmissões presentes em várias frequências ao mesmo tempo, essa divisão do sinal em bandas estreitas tem vantagens em relação ao uso de uma única banda, melhor imunidade à interferência de banda estreita e possibilidade de usar bandas não continuas.

Tendo como principais vantagens sua imunidade às interferências e velocidade de transmissão, porém tem uma grande desvantagem que é a incompatibilidade com outros padrões 802.11 difundidos. “Por trabalhar com frequência maior com o mesmo nível de potência de um dispositivo 802.11b, o alcance do padrão 802.11a acaba sendo 50% menor, além disso, o consumo de energia é maior, o que para dispositivos móveis não é muito adequado” (Moraes, 2010, p. 187).

2.2.2 Padrão 802.11b

Primeiro padrão publicado e usado em grande escala, marcando com isso a popularização da tecnologia de redes sem fio 802.11.

Utiliza a técnica de HR-DSSS (*High Rate Direct Sequence Spread Spectrum*), para alcançar 11 Mbps na banda de 2.4 GHz. Foi aprovado e chegou antes ao mercado que o padrão 802.11a. “O padrão ficou pronto em 1999, com produtos sendo comercializados a partir de 2001” (Nakamura e Geus, 2007, p. 165). Utiliza taxas de transmissão de 1, 2, 5,5 e 11 Mbps, essas taxas podem ser adaptadas dinamicamente durante a operação da conexão para alcançar a melhor velocidade possível sobre condições de carga e ruído. Suporta 32 usuários simultâneos.

Tem como principal vantagem maior alcance que o padrão 802.11a e a utilização de banda de 2.4 GHz que é disponível em todo o mundo. Porém segundo Suzin (2007) esta banda sofre muita interferência, pois vários equipamentos eletrônicos operam nesta faixa, como fornos de micro-ondas, telefones sem fio, *Bluetooth*.

Para uma melhor comparação entre o padrão 802.11a e o padrão 802.11b, podemos observar o Quadro 2 apresentando as diferenças entre eles, segundo Moraes (2010).

	802.11a	802.11b
Banda	Até 54 Mbps (54, 48, 36, 24, 18, 12 e 6 Mbps)	Até 11 Mbps (11, 5.5, 2 e 1 Mbps)
Alcance	50 metros	100 metros
Frequência	UNII e ISM (5 GHz range)	ISM (2.400 – 2.4835 GHz range)
Modulação	OFDM	DSSS

Quadro 2 – Padrão 802.11a x 802.11b.
Fonte: Moraes (2010, p. 187).

2.2.3 Padrão 802.11c

"Destinado a definir procedimentos de operações de ponte entre pontos de acesso" (Nakamura e Geus, 2007, p.165).

2.2.4 Padrão 802.11d

Desenvolvido para regiões fora dos domínios regulatórios (EUA, Canadá, Europa, Japão e Austrália), possui um *frame* estendido com informações dos países, tamanho de frequência e tabelas de parâmetros.

2.2.5 Padrão 802.11e

Responsável por desenvolver aspectos de qualidade de serviço (QoS), aumenta a camada MAC com acesso múltiplo por divisão de tempo (TDMA), adiciona mecanismos de correção de erros para aplicações sensíveis a atraso, como é o caso de voz e vídeo. Adequado especialmente para redes que suportam capacidade de multimídia.

2.2.6 Padrão 802.11f

Define os princípios básicos da arquitetura de redes sem fio, conceitos de *Access Point* e sistemas distribuídos. Descrevendo os serviços dos APs, protocolos compartilhados pelos fornecedores. “Trata da interoperabilidade entre produtos de diferentes fabricantes” (Nakamura e Geus, 2007, p. 166).

O 802.11f também define o protocolo IAPP (*Internet Access Point Protocol*), o qual é destinado à técnica de *handoff*, que permite conter vários *Access Points* para abranger uma maior área de cobertura, e a associação automática imperceptível no ponto de maior sinal, à medida que se movimenta pela área de cobertura.

2.2.7 Padrão 802.11g

Aprovado pelo IEEE em 2001 utiliza o método de modulação OFDM do padrão 802.11a e DSSS do padrão 802.11b, opera na banda de 2.4 GHz. Oferece velocidades de até 54 Mbps e compatibilidade com o padrão 802.11b, porém possui incompatibilidades com dispositivos de diferentes fabricantes. Segundo Moraes (2010, p. 187), o padrão 802.11g por utilizar OFDM consegue atingir o mesmo alcance do padrão 802.11b e as velocidades do padrão 802.11a por utilizar a mesma faixa de frequência, pois o OFDM é mais eficiente em utilização de banda passante. A compatibilidade com o padrão 802.11b é muito importante, pois com isso é possível adicionar equipamentos com este padrão em redes já existentes sem a necessidade de alterar estes equipamentos. “Os produtos começaram a ser comercializados no final de 2002” (Nakamura e Geus, 2007, p. 166).

Para efeito de comparação do padrão 802.11g com o 802.11a, apresenta-se o Quadro 3.

IEEE 802.11a	IEEE 802.11g
5 GHz, 54 Mbps;	2,4 GHz, 54 Mbps
Não é compatível com 802.11b	Compatível com 802.11b

Continua.

Conclusão.

Necessita de mais APs para cobrir a mesma área 25% a mais	Mesma cobertura do padrão 802.11b
802.11b e 802.11a podem ser usados juntos	802.11g opera na mesma frequência do padrão 802.11b

Quadro 3 – Padrão 802.11a x 802.11g.
Fonte: Moraes (2010, p. 188).

Ao aumentar a distância de transmissão, as placas de redes sem fio tendem a reduzir a taxa de transmissão para manter a estabilidade do sinal. As redes 802.11g, reduzem sequencialmente para 48, 36, 24, 18, 12, 11, 9, 6, 5,5, 2 e 1 Mbps, até que o sinal não seja mais suficiente para a transmissão e a conexão é perdida.

A principal diferença entre este padrão e o 802.11b é que o último só utiliza modulação DSSS.

2.2.8 Padrão 802.11h

Este padrão foi elaborado para resolver os problemas de interferência causados pelo uso do padrão 802.11a em algumas regiões, como por exemplo, na Europa, onde radares militares operam na mesma faixa de frequência, 5 GHz, regras do padrão 802.11h foram recomendadas pela *International Telecommunication Union* (ITU), principalmente por problemas de interferência na Europa.

"O 802.11h trata também de gerenciamento de controle de energia" (Nakamura e Geus, 2007, p. 166). Foram introduzidos dois sistemas para minimizar a interferência. *Dynamic Frequency Selection* (DFS), a qual detecta automaticamente outros dispositivos no mesmo canal e troca para outro canal. *Transmit Power Control* (TPC) reduz a potência da transmissão dos transmissores da rede para um nível que permita o desempenho satisfatório da rede com objetivo de minimizar o risco de interferência.

2.2.9 Padrão 802.11i

Criado para melhorar as funções de segurança em redes sem fio 802.11, conhecido como *Enhanced Security Network* (ESN). Tem como objetivo melhorar a segurança das WLANs - Redes locais sem fio, bem como confirmar deficiências de segurança do protocolo WEP - *Wired Equivalent Privacy*, e criar novos protocolos de segurança para redes sem fio.

Este padrão, juntamente com seus protocolos, será tratado mais profundamente, adiante na seção referente à segurança em redes sem fio. Pois os protocolos serão base para o proposto neste trabalho.

2.2.10 Padrão 802.11j

Este padrão foi proposto para utilização no Japão para o 802.11a, tendo como objetivo principal adicionar canais entre 4,9 GHz a 5 GHz, além de requisitos legais referentes à potência do transmissor, modos de operações, disposições dos canais, e níveis de emissão adulteradas.

2.2.11 Padrão 802.11k

Padrão com objetivo de definir como a rede WLAN deve realizar a seleção do canal, *roaming*, e TPC, com objetivo de aperfeiçoar o desempenho da rede. Tendo como principal objetivo melhorar a forma como o tráfego de rede é distribuído em uma rede sem fio.

Comumente em uma rede 802.11 os dispositivos móveis conectam-se ao *Acess Point* com maior potência no sinal, porém se existirem muitos usuários conectados neste AP, o tráfego desta rede será muito grande, e consequentemente irá diminuir o desempenho da rede. Nestes casos em uma rede dentro do padrão 802.11k, existindo outro AP com sinal mais fraco, mas que não esteja sobrecarregado, a conexão se dará neste outro AP, ganhando com isso um desempenho maior do que conectar-se no AP sobrecarregado.

2.2.12 Padrão 802.11n

Em 2004 o IEEE formou uma equipe, força tarefa, destinada a desenvolver um novo padrão 802.11, tendo como objetivo oferecer velocidades de transmissão superiores às das redes cabeadas 802.3 de 100 Mbps. Melhorando também latência, alcance e confiabilidade de transmissão.

Para atingir estes objetivos a solução foi combinar melhorias nos algoritmos de transmissão e do uso do *multiple-input multiple-output* (MIMO), o qual permite utilizar diversos fluxos de transmissão de forma paralela. Com isso a velocidade de transmissão que era de 54 Mbps nos padrões 802.11a e 802.11g passou para 300 Mbps, e utilizando múltiplos fluxos de transmissão foi possível tornar o alcance do sinal quase duas vezes maior.

No padrão 802.11n existem 52 faixas de transmissão diferentemente de 48 encontradas no padrão 802.11g para transmissão de dados. O padrão 802.11g também possui 52 faixas de transmissão, porém 4 delas são destinadas para transmitir informações sobre modulação do sinal, no 802.11n foi realocado estas faixas para transmitirem dados também. Aumentando a banda total utilizada para este fim.

Para chegar à velocidade de transmissão prometidas o padrão trás a combinação de vários rádios e 2 canais simultâneas com a utilização do MIMO, utilizando 4 fluxos simultâneos chegando com isso a taxas de aproximadamente 300 Mbps. Porém aumentando com isso a interferência, pois o padrão utilizará uma faixa de frequência de 40 MHz, utilizando os mesmos canais do padrão 802.11g.

Além das taxas de transmissão um dos diferenciais do padrão 802.11n é o uso das faixas de frequência de 2.4 GHz e 5 GHz.

2.2.13 Padrão 802.11p

Destinado a comunicações entre veículos, utilizando a banda de 5,9 GHz. Também chamado de *Wireless Access in Vehicular Environments* (WAVE), serviços previstos para este padrão incluem, aviso de detecção de colisão, informações de tráfego. Este padrão pode trocar de canal à medida que for necessário para não perder dados importantes de segurança,

ele pode estar transmitindo dados em um canal e quando necessitar de informações de segurança o mesmo deve ser capaz de trocar de canal para poder transmitir.

2.2.14 Padrão 802.11r

Padrão publicado em 2008, com objetivo de que dispositivos sem fio possam trocar de *Access Point* com maior rapidez, é também conhecido como *Fast Basic Service Set Transition*. Para executar esta troca rápida o padrão permite que o dispositivo valide informações de segurança e conexão com outro *Access Point* antes de deixar a conexão com o antigo.

Possibilitando com isto fazer um *roaming* mais rápido e sem perder conexão. Será muito útil para conexões VOIP (*Voice Over Internet Protocol*).

2.2.15 Padrão 802.11s

O padrão tem como objetivo padronizar redes *mesh* entre dispositivos sem fio. Tem como grande vantagem não precisar de nenhuma infraestrutura cabeada para configurar a rede, vários dispositivos sem fio formando uma rede *mesh*, tem como ganho conexões diretas entre os dispositivos, como se fosse uma conexão *ad hoc* entre dois dispositivos, porém neste caso poderá haver vários dispositivos na rede com ligações diretas entre eles.

2.2.16 Padrão 802.11t

Este padrão possui normas que resultam em métodos de testes e métricas em redes 802.11.

2.2.17 Padrão 802.11u

O padrão 802.11u tem como objetivo a autenticação automática e *handoff* transparente, permitindo usuários fazerem *roaming* entre as redes sem necessidade de autenticação adicional.

2.2.18 Padrão 802.11v

Publicado em 2011, traz um padrão para gerenciamento de rede sem fio 802.11, *Wireless Network Management* (WNM) proporcionando gerenciar a carga de tráfego cliente dispositivo.

2.2.19 Padrões em Desenvolvimento

Como descrito anteriormente o IEEE vem trabalhando continuamente para desenvolver a tecnologia das redes sem fio, visto que estas estão em ascensão e necessitam de constante evolução. Assim faz-se necessário aprimorar os padrões já existentes, levando em consideração segurança, desempenho e outras inúmeras vantagens que a tecnologia fornece.

Como as redes cabeadas, as redes sem fio tem a necessidade de aumento nas taxas de transmissão. Para tais questões está em desenvolvimento o padrão 802.11ac. Este padrão atende as necessidades de maiores velocidades e maior alcance, sendo ideal para trafego de multimídia.

Segundo Vaughan-Nichols (2010) o padrão 802.11ac vai funcionar na banda de frequência de 5 GHz, fornecendo taxas de transmissão a 1 Gbps e utilizar segurança do padrão WPA2, a largura dos canais de transmissão vão ser de 40, 80 ou 160 MHz, diferentemente do padrão 802.11a que utiliza 20 Mhz.

Segundo a Netgear (2011), o 802.11ac possui como principais vantagens à velocidade superior ao padrão 802.11n em 3 vezes, melhores distâncias de propagação, podendo cobrir o ambiente com menos APs, mais confiável, sendo ideal para vídeos, e também para

dispositivos móveis. Também possui compatibilidade com o padrão 802.11a que também utiliza a banda de 5 GHz.

Além do padrão 802.11ac estão em fase de desenvolvimento outros padrões para as redes sem fio 802.11, os quais podem ser consultados em IEEE (2012).

3 SEGURANÇA

3.1 Conceitos Básicos

Segurança na computação é um tema sempre muito discutido, muito porque este está sempre mudando, pois novas ameaças surgem o tempo todo. Segundo Nakamura e Geus (2007) o mundo da segurança é formado por um ciclo, pois novos ataques tem como resposta novas formas de proteção, levando ao desenvolvimento de novas técnicas de ataque, e assim sucessivamente.

Para demonstrar como é importante a questão de segurança em redes de computadores, pode-se observar a Figura 4. A qual trás informações de incidentes reportados ao CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil).

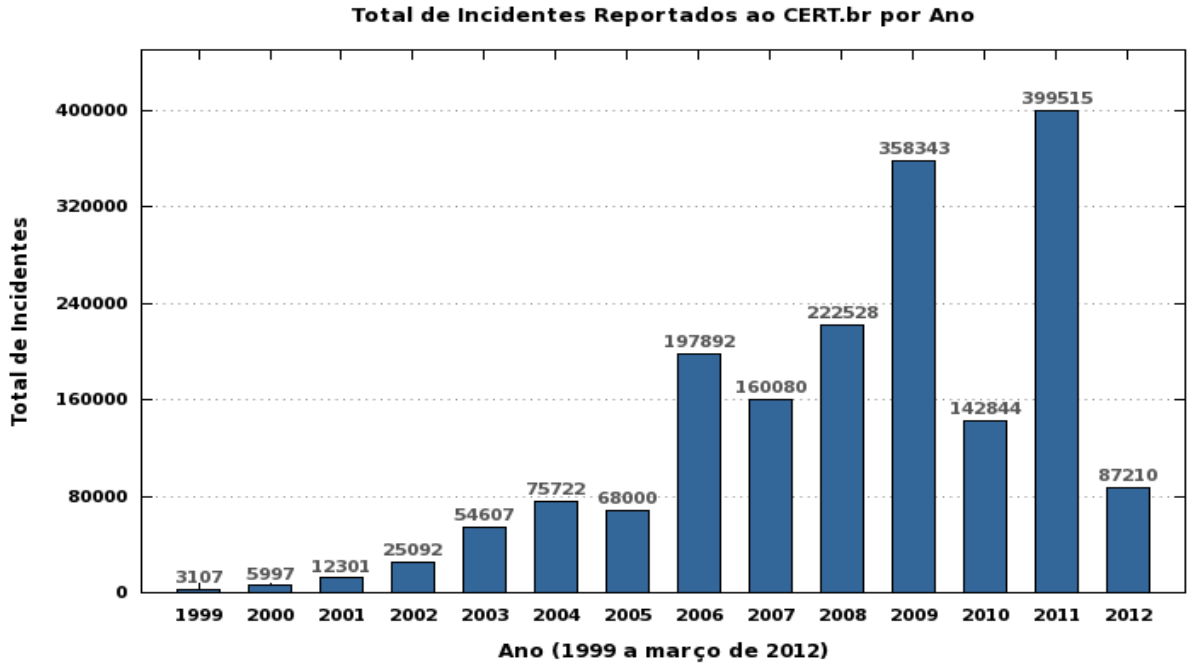


Figura 4 - Crescimento dos incidentes reportados ao CERT.br, de 1999 a março de 2012.
Fonte: CERT.br.

O gráfico da Figura 4 demonstra que a partir de 2006 os incidentes relatados aumentaram consideravelmente em relação aos anos anteriores, pois se forem somados os

incidentes reportados do ano de 2006 e 2007, tem-se um total de 357.972 incidentes, e somando os incidentes reportados de 1999 a 2005, tem-se um total de 244.826 incidentes reportados, ou seja, em 2 anos o número de incidentes superou em mais de 30% (31, 61%) o número de incidentes nos 7 anos anteriores. Porém como pode ser observado em 2010 o número de incidentes reportados é bem inferior em relação aos anos adjacentes, isto não significa necessariamente que o número de incidentes neste ano foi inferior à média dos anos próximos, pois o gráfico só trás os incidentes reportados ao CERT.br. Pode-se estimar que, permanecendo os mesmos perfis de comportamento, em 2012 o número de incidentes reportados do ano chegará próximo aos 350.000. Pode-se observar na Figura 5 o número de incidentes reportados em 2012 de forma mais detalhada, para uma melhor análise do cenário atual.

Incidentes Reportados ao CERT.br -- Janeiro a Março de 2012

Tabela: Totais Mensais e Trimestral Classificados por Tipo de Ataque.

Mês	Total	worm (%)		dos (%)		invasão (%)		web (%)		**scan** (%)		**fraude** (%)		outros (%)	
jan	**27148**	6830	25	7	0	603	2	2137	7	8478	31	4096	15	4997	18
fev	**25266**	4404	17	34	0	452	1	2211	8	8523	33	4183	16	5459	21
mar	**34796**	2380	6	22	0	559	1	3508	10	10616	30	5126	14	12585	36
Total	**87210**	13614	15	63	0	1614	1	7856	9	27617	31	13405	15	23041	26

Figura 5 - Incidentes reportados ao CERT.br no 1º trimestre de 2012.
Fonte: CERT.br.

Segundo Nakamura e Geus (2007) a integridade, disponibilidade, confidencialidade e sigilo formam as propriedades mais importantes para segurança. “Toda a informação deve chegar aos usuários de forma integra e confiável. Para que isso aconteça, todos os elementos da rede por onde a informação flui até chegar ao seu destino devem estar disponíveis, e devem também preservar integridade das informações" (Nakamura e Geus, 2007, p. 43).

Tem-se como segurança aspectos físicos e lógicos. Entre os aspectos físicos está o controle de acesso aos equipamentos presentes na rede, onde deve-se controlar quem acessa esses equipamentos e o que fez durante o acesso, principalmente em equipamentos fundamentais para o funcionamento da rede. Já na parte lógica é mais difícil manter este

controle, pois tentativas de acesso às redes acontecem frequentemente, e para isto basta estar conectado na Internet. Redes locais normalmente tem uma conexão com a Internet, pois muitos serviços acessados por essas redes em empresas são através da Internet.

Em redes domésticas o objetivo principal é o acesso à Internet. E muitas vezes este acesso se dá através de redes *wireless*, estas estão mais vulneráveis que redes cabeadas, pois o acesso ao meio de transmissão é simplesmente o ar, o que qualquer dispositivo dentro do alcance do sinal tem com facilidade. Por isto existe o Padrão 802.11i, para prover mecanismos que assegurem a segurança neste meio.

Mas para entendimento de segurança em redes *wireless* é de fundamental importância conhecimentos gerais sobre segurança da informação os quais serão apresentados nesta seção.

3.2 Mecanismos de Segurança

Segundo Stallings (2008) existem mecanismos de segurança definidos na recomendação X.800, a qual traz mecanismos de criptografia reversíveis e irreversíveis. Mecanismos reversíveis são basicamente algoritmos de criptografia que permite que os dados sejam criptografados e decriptografados. Já mecanismos irreversíveis incluem algoritmos de *hash* e códigos de autenticação de mensagens, os quais serão descritos na seção 4.

Stallings (2008) cita os principais mecanismos de segurança descritos na X.800, que divide em mecanismos de segurança específicos, que podem ser implementados em uma camada específica do modelo OSI (*Open Systems Interconnection*) oferecendo alguns dos serviços do modelo OSI. E os mecanismos de segurança pervasivos que não estão ligados a qualquer serviço ou camada de protocolo OSI.

3.2.1 Mecanismos de Segurança Específicos

Nesta seção serão abordados os mecanismos de segurança específicos a uma camada do modelo OSI ou a um serviço de segurança oferecido por este modelo.

3.2.1.1 Cifragem

Cifragem é o uso de algoritmos matemáticos para transformar os dados originais em dados desconhecidos para outros usuários. Para transformar esses dados em dados cifrados é necessário um algoritmo de criptografia e chaves de criptografia.

3.2.1.2 Assinatura Digital

Assinatura digital, segundo Stallings (2008) é a comprovação da origem e da integridade de uma unidade de dados, ou seja, é adicionar dados a uma unidade para comprovar a origem destes dados, garantindo a proteção contra falsificação da origem dos dados.

3.2.1.3 Controle de Acesso

“Uma série de mecanismos que impõem direitos de acesso aos recursos” (Stallings, 2008, p. 11).

3.2.1.4 Integridade de Dados

Mecanismos para garantir a integridade e, ou, fluxo dos dados.

3.2.1.5 Troca de Informação de Autenticação

“Um mecanismo com o objetivo de garantir a identificação de uma entidade por meio da troca de informações” (Stallings, 2008, p. 11).

3.2.1.6 Preenchimento de Tráfego

Inserir *bits* durante as lacunas de um fluxo de dados com objetivo de dificultar tentativas de análise de tráfego.

3.2.1.7 Controle de Roteamento

“Permite a seleção de determinadas rotas fisicamente seguras para certos dados e permite mudanças de roteamento, especialmente quando existe suspeita de uma brecha de segurança” (Stallings, 2008, p. 11).

3.2.1.8 Certificação

Segundo Stallings (2008), na certificação é utilizada uma terceira entidade, confiável, para garantir propriedades de uma troca de dados.

3.2.2 Mecanismos de Segurança Pervasivos

Nesta seção serão apresentados os mecanismos de segurança que não estão presos a uma camada ou a um serviço do modelo OSI.

3.2.2.1 Funcionalidade Confiável

É uma funcionalidade que obedece alguns critérios pré-estabelecidos.

3.2.2.2 Rótulo de Segurança

Segundo Stallings (2008) é uma marcação para nomear ou designar atributos de segurança de um determinado recurso.

3.2.2.3 Detecção de Evento

Detectar eventos relevantes à segurança é sempre um bom procedimento para a segurança, pois através destes eventos pode ser possível detectar ataques ou tentativas de ataques à segurança, podendo evitar estes ataques.

3.2.2.4 Registro de Auditoria de Segurança

Serve para uma posterior revisão e exame da segurança, através de auditorias é possível detectar um ataque que já aconteceu e talvez descobrir a origem deste ataque. Por isso é muito importante armazenar os dados coletados referentes à segurança.

3.2.2.5 Recuperação de Segurança

“Lida com solicitações de mecanismos, como funções de tratamento e gerenciamento de eventos, e toma medidas de recuperação” (Stallings, 2008, p. 11).

4 CRIPTOGRAFIA

4.1 Conceito

Segundo RSA *Security* (2000) a criptografia tem como finalidade garantir a privacidade, mantendo a mensagem escondida de qualquer pessoa para a qual não são destinadas, mesmo os que tiverem acesso aos dados não terão acesso ao significado da informação.

"A palavra *criptologia* é de origem grega, onde *kriptos* designa coisa oculta, e *logos* designa estudo, portanto, o estudo das coisas secretas" (Suzin, 2007, p. 23). "É a ciência que por meio de matemática permite criptografar (cripto = esconder) e decriptografar dados" (Moraes, 2010, p. 213).

Segundo Stallings (2008) a mensagem original é chamada de texto claro (*plaintext*) e a mensagem codificada é chamada de texto cifrado (*ciphertext*). A criptografia também podendo ser chamada de cifragem é a transformação do texto claro em texto cifrado, e a restauração do texto cifrado em texto claro é a decifragem ou decriptografia. O sistema criptográfico ou cifra é todo o processo de criptografia e decriptografia.

Existe uma ciência denominada criptoanálise, a qual é destinada a decifrar mensagens criptografadas sem nenhum conhecimento dos detalhes da criptografia. A criptoanálise descobre falhas nos algoritmos de criptografia, com a finalidade de desenvolver sistemas criptográficos seguros. "As áreas de criptografia e criptoanálise juntas são chamadas de criptologia" (Stallings, 2008, p. 18).

A criptografia é utilizada bem antes dos computadores, pois governos e, ou, impérios utilizavam esta técnica para enviar mensagens sem permitir que se fossem interceptadas, estas fossem lidas. Moraes (2010) traz um exemplo de utilização de um modelo criptográfico denominado Júlio Cyper, o qual foi utilizado por Júlio César, na época do Império Romano, para evitar que as mensagens enviadas nos campos de batalha, as quais eram enviadas por um mensageiro a cavalo, não fossem lidas, ou pelo menos entendidas, se fossem interceptadas.

Outra utilização bastante importante de criptografia foi na segunda guerra mundial, onde mensagens criptografadas definiram o rumo da guerra. Segundo Tanenbaum (2003) os Estados Unidos conseguiram quebrar o código japonês e estes não terem conseguido quebrar o código utilizado pelos americanos foi decisivo nas vitórias americanas no Pacífico.

> No mundo digital, a criptografia é realizada a partir de algoritmos, que realizam a encriptação e decriptação dos dados, ou seja, transformam um texto simples (claro) em um texto cifrado. Para a realização desse processo, o algoritmo precisa de uma chave, que consiste em um conjunto de números aleatórios, e que pode ser vista analogamente a uma chave de fechadura convencional, onde apenas a que fecha é capaz de abrir novamente (chave simétrica) (Suzin, 2007, p. 23-24).

4.2 Aplicações da Criptografia

Esta seção apresenta as principais aplicações da criptografia, segundo a RSA *Security* (2000).

4.2.1 Comunicações Seguras

Esta é um dos principais usos de criptografia, pois sistemas necessitam comunicar-se de forma segura e eficiente, não permitindo que um terceiro, mal intencionado, intercepte estas mensagens e possa ser capaz de decifrá-las. Ferramentas de criptografia que garantem esta comunicação estão presentes graças ao desenvolvimento de criptografia de chave pública. Estas ferramentas são capazes de criar redes de larga escala, para comunicações seguras, permitindo estas comunicações mesmo que nunca tivesse acontecido antes.

4.2.2 Identificação e Autenticação

São aplicações amplamente utilizadas da criptografia. “A identificação é um processo através do qual se verifica a identidade de outra pessoa ou entidade” (RSA *Security*, 2000, p. 45). Tendo como ideia associar a cada pessoa ou entidade algo único. A autenticação é semelhante à identificação, porém mais ampla, pois não envolve necessariamente a identificação de uma pessoa ou entidade, ela apenas determina se esta pessoa ou entidade está autorizada para o acesso em questão.

4.2.3 Compartilhamento de Chave

"Permite que um "segredo" possa ser compartilhado entre um determinado grupo de pessoas. Em qualquer esquema de compartilhamento de chave, há um designado conjunto de pessoas que acumulam informação suficiente para determinar o segredo" (RSA *Security*, 2000, p. 14).

Alguns sistemas de compartilhamento de chaves, as mesmas são disponíveis depois de serem geradas, em outros os usuários o segredo real nunca se torna visível aos participantes.

4.2.4 *E-Commerce*

O comércio eletrônico, ou *e-commerce* está muito em uso atualmente, mas para seu sucesso é fundamental um mecanismo de segurança eficiente, a criptografia é este mecanismo.

Ao digitar o numero de cartão de crédito na realização de uma compra na Internet é necessário criptografar os dados enviados para impedir que quando interceptada as mensagens estas não possam ser decifradas, pois caso sejam o interceptador obterá os dados do cliente, podendo se passar pelo cliente utilizando seus dados, por exemplo, em compras na Internet.

4.2.5 Certificação

Certificação é um esquema no qual agentes confiáveis enviam um certificado digital para um agente desconhecido. Foi desenvolvido para tornar a identificação e autenticação possível em grande escala.

4.2.6 Recuperação de Chave

Tecnologia que permite que uma chave seja liberada em certas circunstâncias sem que o proprietário da chave a revele. Útil para um usuário que perder a chave e para uma decriptografia de dados de um suspeito criminal.

4.2.7 Acesso Remoto

O uso de criptografia em acesso remoto seguro é importante, pois apenas uma senha poderia ser copiada facilmente, com a criptografia isto não é possível. Muitos produtos oferecem acesso remoto seguro com alto grau de segurança.

4.2.8 Outras Aplicações

A criptografia pode ser utilizada para os mais variados sistemas tecnológicos, não se limitando a computadores, podendo ser empregada em telefones móveis e outros equipamentos, ganhando segurança nas informações contidas e transmitidas por estes.

4.3 Tipos de Criptografia

A criptografia e dividida por dois tipos de algoritmos, o primeiro conhecido como algoritmo de chave simétrica, também chamado de algoritmo de chave secreta, este tipo de criptografia todos os envolvidos na comunicação devem conhecer a chave. O segundo tipo de criptografia é conhecido como algoritmo de chave assimétrica ou algoritmo de chave publica, considerado mais seguro, nesse sistema de criptografia todas as partes conhecem a chave pública, porém cada um tem uma chave privada. A chave publica serve para criptografar os dados, porém para decriptografar é usada à chave privada, e somente esta poderá ser capaz de decriptografar a mensagem.

4.3.1 Algoritmos de Chave Simétrica

"No algoritmo de chave simétrica a chave usada para criptografar é a mesma usada para decriptografar os dados. A criptografia simétrica era o único tipo de criptografia em uso antes do desenvolvimento da criptografia por chave pública na década de 1970" (Stallings, 2008, p.18).

O mesmo autor afirma que existem cinco elementos para um modelo de cifra simétrica:

- Texto claro: É a mensagem de entrada para o algoritmo de criptografia, original e perceptível.

- Algoritmo de criptografia: Realiza transformações e substituições no texto claro, com objetivo de deixa-lo indecifrável para quem não possuir a chave secreta.

- Chave secreta: Também é entrada para o algoritmo de criptografia. Através da chave secreta o algoritmo faz as substituições e transformações no texto claro.

- Texto cifrado: É o texto produzido como saída do algoritmo de criptografia, incompreensível para um interceptador da mensagem que não possuir a chave secreta.

- Algoritmo de decriptografia: Tem como entrada o texto cifrado e a chave secreta, fazendo a execução de forma inversa a do algoritmo de criptografia para tornar o texto compreensível, ou seja, tendo como saída o texto claro.

Pode-se observar as etapas para o processo de criptografia e decriptografia demonstrados anteriormente na Figura 6.

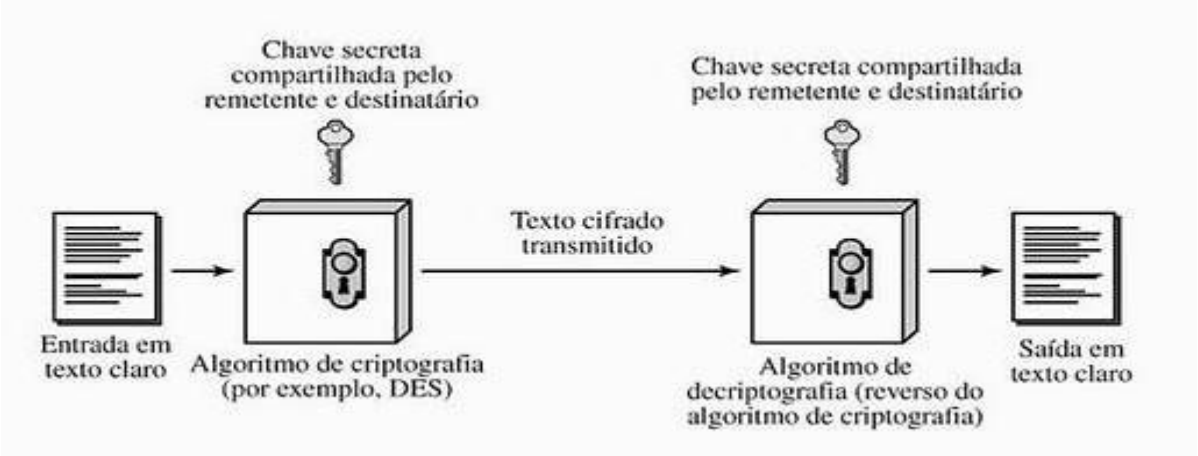


Figura 6 - Modelo de criptografia de chave simétrica.
Fonte: Stallings (2008, p. 18).

Para ser possível a utilização em larga escala deste tipo de criptografia foi necessário tornar públicos os algoritmos, pois caso o algoritmo fosse secreto, não seria viável fabricar chips de baixo custo com algoritmos de criptografia de dados. Para isto foram desenvolvidos algoritmos fortes.

Stallings (2008) comenta que o emissor e receptor precisam ter de forma segura as cópias da chave secreta, pois caso seja descoberta a chave toda a comunicação usando essa chave poderá ser lida. Pois como o algoritmo é publico basta saber a chave para poder decifrar os dados criptografados.

Para criptografia de chave simétrica existem dois tipos de algoritmos de criptografia, um por bloco e outro por fluxo. Na cifra de fluxo é codificado em um fluxo de dados um *bit* ou *byte* de cada vez.

"Uma cifra de bloco é um esquema de criptografia/decriptografia em que um bloco de texto claro é tratado como um todo e usado para produzir um bloco de texto cifrado de mesmo tamanho" (Stallings, 2008, p. 40). Na cifra de bloco é normalmente utilizado blocos de tamanho de 64 ou 128 bits, podendo ser usada para conseguir o mesmo efeito da cifra de fluxo.

4.3.2 Algoritmos de Chave Pública

No algoritmo de chave publica, ou assimétrica, a chave utilizada para criptografia é uma chave publica, ou seja, disponibilizada para todos os usuários envolvidos, já a chave para decriptografia é uma chave privada relacionada com a chave pública. Segundo Stallings (2008) a evolução do conceito de criptografia de chave pública buscou solucionar dois dos problemas mais difíceis da criptografia simétrica. A distribuição de chaves e as assinaturas digitais.

Stallings (2008) afirma que os algoritmos de chave assimétrica tem uma característica importante, como ser computacionalmente inviável determinar a chave de decriptografia através apenas do algoritmo e da chave de criptografia.

Segundo Stallings (2008) existem seis elementos para um modelo de cifra assimétrica:

Os elementos da cifra assimétrica são os mesmos da cifra simétrica, exceto pela chave secreta existente na cifra simétrica, no lugar dela existem a chave pública e a chave privada. Essas chaves são selecionadas de maneira que se uma for usada para criptografia à outra é usada para decriptografia.

Para entender melhor o processo de criptografia e decriptografia assimétrica, pode-se considerar um exemplo dos passos para o processo da mesma, segundo Stallings (2008):

1º - Cada usuário gera um par de chaves destinadas à criptografia e decriptografia.

2º - Cada usuário disponibiliza uma das duas chaves, sendo esta considerada a chave pública.

3º - Se um usuário A deseja enviar uma mensagem para um usuário B, o usuário A criptografa a mensagem com a chave pública do usuário B.

4º - Quando o usuário B recebe a mensagem, decriptografa usando a chave privada. Nenhum outro destinatário pode decriptografar a mensagem, pois somente o usuário B conhece a chave privada correspondente para a decriptografia.

Pode-se observar na Figura 7 o processo de criptografia e decriptografia de chave pública.

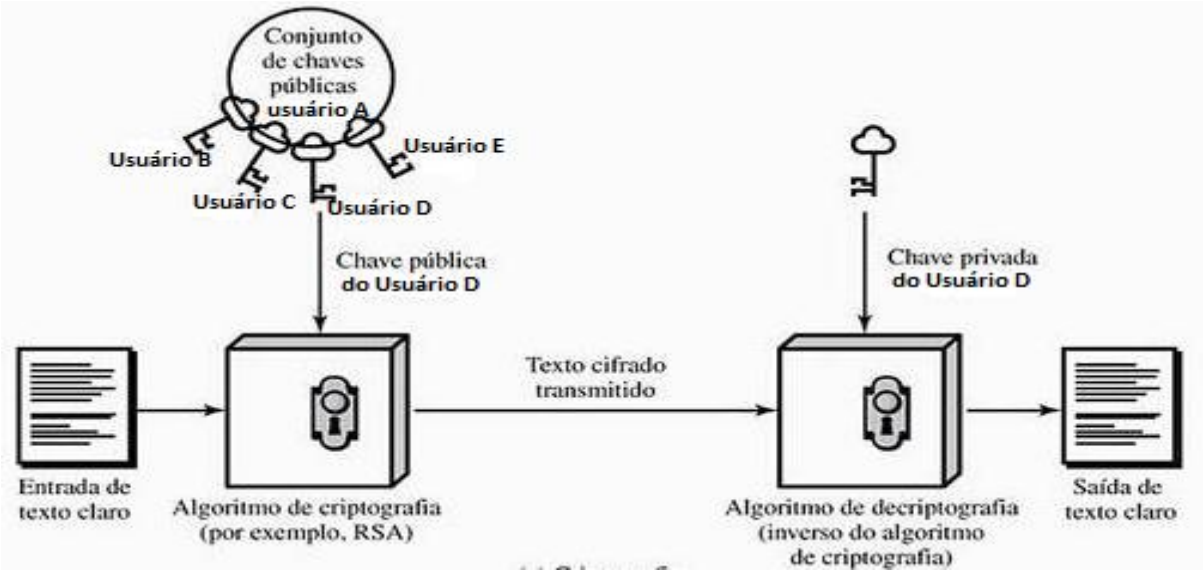


Figura 7 - Processo de criptografia e decriptografia assimétrica.
Fonte: Adaptada de Stallings (2008, p. 184).

Pode-se observar as diferenças entre a criptografia de chave publica (assimétrica) e a criptografia de chave secreta (simétrica) no Quadro 4 conforme Stallings (2008).

	Criptografia de chave simétrica	Criptografia de chave assimétrica
Necessário para funcionar	1 – O mesmo algoritmo com a mesma chave é usado para criptografia e decriptografia. 2 – O emissor e o receptor precisam compartilhar o algoritmo e a chave.	1 – Um algoritmo é usado para criptografia e decriptografia com um par de chaves, uma para criptografia e outra para decriptografia. 2 – O emissor e o receptor precisam ter uma das chaves do par casado de chaves (não a mesma chave).
Necessário para segurança	1 - A chave precisa permanecer secreta 2 - Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível 3 – O conhecimento do Algoritmo mais amostras do texto cifrado precisam ser insuficientes para determinar a chave.	1 – Uma das duas chaves precisa permanecer secreta. 2 – Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível 3 – O conhecimento do algoritmo mais uma das chaves mais amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.

Quadro 4 - Criptografia de chave Simétrica x Assimétrica.
Fonte: Stallings (2008, p. 184).

4.3.3 Vantagens e Desvantagens dos Tipos de Criptografia

Segundo a RSA *Security* (2000) é apresentado comparações das vantagens e desvantagens do uso de cada tipo de criptografia.

Chave Publica tem como principais vantagens o aumento da segurança e praticidade, pois as chaves privadas nunca precisam ser transmitidas ou reveladas a ninguém. Já na criptografia de chave secreta devem ser transmitidas ou divulgadas, pois a mesma é utilizada para criptografia e decriptografia.

Outra vantagem dos sistemas de chaves públicas é poder fornecer assinaturas digitais que não podem ser repudiadas.

Desvantagem do uso da criptografia de chave pública é a velocidade comparada com a criptografia de chave secreta. A criptografia de chave pública pode ser usada com a criptografia de chave secreta para combinar a segurança da chave publica com a velocidade da chave secreta.

Criptografia de chave publica pode ser vulnerável a representação, pois um ataque bem sucedido em uma autoridade de certificação pode permitir que este represente quem ele quiser.

4.4 Sistemas Criptográficos

São considerados sistemas criptográficos um conjunto de algoritmos que implementem criptografia e decriptografia e geração de chaves. A seguir são apresentados os principais sistemas criptográficos.

4.4.1 DES

Em 1972, o *National Institute of Standards and Technology* (NIST) decidiu que era necessário um robusto algoritmo de criptografia para proteger informações secretas. Então foi desenvolvida uma proposta para o algoritmo em questão, o qual deveria ser barato, flexível, facilmente distribuído, e muito seguro.

Em 1974 foi submetido o algoritmo Lúcifer pela IBM, atingindo a maioria das exigências básicas definidas pelo NIST. O Lúcifer incluía 128 *bits* de comprimento. Segundo Thomas (2007) o NIST não possuía conhecimento para avaliar completamente o Lúcifer então foi solicitada ajuda da *National Security Agency* (NSA).

A NSA aconselhou o NIST para que a chave fosse de 56 *bits*, encurtando-a em 72 *bits*. O NIST adotou o algoritmo Lúcifer como padrão em 1976, alterando seu nome para *Data Encription Standard* (DES). No começo de 1977 foi publicada a especificação do algoritmo, o qual se tornou amplamente utilizado em pouco tempo, pois teve apoio oficial do governo.

Segundo Terada (2008) o DES foi projetado para ser implementado em circuito integrado não sendo adequado para implementação em *software*, pois ocorrem diversas

permutações de sequencias longas de *bits* em seu processo, possuindo entrada de 64 *bits*, chave de 56 *bits* utilizando a mesma chave para decriptografia.

Em 1997 o NIST descontinuou o algoritmo DES, lançou uma competição para adotar o seu sucessor, começando a trabalhar no *Advanced Encription Standard* (AES).

4.4.2 Triple DES

Segundo Tanenbaum (2003) em 1979, a IBM percebendo que o tamanho da mensagem do DES era muito pequeno criou uma forma de aumenta-la usando a criptografia tripla. O método utiliza apenas duas chaves e segue um esquema criptográfico de criptografar com a primeira chave, decriptografar com a segunda chave, e criptografar novamente com a primeira chave.

"Única vantagem de utilização da decriptografia na sequência é permitir que usuários do 3DES decriptografem dados criptografados pelos usuários do DES simples" (Stallings, 2008, p. 124). Permitindo a utilização dos dois sistemas criptográficos simultaneamente, sem necessidade de substituir o DES para o 3DES somente por motivo de compatibilidade entre os sistemas.

Segundo Oliveira (2012a) o 3DES pode ser empregado em versões com duas ou três chaves diferentes. A utilização de duas chaves ao invés de três deve-se ao fato de que o uso de 168 bits para chaves, sendo que cada chave possui 56 bits, não teria muito ganho real e causaria *overhead* desnecessário de gerenciar e transportar outra chave. As funções de criptografia e decriptografia do 3DES são mapeamentos entre conjuntos de números de 64 bits.

Oliveira (2012a) também comenta que o algoritmo é seguro, porém é muito lento para ser utilizado como um algoritmo padrão.

4.4.3 AES

Como o 3DES é relativamente lento em software e utiliza um tamanho de bloco de 64 *bits*, era necessário, por motivo de segurança e eficiência um tamanho de bloco maior.

Segundo Tanenbaum (2003) o NIST decidiu que o governo americano precisava de um novo padrão criptográfico para uso não confidencial.

Segundo Stallings (2008) em 1997 o NIST patrocinou um concurso de criptografia, onde pesquisadores do mundo inteiro foram convidados a participar com propostas para um novo algoritmo de criptografia padrão, o *Advanced Encryption Standard,* o qual devia ter um grau de segurança igual ou superior ao 3DES e eficiência bem melhorada.

O AES deveria ter uma cifra de bloco simétrica com um tamanho de bloco de 128 *bits* e suporte para chave de 128, 192 e 256 *bits*, deveria ser possível implementações em *software* e *hardware*, e o algoritmo deveria ser publico.

Tanenbaum (2003) comenta que foram feitas 15 propostas sérias, sendo que em 1998 o NIST selecionou 5 finalistas. Destes 5 finalistas foram feitas conferências e tentativas de encontrar falhas nos algoritmos, sendo que na última conferência ocorreu uma votação nos algoritmos concorrentes. A seguir são listados os cinco algoritmos finalistas e suas respectivas pontuações, segundo Tanenbaum (2003).

- Rijndael (de Joan Daemen e Vicent Rijmen, 86 votos).
- Serpent (de Ross Anderson, Eli Biham e Lars Knudsen, 59 votos).
- Twofish (de uma equipe liderada por Bruce Schneier, 31 votos).
- RC6 (da RSA *Laboratories*, 23 votos).
- MARS (da IBM, 13 votos).

Em 2000, o NIST anunciou que também votou no Rijndael, sendo que em 2001 este se tornou o padrão do Governo dos Estados Unidos publicado como *Federal Information Processing Standard* FIPS 197.

Segundo Stallings (2008) para a avaliação final do algoritmo que seria o vencedor do concurso e se tornaria o novo algoritmo de criptografia padrão foram considerados os aspectos de segurança geral, implementação em *software*, ambiente de espaço restrito, implementação em *hardware*, ataques nas implementações, criptografia versus decriptografia, agilidade de chaves, outras versatilidades e flexibilidades, e potencial para paralelismo em nível de instrução.

O algoritmo escolhido, Rijndael admite tamanho de chaves e de blocos de 128, 192 ou 256 *bits*, podendo ser escolhidos independentemente. Utiliza substituições e permutações empregando várias rodadas, sendo que o número de rodadas depende do tamanho da chave e

do tamanho do bloco. Tanenbaum (2003) afirma que são 10 rodadas para chaves com blocos de 128 *bits*, passando para 14 rodadas para a maior chave e maior bloco. Sendo semelhante ao DES, porém diferentemente deste utiliza *bytes* inteiros nas operações, permitindo implementações eficientes em software e hardware. Conforme Stallings (2008) a especificação do AES utiliza as mesmas três alternativas do tamanho de chave limitando o tamanho do bloco em 128 *bits*.

Oliveira (2012a) afirma que o AES é um dos algoritmos mais populares desde 2006 para criptografia de chave simétrica, e é considerado o substituto do DES, ele é rápido em software e hardware e é relativamente fácil de executar utilizando pouca memória.

4.4.4 RSA

O RSA é um sistema de criptografia de chave publica e foi desenvolvido em 1977 por Ronald Rivest, Adi Shamir e Len Adleman, no MIT, sendo publicado em 1978. Segundo Stallings (2008) o esquema Rivest-Shamir-Adleman (RSA) tem reinado como a técnica de uso geral mais aceita e implementada para este tipo de criptografia. Sendo uma cifra de bloco onde o texto claro e texto cifrado são inteiros entre 0 e n-1, sendo n um número qualquer.

Segundo Tanenbaum (2003) o RSA sobreviveu a todas as tentativas de rompimento por mais de um quarto de século, sendo considerado um algoritmo muito forte. Tendo como desvantagem exigir chaves de pelo menos 1024 *bits* para manter um bom nível de segurança, tornando-o bastante lento.

O RSA baseia-se em alguns princípios da teoria dos números. Segundo Tanenbaum (2003) a segurança do RSA está na dificuldade de fatorar números extensos, pois matemáticos têm tentado fatorar números extensos por 300 anos, descobrindo que com o conhecimento acumulados sugere-se que o problema é extremamente difícil.

Oliveira (2012a) afirma que o RSA é o algoritmo de chave publica mais utilizado, sendo uma das mais poderosas formas de criptografia de chave publica conhecida. Sendo que o RSA tem como premissa a facilidade de multiplicar dois números primos com o objetivo de obter um terceiro, porém a partir desse é muito difícil recuperar os dois números primos. Sendo esta técnica conhecida como fatoração.

> Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia se na dificuldade de fatoração de números grandes. Deste modo, a fatoração representa um limite superior do tempo necessário para quebrar o algoritmo (Oliveira, 2012a, p. 14).

Oliveira (2012a) também comenta sobre um caso da chave RSA ter sido quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, tendo o apoio dos cientistas de mais de 6 países, neste caso a chave quebrada possui o tamanho de apenas 512 *bits*, não sendo do tamanho mínimo para garantir a segurança, a quebra da chave levou cerca de 7 meses e 300 estações de trabalho foram utilizadas para a quebra.

Oliveira (2012a) cita um exemplo de uso do RSA no Brasil, onde este é utilizado pela ICP-Brasil, para emitir certificados digitais, a qual utilizava chave de 2048 *bits* e a partir de 2012 passaram a utilizar chave de 4096 *bits*.

Segundo Tanenbaum (2003) o problema do RSA é que ele é muito lento para codificar um grande volume de dados, porém é muito utilizado para a distribuição de chaves.

4.4.5 Sistemas de Criptografia Baseados em Curvas Elípticas

Conforme descrito na seção que trata do RSA, este é um dos sistemas criptográficos baseados em chave publica mais utilizado. Porém segundo Stallings (2008) o tamanho da chave do RSA tem aumentado nos últimos anos, o que está gerando uma carga de processamento maior sobre as aplicações que o utilizam.

Segundo Stallings (2008) um sistema concorrente começou a desafiar o RSA, a criptografia de curva elíptica (ECC – *Elliptic Curve Cryptography*), sendo que esta tem como atrativo principal oferecer igual segurança se comparado com o RSA com chave muito menor, consequentemente reduzindo o *overhead* do processamento.

Segundo Oliveira (2012a) a proposta de utilização de curvas elípticas para sistemas criptográficos de chave publica foi feita por Neal Koblitz e V. S. Miller em 1985, que implementaram algoritmos de chave pública já existentes usando o domínio das curvas elípticas ao invés de trabalharem no domínio dos corpos finitos.

Uma desvantagem que Stallings (2008) apresenta sobre este tipo de criptografia é que tem havido interesse criptoanalítico contínuo em encontrar pontos fracos na criptografia, desencadeando um nível de confiança no ECC não tão alto quanto ao RSA. Oliveira (2012a) enfatiza que os algoritmos de curvas elípticas atuais, possuem o potencial de serem rápidos, porém em geral são mais lentos que o RSA.

4.4.6 RC4

O RC4 é uma cifra de fluxo que foi projetada por Ronald Rivest para a RSA *Security*, sendo uma cifra com tamanho de chave variável com operações orientadas a *byte*. É baseado no uso de permutação aleatória. Segundo a RSA *Security* (2000) análises mostram que o período da cifra é maior que 10^{100} e que 8 a 16 operações de máquinas são necessárias para cada *byte* de saída, podendo a cifra ser executada muito rapidamente em *software*.

Segundo Stallings (2008) o RC4 foi mantido em segredo comercial pela RSA *Security*, sendo que em setembro de 1994 foi colocado anonimamente na Internet. Sendo um algoritmo simples, onde uma chave de tamanho variável entre 1 a 256 *bytes* é usada para inicializar um vetor de estado de 256 *bytes*. Este vetor de estado em todos os momentos contém uma permutação de todos os números de 8 *bits* de 0 a 255.

Para criptografar e decriptografar é gerado um *byte* a partir do vetor de estado selecionando uma das entradas do vetor em um padrão sistemático, sendo que em cada *byte* gerado as entradas do vetor são trocadas.

Segundo Stallings (2008) e RSA *Security* (2000) o RC4 é usado nos padrões SSL/TLS (*Secure Sockets Layer/Transport Layer Security*), que são definidos para a comunicação entre os navegadores Web e servidores, usado para criptografia de arquivos em produtos como o RSA *SecurPC*, sendo usado também nos padrões de segurança para redes 802.11 WEP e WPA (*WiFi Protect Access*).

Stallings (2008) afirma que foram publicados vários artigos analisando métodos de ataque ao RC4, sendo nenhuma das técnicas práticas contra o algoritmo, mas sim em um de seus utilizadores, o padrão WEP, mas alega que o problema não está no RC4, mas na maneira como as chaves são geradas para uso como entrada no RC4.

4.4.7 RC5

Também projetado por Ronald Rivest para a RSA *Security*, em 1994. É uma cifra de bloco parametrizada com blocos, chave e rodadas variáveis. Segundo a RSA *Security* (2000) são permitidos tamanhos de blocos de 32 *bits* (para experimentação e propósitos de avaliação), 64 *bits* (para usar como substituto para o DES), e 128 *bits*. O número de rodadas pode variar de 0 a 255, enquanto que a chave pode variar de o a 2040 *bits*.

De acordo com a RSA *Security* (2000) há rotinas no RC5. A rotina de expansão de chave, onde a chave secreta é expandida para preencher uma tabela de chave, esta depende do numero de rodadas. A rotina de criptografia consiste nas operações de adição de inteiro, XOR *bit* a *bit*, e rotação variável. Sendo o RC5 simples e fácil de implementar e analisar.

4.4.8 RC6

O RC6 é uma cifra de bloco baseada no RC5, projetada por Ronald Rivest, Sidney, e Yin para a RSA *Security* com o objetivo de atender os requisitos da AES, pois RC6 está entre os cinco finalistas do concurso. Sendo igualmente como o RC5, um algoritmo parametrizado, com tamanho de bloco, tamanho da chave, e número de rodadas variáveis. O tamanho da chave tem como limite máximo o mesmo tamanho do RC5, 2040 *bits*.

Segundo RSA *Security* (2000) as características novas em comparação ao RC5, é a inclusão de multiplicação por inteiro e uso de quatro blocos registros em vez de dois. A multiplicação de inteiro é utilizada para aumentar a difusão conseguida por rodada para diminuir o numero de rodadas e a cifra aumentar a eficiência.

4.4.9 Funções de *Hash*

Segundo Oliveira (2012b) a assinatura digital obtida através da criptografia assimétrica não pode ser empregada de forma isolada sendo necessário o emprego de um mecanismo denominado função *hashing* ou função de *hash*. A função *hashing* gera um valor

pequeno de tamanho fixo derivado da mensagem de qualquer tamanho, oferecendo agilidade e integridade confiável nas assinaturas digitais.

> Serve, portanto, para garantir a integridade do conteúdo da mensagem que representa, por isto, após o valor *hash* de uma mensagem ter sido calculado através do emprego de uma função *hashing*, qualquer modificação em seu conteúdo – mesmo em apenas um *bit* da mensagem – será detectada, pois um novo cálculo do valor *hash* sobre o conteúdo modificado resultará em um valor *hash* bastante distinto (Oliveira, 2012b, p. 22).

Segundo Stallings (2008) a função de *hash* não utiliza uma chave, sendo função apenas da mensagem de entrada, sendo o código de *hash* uma função de todos os *bits* da mensagem oferecendo uma capacidade de detecção de erros. O código de *hash* também é conhecido como síntese de mensagem ou valor de *hash*. As principais funções de *hash* são descritas no Quadro 5 segundo Oliveira (2012b).

Algoritmo	Descrição
SHA-1 (*Secure Hash Algorithm* 1)	- Função de espalhamento unidirecional; - Inventado pela NSA; - Gera valor *hash* de 160 bits; - Funcionamento interno muito parecido com o MD4; - Em 2005, foi descoberto falhas de segurança.
SHA-2 (*Secure Hash Algorithm* 2)	- Difere significantemente do SHA-2; - Projetado pela NSA; - Uma família de duas funções *hash* similares com diferentes tamanhos de blocos: SHA-256 e SHA-512, o qual indica a quantidade de bits;
MD4 (*Message Digest* 4)	- Inventado por Ronald Rivest; - Descoberto algumas fraquezas; - O MD4 não é mais utilizado.
MD5(*Message Digest* 5)	- Inventado por Ronald Rivest; - Função de espalhamento unidirecional; - Gera valor *hash* de 128 bits; - Projetado para ser rápido, simples e seguro.

Quadro 5 - Principais funções *hashing*.
Fonte: Oliveira (2012b).

5 SEGURANÇA EM REDES SEM FIO

Esta seção apresenta os padrões de segurança para redes sem fio disponíveis atualmente.

5.1 Padrões de Segurança para Redes sem Fio

5.1.1 WEP

O *Wired Equivalent Privacy* é um padrão de segurança disponibilizado juntamente com o padrão 802.11 em 1999. O comitê 802.11 disponibilizou o protocolo sabendo de suas limitações, sendo o WEP a melhor opção disponível para a época. “Projetado para tornar seus dados tão seguros como se estivessem em uma rede *ethernet* cabeada” (Thomas, 2007, p. 278).

O WEP utiliza chaves fixas de 64 ou 128 *bits*, com conceito de *Shared Key*, na verdade desses *bits* 24 são do vetor de inicialização (IV) do WEP, restando, no caso do WEP64, 40 *bits* para a chave, ou seja, apenas 5 caracteres de chave e para o WEP128, 104 *bits*, 13 caracteres. Estas chaves devem ser compartilhadas entre os usuários, pois a mesma serve para criptografia e decriptografia dos dados.

O WEP combina o IV com a chave fixa para gerar pseudo-chaves, as quais servem para criptografar os dados. Para cada quadro transmitido é gerada uma nova pseudo-chave, isto torna a criptografia de cada quadro única.

Segundo Nakamura e Geus (2007) o pacote gerado pelo protocolo é composto pelo IV, *byte* de identificação de chave – *Key ID Byte*, algoritmo de integridade CRC-32 e algoritmo criptográfico RC4. O CRC-32 realiza um cálculo sobre os dados a serem transmitidos e gera um resultado ICV (*Integrity Check Value*). O RC4 só é aplicado no *payload* e no ICV, sendo que o IV é transmitido em texto claro.

Segundo Kurose e Ross (2010) o algoritmo RC4 necessita que o mesmo valor de chave nunca seja repetido, porém no WEP como o IV de 24 *bits* muda a cada quadro e estes são escolhidos de modo aleatório, tem-se somente 2^{24} (16.777.216) chaves possíveis, a cada 12.000 quadros a probabilidade de ter sido escolhido o mesmo IV é de 99%.

Pelo fato do vetor de inicialização ser curto, ser transmitido em texto claro e fazer parte da chave de criptografia do RC4, uma chave WEP pode ser quebrada pelos atacantes, para isto basta estes adquirirem um número considerado de quadros e através dos IVs repetidos conseguiram adquirir a chave WEP.

"Diferença entre a criptografia de 64 e 128 bits. A de 128 bits deveria ser duas vezes mais segura, porém ambas utilizam um IV de 24 bits, o qual possui a fraqueza, tornando as duas chaves igualmente fracas" (Thomas, 2007, p. 278).

5.1.2 WPA

O *Wi-Fi Protected Access* foi criado para solucionar os problemas do WEP. Pode ser usado com chaves compartilhadas, como no WEP, ou utilizando o padrão 802.1x, e EAP (*Extensible Authentication Protocol*) que identifica usuários através de certificados digitais. Através do 802.1X pode-se fornecer centralização de autenticação através do RADIUS (*Remote Authentication Dial In User Service*).

O padrão WPA pode ser usado de duas maneiras, *Enterprise* e *Personal.* Na utilização como *Enterprise* é utilizado o padrão 802.1x e EAP para prover autenticação através de um servidor RADIUS, este fica encarregado de fazer a autenticação do usuário, todos os APs presentes na rede estarão associados a este servidor RADIUS, com isso a autenticação ficará centralizada em um único servidor para todos os APs.

Através da utilização de modo *Personal*, a autenticação é feita diretamente no AP com uma chave compartilhada, este tipo é conhecido como WPA-PSK, PSK vem de *Pre-Shared Key*. Para o padrão de chave compartilhada foram adicionadas melhorias em relação ao WEP.

"Utiliza um esquema de criptografia denominado TKIP (*Temporal Key Integrity Protocol*), o qual embaralha todos os *frames* utilizando um algoritmo de *hash*, onde, a cada 10 pacotes, a chave de criptografia é modificada" (Suzin, 2007, p. 48).

Segundo Moraes (2010) o WPA aumenta o IV para 48 *bits*, adiciona MIC (*Message Integrity Code*), derivação e distribuição de chave, e TKIP gerando chaves por pacotes.

O WPA utiliza o protocolo TKIP para criptografia dos dados através do algoritmo RC4, porém tomando algumas preocupações como não enviar a chave em texto claro e trabalha com uma politica de IV mais inteligente. O WPA pode ser utilizado com uma chave secreta entre 32 e 512 *bits*.

> A grande diferença está na maneira com que a chave criptográfica a ser usada pelo algoritmo RC4 é gerada. O vetor de inicialização de 48 *bits* é misturado à chave criptográfica configurada no ponto de acesso e ao endereço MAC da estação transmissora para se obter a chave criptográfica a ser usada pelo algoritmo RC4. Na chave final, apenas 16 dos 48 bits do contador estão disponíveis de forma não criptografada (Farias e Monks, 2010, p. 3).

5.1.3 WPA2

O WPA2 é o padrão IEEE 802.11i na sua forma final, sendo que o WPA é a implementação de parte do padrão. Segundo Caixeta (2012) o WPA2 foi desenvolvido para a obtenção de um nível de segurança ainda maior que no padrão WPA.

Caixeta (2012) afirma que uma grande inovação do WPA2 é a substituição do método criptográfico do WPA, o AES-CCMP. O CCMP (*Counter-Mode/CBC-MAC Protocol*) é um modo de operação em cifragens de bloco, ele evita que a mesma chave seja usada para criptografia e autenticação.

> Os dois modos empregados no CCMP incluem CTR (*Counter Mode*), que realiza criptografia de dados; e CBC-MAC (*Cipher Block Chaining Message Authentication Code*), que provê integridade dos dados. A diferença entre o WPA e WPA2 recai justamente aqui, pois com aquele é requerido, adicionalmente, um mecanismo para integridade dos dados, o MIC (Suzin, 2007, p. 50).

O WPA2, assim como o WPA, suporta modos de operações *Enterprise* e *Personal.* Segundo Caixeta (2012) o 802.11i implementa rede robusta de segurança (RSN – *Robust Security Network*), composta pelo método de criptografia AES e o padrão 802.1x.

5.1.4 IEEE 802.1x

Foi definido pelo IEEE, o 802.1x faz o controle do acesso às redes baseado em portas e distribuição de chaves para as LANS com e sem fio, podendo fazer este controle através de servidores do tipo RADIUS o qual tem o controle baseado em autenticação mútua entre o cliente e a rede.

Segundo Caixeta (2012) o IEEE 802.1x necessita de uma infraestrutura superior aos outros padrões de segurança para o seu bom funcionamento, indicando que este tipo de autenticação é mais utilizada em ambientes corporativos, mas também pode ser usado em ambientes domésticos, configurando o próprio *Access Point* para assumir o papel do servidor RADIUS, desde que este tenha suporte para tal configuração.

É utilizado no padrão WPA e WPA2, resolvendo problemas relativos à autenticação. Segundo Nakamura e Geus (2007) o IEEE 802.1x procura melhorar a segurança com uso do TKIP, e pode ter diferentes métodos de autenticação em diferentes redes, através do uso do EAP descrito na RFC 2284, incluindo geração dinâmica de chaves, autenticação mútua entre clientes e APs, podendo utilizar certificados digitais.

> A autenticação ocorre com a participação de três partes: o suplicante, que é o usuário que deseja ser autenticado, o servidor RADIUS, que realiza a autenticação dos requisitantes e o autenticador, que é quem intermedia esta transação entre as partes citadas inicialmente, papel este designado ao *Access Point* (Caixeta, 2012, p. 28).

Amaral e Maestrelli (2004) apresentam os métodos EAP mais comuns de autenticação:

- EAP-MD5 (*Message Digest* 5): Método de autenticação baseado em senha, raramente utilizado por não garantir um mecanismo eficaz para troca de chaves novas.

- EAP-TLS (*Transport Layer Security*): Requer uso de servidor RADIUS e certificado digital na estação e no servidor.

- LEAP (*Lighweight Extensible Authentication Protocol)*: Autenticação mútua baseada em senha com um servidor RADIUS, constantemente modifica as chaves WEP para impedir que invasores possam descobrir a chave.

- EAP-TTLS (*Tunneled* TLS): Suportado por várias marcas de produtos WLAN, utiliza certificados digitais, mas diferente do EAP-TLS requerem autenticação apenas no servidor RADIUS.

- PEAP (*Protected* EAP): Similar ao EAP-TTLS.

5.2 Comparação entre os Padrões de Segurança para Redes Sem Fio

Segundo Amaral e Maestrelli (2004) o TKIP foi desenvolvido para solucionar as deficiências do WEP, levando em consideração que a maioria dos equipamentos 802.11b utiliza baixo poder de processamento com limitações para grandes processamentos de segurança. O TKIP foi desenvolvido para poder ser utilizado nesses equipamentos sem necessidade de que os mesmos fossem trocados para poder obter uma melhor segurança, bastando atualização do *firmware* do mesmo para poder utilizar este novo método de segurança que foi incorporado no padrão WPA.

O AES foi desenvolvido pensando na maior segurança possível para redes sem fio, visto que as principais deficiências do WEP já haviam sido solucionadas pelo TKIP. Segundo Amaral e Maestrelli (2004) o TKIP não prove o mesmo nível de segurança do AES, e a especificação da IEEE 802.11 descreve que o TKIP é recomendado para atualizações de equipamentos pré-RSN, ou seja, utilizar o WPA como atualização para o WEP principalmente por deficiência de equipamentos que não suportam o AES que necessita de maior poder de processamento.

Amaral e Maestrelli (2004) trazem um comparativo entre as diferenças nos padrões de segurança para redes *wireless*, demostrando a evolução da segurança, o que pode-se observar na Figura 8.

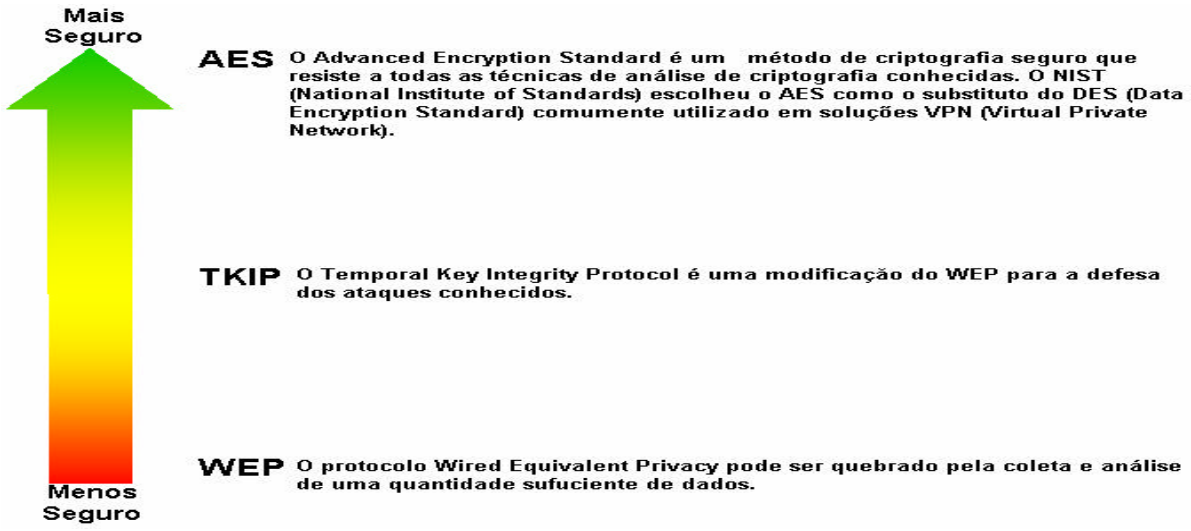


Figura 8 - Comparativo entre os padrões de segurança em redes wireless.
Fonte: Amaral e Maestrelli (2004).

6 DESEMPENHO EM REDES SEM FIO

Esta seção apresenta as principais métricas de desempenho em redes sem fio, bem como as possíveis topologias desta tecnologia.

6.1 Métricas

6.1.1 *Throughput*

O *Throughput* em uma rede de computadores pode ser definido como a vazão da rede, ou seja, é a capacidade total de um canal de transmissão processar e transmitir em um determinado intervalo de tempo. Segundo Suzin (2007), *Throughput* é a taxa de itens processados por unidade de tempo (*bits* por segundo).

O *throughput* pode ser afetado por inúmeros fatores, neste trabalho será feita a analise desta métrica para diferentes padrões de segurança em uma rede 802.11.

6.1.2 *Delay* (Atraso)

É a medida de quanto tempo irá demorar em um *bit* ir de um computador a outro. É interessante medir o *delay* máximo e o médio para as redes de computadores, através dessas medidas poderá ser conhecido o atraso na propagação dos pacotes na rede. Suzin (2007) apresenta o *delay* médio como a medida de tempo de retardo no envio dos pacotes. O *delay* está relacionado com o equipamento e arquitetura da rede em questão.

6.1.3 *Jitter*

O *Jitter* em uma rede de computadores pode ser definido como o tempo entre a chegada dos pacotes. O *Jitter* médio de uma rede de computadores é a variação do tempo entre a chegada de uma série de pacotes.

Segundo Augusto (2002) a variação de atraso corresponde à diferença entre os atrasos na transmissão de pacotes subsequentes e é uma métrica derivada do *delay*.

6.2 Topologia de Redes 802.11

Redes *wireless* podem ser divididas com relação a sua topologia, Redes de infraestrutura e redes *Ad hoc.* A seguir são apresentadas as duas topologias correspondentes a estas redes.

6.2.1 Redes de Infraestrutura

Segundo Moraes (2010) as redes de infraestrutura são controladas pelo *Access Point*, este controla o alcance, nesse tipo de rede a topologia é definida pelo AP, o qual é responsável pela alocação dos recursos.

As redes 802.11 de infraestrutura são redes que dependem de um no central para estabelecerem conexão, este nó é denominado *Access Point* (AP). Segundo Carissimi, Rochol e Granville (2009) um cliente sem fio, ou estação sem fio, para poder se comunicar deve se associar ao ponto de acesso, e que, para poder permitir esta associação, cada AP deve possuir um identificador, um nome, o qual é denominado SSID (*Service Set Identifier*).

“Cada ponto de acesso é ainda configurado para usar um número de canal que corresponde a uma faixa de frequência a ser utilizado na transmissão de dados” (Carissimi, Rochol e Granville, 2009, p. 191). Nas redes de infraestrutura toda a comunicação passa pelo ponto de acesso e os clientes não fazem a comunicação direta um para o outro.

Segundo Thomas (2007) as redes sem fio com modo de operação de infra-estrutura, exigem um *Basic Service Set* (BSS), que é um conjunto básico de serviços para redes sem fio,

ou seja, utilizam um ponto de acesso. Thomas (2007) afirma que o ponto de acesso serve não somente para conexão entre os clientes associados a eles, mas também pode se comunicar a rede cabeada através do ponto de acesso.

"A maioria das WLANs corporativas operam em modo de infraestrutura porque exigem acesso a LAN cabeada para usar serviços como, impressoras e servidores de arquivos" (Thomas, 2007, p. 260).

6.2.2 Redes *Ad hoc*

Segundo Moraes (2010) em redes *Ad hoc* estão interconectados vários dispositivos sem fio, os quais oferecem e gerenciam os serviços, não havendo uma topologia predefinida.

Segundo Stallings (2005) as redes *Ad hoc* são configuradas para serem temporárias, somente para atender necessidades imediatas, por exemplo, durante uma reunião.

As redes *Ad Hoc* não necessitam de um ponto de acesso (AP) para realizarem a comunicação entre si. Segundo Thomas (2007) esse tipo de rede é conhecido como rede ponto-a-ponto e necessita de um *Independent Basic Service Set* (IBSS).

> Cada Computador pode se comunicar diretamente com todos os outros computadores sem fio. Assim eles podem compartilhar arquivos e impressoras, mas são incapazes de acessar recursos da LAN cabeada, a menos que um dos computadores atue como um ponto para a LAN cabeada usando um software especial (Thomas, 2007, p. 261).

7 AMBIENTE DE TESTES

Esta seção irá descrever o ambiente, os equipamentos e os softwares, em que os testes foram realizados.

7.1 Equipamentos

Os equipamentos utilizados para a realização dos testes foram:

- 1 Roteador *Wireless* D-Link modelo DI-524;

- 2 microcomputadores AMD Phenon II X2, 3.00 GHz, 2 GB RAM, com interface de rede Wireless Encore ENLWI-G2 (RTL8185).

7.2 Softwares

O software utilizado para geração de tráfego de rede para os testes foi o Rude e Crude Versão 0.62 (Rude & Crude) disponível sob a licença GPL versão 2. O Rude serve para geração de pacotes UDP (*User Datagram Protocol*) na rede, o Crude serve para a recepção dos pacotes na outra extremidade da rede.

Os pacotes gerados pelo rude são determinados por um *script* de configuração, o qual possui o tempo de inicio do fluxo, uma identidade para o fluxo, tamanho dos pacotes, taxa de transmissão, endereço de destino com porta de destino, e porta de origem. Pode-se observar o *script* de configuração para o tempo de 1 minuto na Figura 9.

```
START NOW
## Fluxo 1: (flow ID = 10)
##
## Inicia o fluxo imediatamente com os seguintes parâmetros:
## 256 pacotes/segundo, cada pacote com 108 bytes
##
## onde:
## TI -> Tempo de inicio do fluxo
## IF -> Identificador do fluxo
## Destino: Porta -> IP de destino com a porta de destino
## pct -> Quantidade de pacotes por segundo
## Tam -> Tamanho dos pacotes
##
## ON -> indica para o fluxo iniciar
## 5000 -> é a porta de origem do fluxo
## CONSTANT -> indica que o fluxo será constante durante todo o tempo estabelecido

#TI  IF           Destino:Porta          Pct Tam
0000 0001 ON 5000 10.1.1.3:40000 CONSTANT 256 108
60000 0001 OFF

## ON -> indica para o fluxo iniciar
## 5000 -> é a porta de origem do fluxo
## CONSTANT -> indica que o fluxo será constante durante todo o tempo estabelecido
##
## Ultima linha contém tempo total da transmissão em milisegundos (60000 = 60 segundos)
## identificador do fluxo com o parametro "OFF" para parar o fluxo imediatamente no tempo estipulado.
```

Figura 9 - Exemplo de script de configuração do Rude, denominado script_testes.cfg

O Crude recebe os dados enviados da conexão correspondente, e ao final mostra informações referentes à transmissão executada, como a perda de pacotes, *delay*, *jitter*, *throughput*, entre outros, conforme Figura 10.

```
crude version 0.62, Copyright (C) 1999 Juha Laine and Sampo Saaristo
crude comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under GNU GENERAL PUBLIC LICENSE Version 2.
^C
Runtime statistics results:
---------------------------

Flow_ID=1
Packets: received=15361   out-of-seq=0   lost(est)=0
Total bytes received=1658988
Sequence numbers: first=0   last=15360
Delay: average = 0.000033   jitter=0.000004   seconds
Absolute maximum jitter=0.003517   seconds
Throughput=27651.7   Bps  (from first to last packet received)
```

Figura 10 - Informações armazenadas pelo Crude.

Nos microcomputadores foi utilizados sistema operacional Linux Ubuntu 10.04 LTS 32bits, configurados igualmentes. Também foi utilizado o software de gerenciamento Cacti.

7.3 Estrutura da Rede do Ambiente de Testes

Foi utilizado a arquitetura de infraestrutura para a realização dos testes, sendo que o roteador *wireless* foi posicionado entre os dois microcomputadores distante 1 metro, conforme Figura 11.

Figura 11 - Estrutura da Rede do Ambiente de Testes.

Os microcomputadores foram conectados a um servidor NTP (*Network Time Protocol*), para que seus relógios fossem sincronizados. Isto se faz necessário uma vez que as medidas de tempo de tráfego coletadas pelo CRUDE se baseiam nos tempos medidos no momento do envio e recebimento dos pacotes.

7.4 Testes Realizados

Foram realizados testes para os seguintes padrões de segurança em redes *wireless*.

- Open (Sem segurança);
- WEP64, chave criptográfica de 40 bits + IV 24 bits;
- WEP128, chave criptográfica de 104 bits + IV 24 bits;
- WPA-PSK TKIP, com chave criptografia de maior tamanho possível (512 bits);
- WPA-PSK AES, com a mesma chave criptografia do teste anterior;
- WPA2-PSK AES, com a mesma chave criptográfica do teste anterior.

Para cada um dos padrões de segurança citados acima foram realizados testes com tempos de duração de 1, 2, 4 e 8 minutos. Os testes foram feitos três vezes para comparar os resultados e obter maior precisão nos resultados obtidos. Ficando cada padrão e respectivo tempo com 3 arquivos de *logs* para realizar a comparação. Totalizando 72 arquivos de *logs* para serem analisados.

Para coleta dos dados é necessário que o *Crude* seja executado antes do *Rude*, a inicialização é feita a partir do *prompt* de comando do Linux, através de comandos específicos.

```
# crude -p 50000 -s 1
# rude -s script_testes.cfg
```

Foram adicionados aos comandos específicos, parâmetros para que os mesmos enviassem os resultados para um arquivo, com o intuito de armazenar *logs* dos testes executados, ficando os comandos assim representados:

echo “## Teste X minutos Padrão XXX” >> recebeTestes.txt | crude -p 10001 -s 10 >> recebeTestes.txt

echo “## Teste X minutos Padrão XXX” >> envioTestes.txt | date >> envioTestes.txt | rude -s script_testes.cfg >> envioTestes.txt

O arquivo envioTestes.txt armazena os dados de envio de fluxo com o tempo do teste e o padrão de segurança, além de obter o horário em que a transmissão iniciou a fim de

verificar com o *software* de gerenciamento Cacti as alterações de utilização de *hardware* dos microcomputadores. Após encerrado o teste em questão, o resultado do Rude fica armazenado no arquivo, conforme Figura 12.

```
## Teste 8 minutos Padrão WEP128
Sex Jun  8 11:49:30 BRT 2012
rude version 0.62, Copyright (C) 1999 Juha Laine and Sampo Saaristo
rude comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under GNU GENERAL PUBLIC LICENSE Version 2.

F_ID: F_START: F_STOP: F_SPORT: F_DADD: F_DPORT: F_err: F_suc: F_seq: F_TYPE: [+ type params]
1  1339166970.535966 1339167450.535966 5000 10.1.1.3 40000 0 122888 122888 CBR [r:256 s:108]
```

Figura 12 - Log de exemplo do rude.

O arquivo recebeTestes.txt armazena os dados recebidos no fluxo com o tempo do teste e o padrão de segurança. Após encerrado o teste em questão, o resultado do Crude fica armazenado no arquivo, conforme Figura 13.

```
## Teste 8 minutos Padrão WEP128
crude version 0.62, Copyright (C) 1999 Juha Laine and Sampo Saaristo
crude comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under GNU GENERAL PUBLIC LICENSE Version 2.

Runtime statistics results:
---------------------------

Flow_ID=1
Packets: received=121679   out-of-seq=0   lost(est)=1209
Total bytes received=13141332
Sequence numbers: first=0   last=122887
Delay: average = 0.910864   jitter=0.000934   seconds
Absolute maximum jitter=0.638943   seconds
Throughput=27376.5   Bps  (from first to last packet received)
```

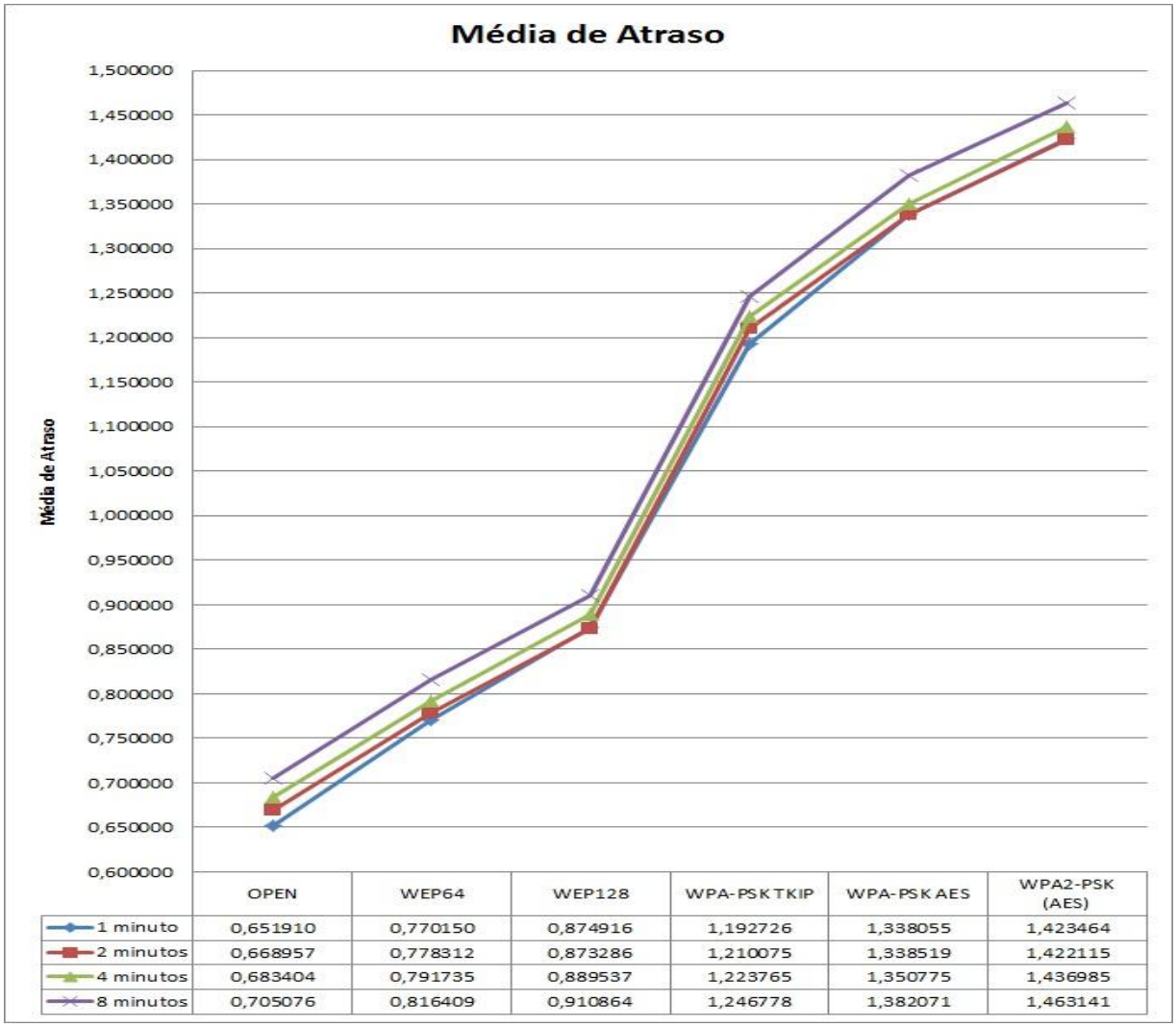
Figura 13 - Log de exemplo Crude.

8 ANÁLISE DOS RESULTADOS

Através da análise e comparação entre os *logs* de cada algoritmo de criptografia pode-se adquirir o *log* adequado para cada padrão de segurança e tempos de testes. Fazendo o comparativo entre as seguranças para redes sem fio, foram analisadas as métricas citadas neste trabalho, que são:

- *Jitter* médio;
- *Jitter* máximo;
- Média de atraso, e;
- *Throughput*.

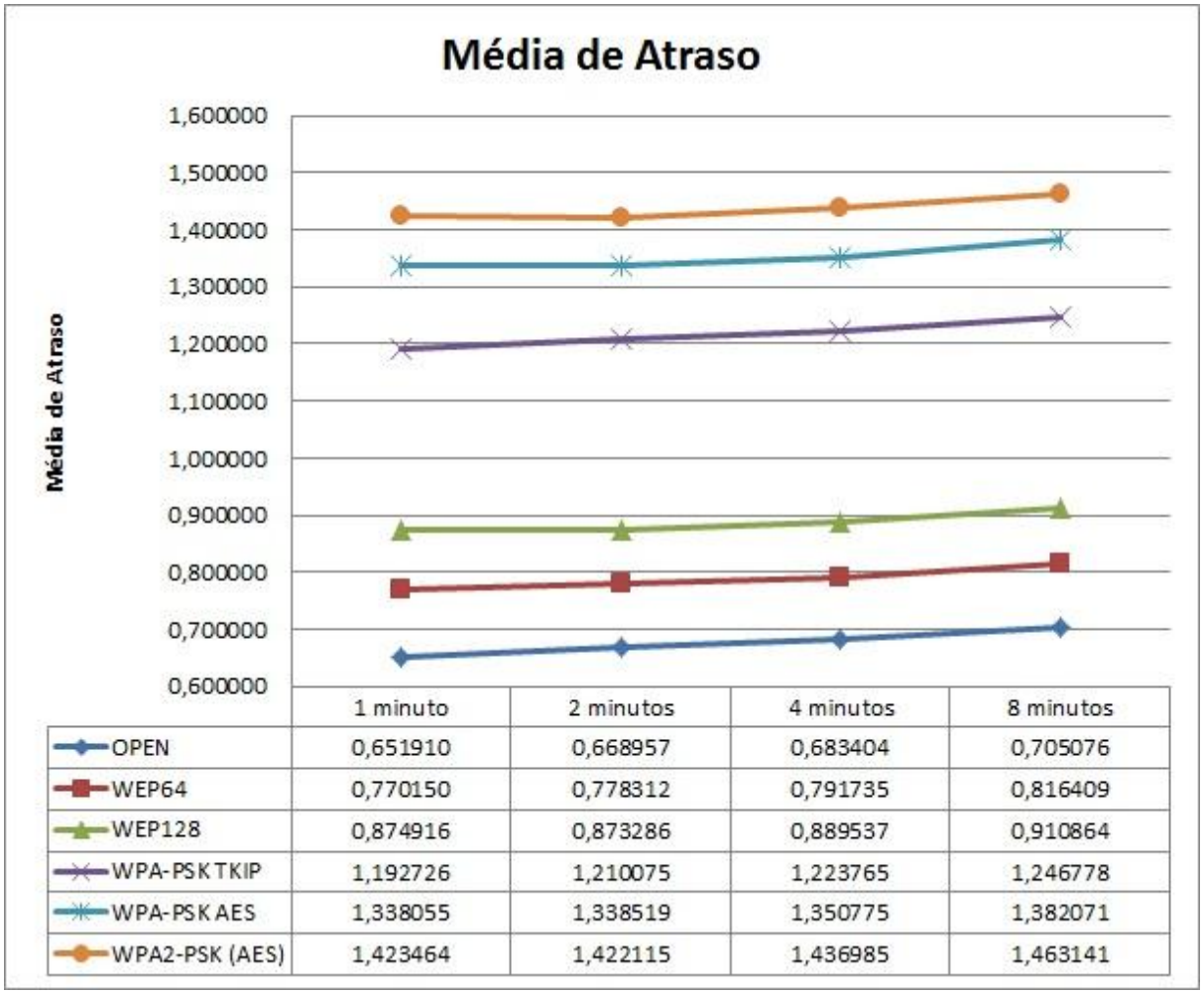
A média de atraso está representada pelo gráfico da Figura 14, através desta pode-se observar que a média de atraso aumenta conforme aumenta o padrão de segurança. Pode-se observar que a maior diferença, considerando os padrões de segurança disponibilizados, está entre o padrão WEP128 para o padrão WPA-PSK TKIP, com aumento de mais de 70% (72,82%) em média para os quatro tempos de teste.



	OPEN	WEP64	WEP128	WPA-PSK TKIP	WPA-PSK AES	WPA2-PSK (AES)
1 minuto	0,651910	0,770150	0,874916	1,192726	1,338055	1,423464
2 minutos	0,668957	0,778312	0,873286	1,210075	1,338519	1,422115
4 minutos	0,683404	0,791735	0,889537	1,223765	1,350775	1,436985
8 minutos	0,705076	0,816409	0,910864	1,246778	1,382071	1,463141

Figura 14 - Média de atraso para os padrões de segurança em função do tempo de coleta.

Na Figura 15 pode-se observar a diferença da média de atraso para cada padrão de segurança nos diferentes tempos dos testes efetuados.



	1 minuto	2 minutos	4 minutos	8 minutos
OPEN	0,651910	0,668957	0,683404	0,705076
WEP64	0,770150	0,778312	0,791735	0,816409
WEP128	0,874916	0,873286	0,889537	0,910864
WPA-PSK TKIP	1,192726	1,210075	1,223765	1,246778
WPA-PSK AES	1,338055	1,338519	1,350775	1,382071
WPA2-PSK (AES)	1,423464	1,422115	1,436985	1,463141

Figura 15 - Média de atraso para cada padrão de segurança.

A Figura 16 mostra o *Jitter* médio em função do tempo de coleta e a Figura 17 mostra o *Jitter* médio para cada padrão de segurança nos diferentes tempos dos testes efetuados.

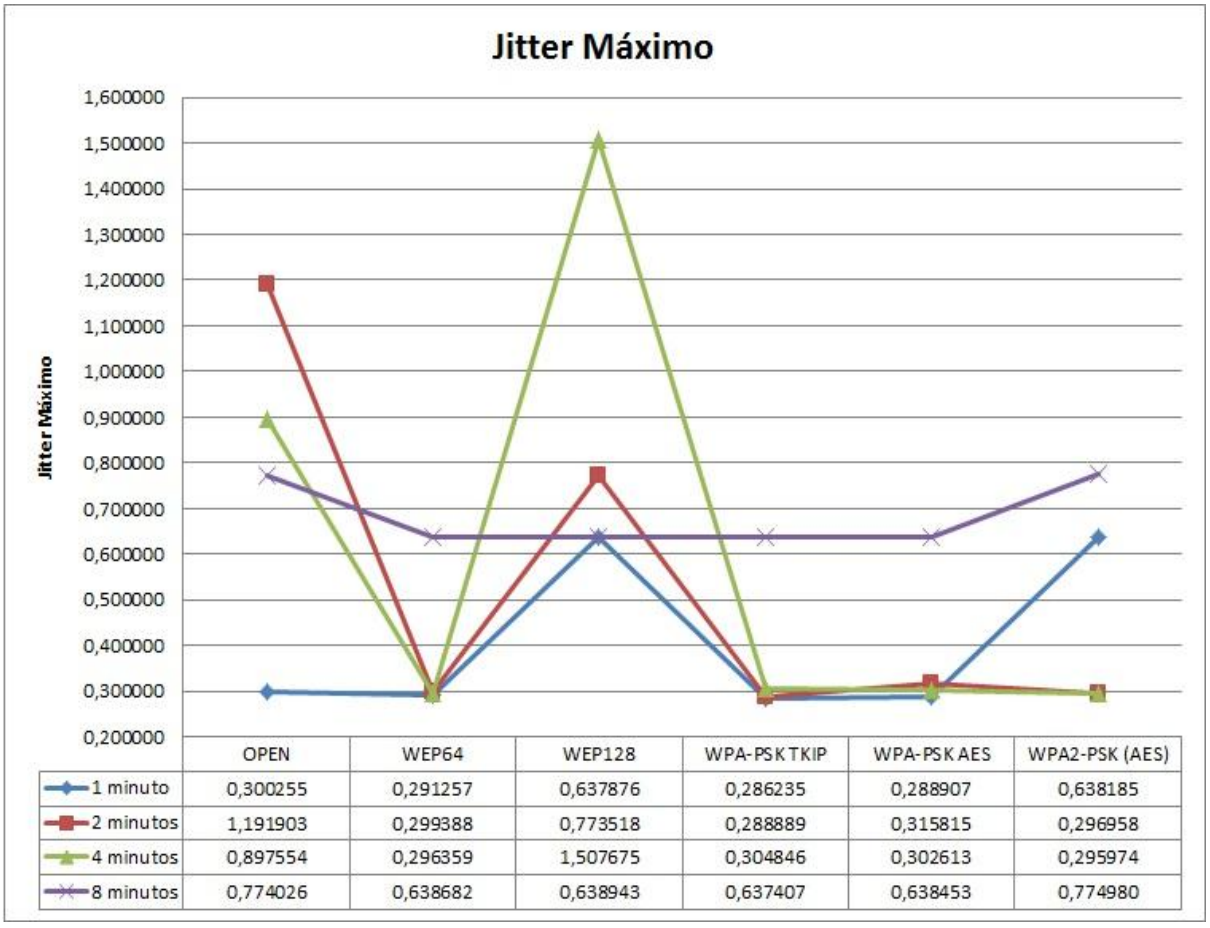
	OPEN	WEP64	WEP128	WPA-PSK TKIP	WPA-PSK AES	WPA2-PSK (AES)
1 minuto	0,000961	0,000903	0,001483	0,001002	0,001446	0,002105
2 minutos	0,000982	0,000854	0,000973	0,000938	0,001008	0,001043
4 minutos	0,000970	0,000908	0,001010	0,001219	0,000938	0,001017
8 minutos	0,000987	0,000943	0,000934	0,001102	0,000942	0,000953

Figura 16 - *Jitter* médio para os padrões de segurança em função do tempo de coleta.

	1 minuto	2 minutos	4 minutos	8 minutos
OPEN	0,000961	0,000982	0,000970	0,000987
WEP64	0,000903	0,000854	0,000908	0,000943
WEP128	0,001483	0,000973	0,001010	0,000934
WPA-PSK TKIP	0,001002	0,000938	0,001219	0,001102
WPA-PSK AES	0,001446	0,001008	0,000938	0,000942
WPA2-PSK (AES)	0,002105	0,001043	0,001017	0,000953

Figura 17 - *Jitter* médio para cada padrão de segurança.

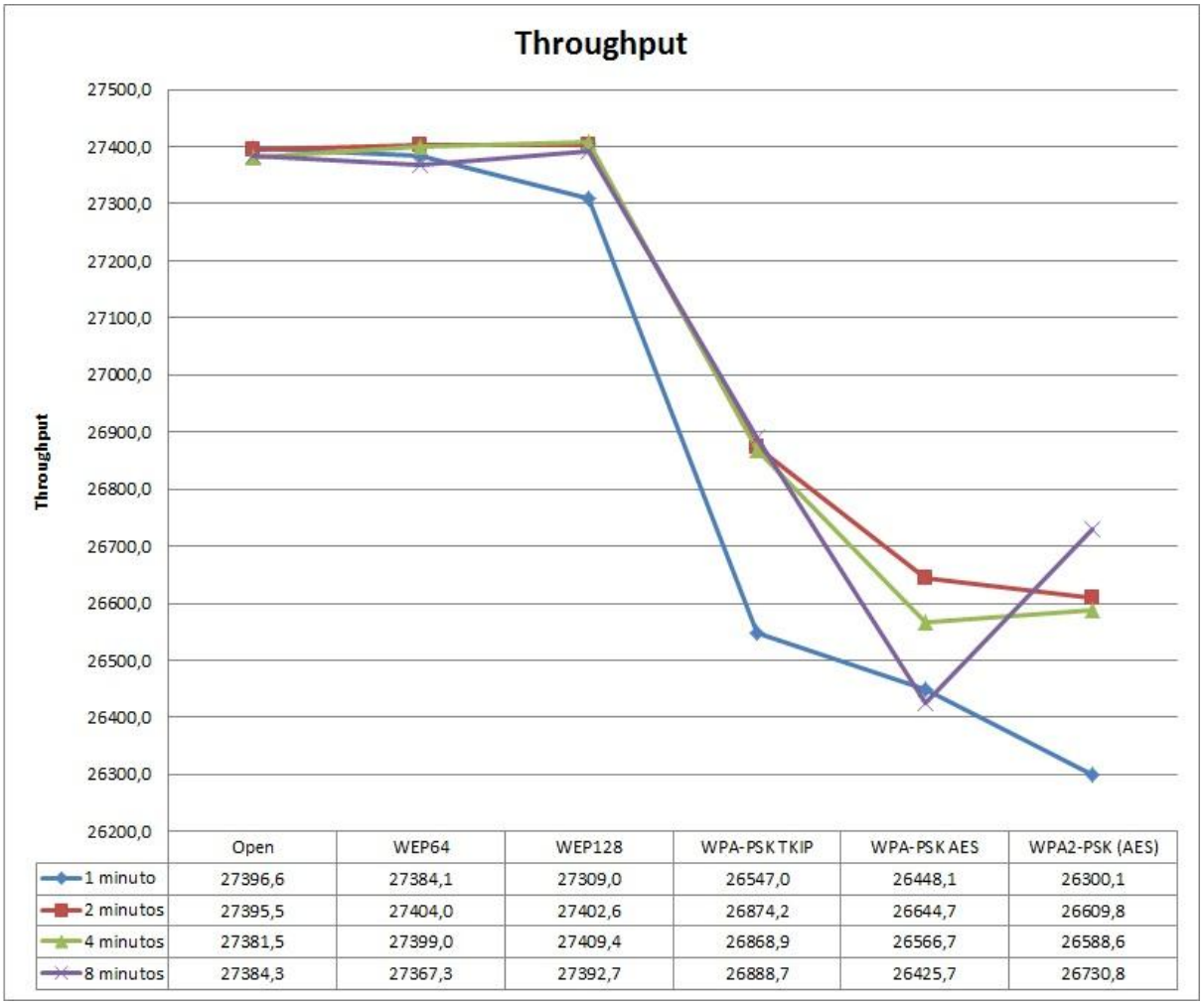
Através da Figura 18 pode-se observar o *Jitter* máximo para os padrões de segurança em cada teste.



	OPEN	WEP64	WEP128	WPA-PSK TKIP	WPA-PSK AES	WPA2-PSK (AES)
1 minuto	0,300255	0,291257	0,637876	0,286235	0,288907	0,638185
2 minutos	1,191903	0,299388	0,773518	0,288889	0,315815	0,296958
4 minutos	0,897554	0,296359	1,507675	0,304846	0,302613	0,295974
8 minutos	0,774026	0,638682	0,638943	0,637407	0,638453	0,774980

Figura 18 - *Jitter* máximo para os padrões de segurança em função do tempo de coleta.

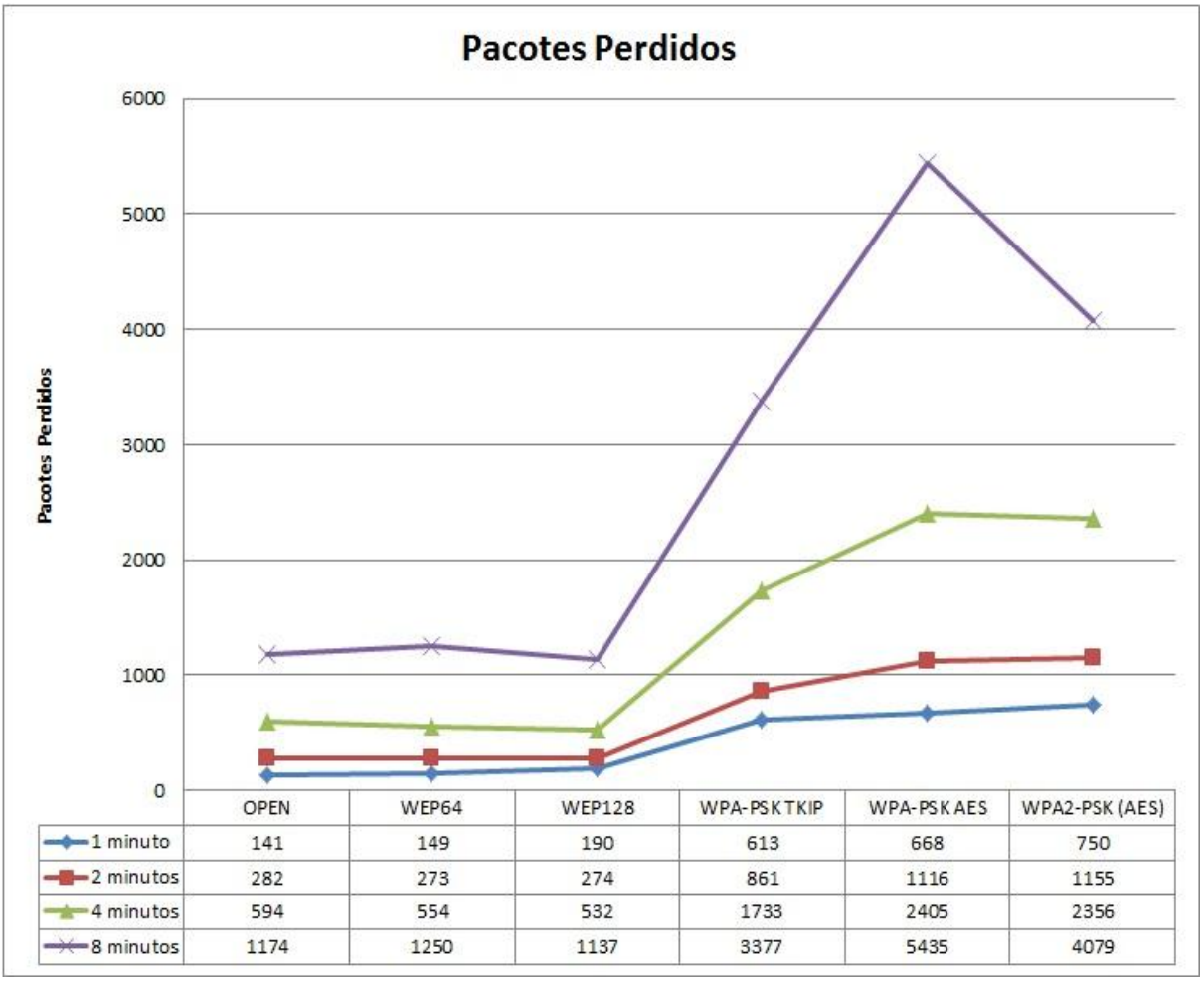
Em relação à vazão da rede, pode-se observar que esta diminui conforme aumenta a segurança, principalmente do padrão WEP128 para o padrão WPA-PSK TKIP, conforme Figura 19.



	Open	WEP64	WEP128	WPA-PSK TKIP	WPA-PSK AES	WPA2-PSK (AES)
1 minuto	27396,6	27384,1	27309,0	26547,0	26448,1	26300,1
2 minutos	27395,5	27404,0	27402,6	26874,2	26644,7	26609,8
4 minutos	27381,5	27399,0	27409,4	26868,9	26566,7	26588,6
8 minutos	27384,3	27367,3	27392,7	26888,7	26425,7	26730,8

Figura 19 - *Throughput* para os padrões de segurança em função do tempo de coleta.

Na Figura 20 pode-se observar a perda de pacotes durante os testes, através desta informação podemos concluir que aumentando o nível de segurança da rede, aumenta também a perda de pacotes nesta rede. Principalmente a partir do padrão de segurança WPA-PSK TKIP. Quanto maior a segurança maior será o poder de processamento necessário para a transmissão dos dados na rede, o que pode-se verificar através do gráfico abaixo.



	OPEN	WEP64	WEP128	WPA-PSK TKIP	WPA-PSK AES	WPA2-PSK (AES)
1 minuto	141	149	190	613	668	750
2 minutos	282	273	274	861	1116	1155
4 minutos	594	554	532	1733	2405	2356
8 minutos	1174	1250	1137	3377	5435	4079

Figura 20 - Pacotes Perdidos para os padrões de segurança em função do tempo de coleta.

8.1 Utilização de Recursos de Hardware nos Diferentes Testes

Conforme mencionado anteriormente, foi utilizado o software de gerenciamento *Cacti* para a verificação da utilização de hardware dos computadores utilizados para a realização dos testes. Para estas informações foi realizada uma nova bateria de testes, nesta somente foi avaliada a utilização dos recursos dos computadores, foram realizados testes de 10 minutos para cada padrão de rede sem fio analisado neste trabalho.

A seguir, na Figura 21, é apresentado o gráfico da carga do sistema para os diferentes padrões de segurança nos computadores gerador e receptor de tráfego.

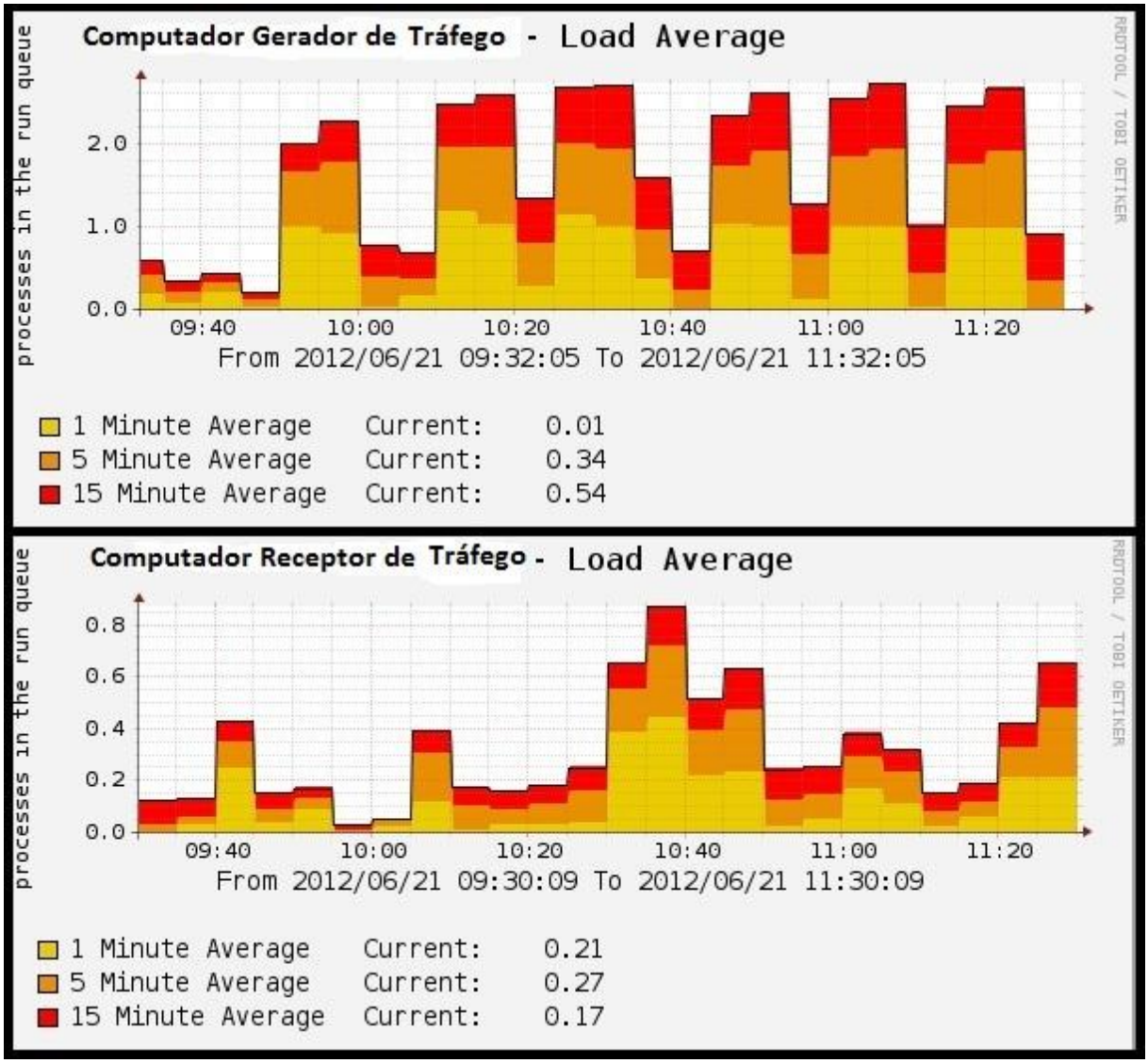


Figura 21 - Comparação entre a carga média do computador transmissor x receptor.

Através da Figura 21 pode-se observar o gráfico da máquina receptora teve variações na carga, entre os testes realizados com os diferentes padrões de segurança para redes sem fio utilizados. Porém não foi possível estabelecer um padrão de utilização do sistema para os tipos de criptografia com maior nível de segurança em relação às de menor nível de segurança. O que pode ser observado na máquina receptora o padrão WEP128 e o padrão WPA-PSK TKIP gerou maior carga de processamento, conforme Figura 22.

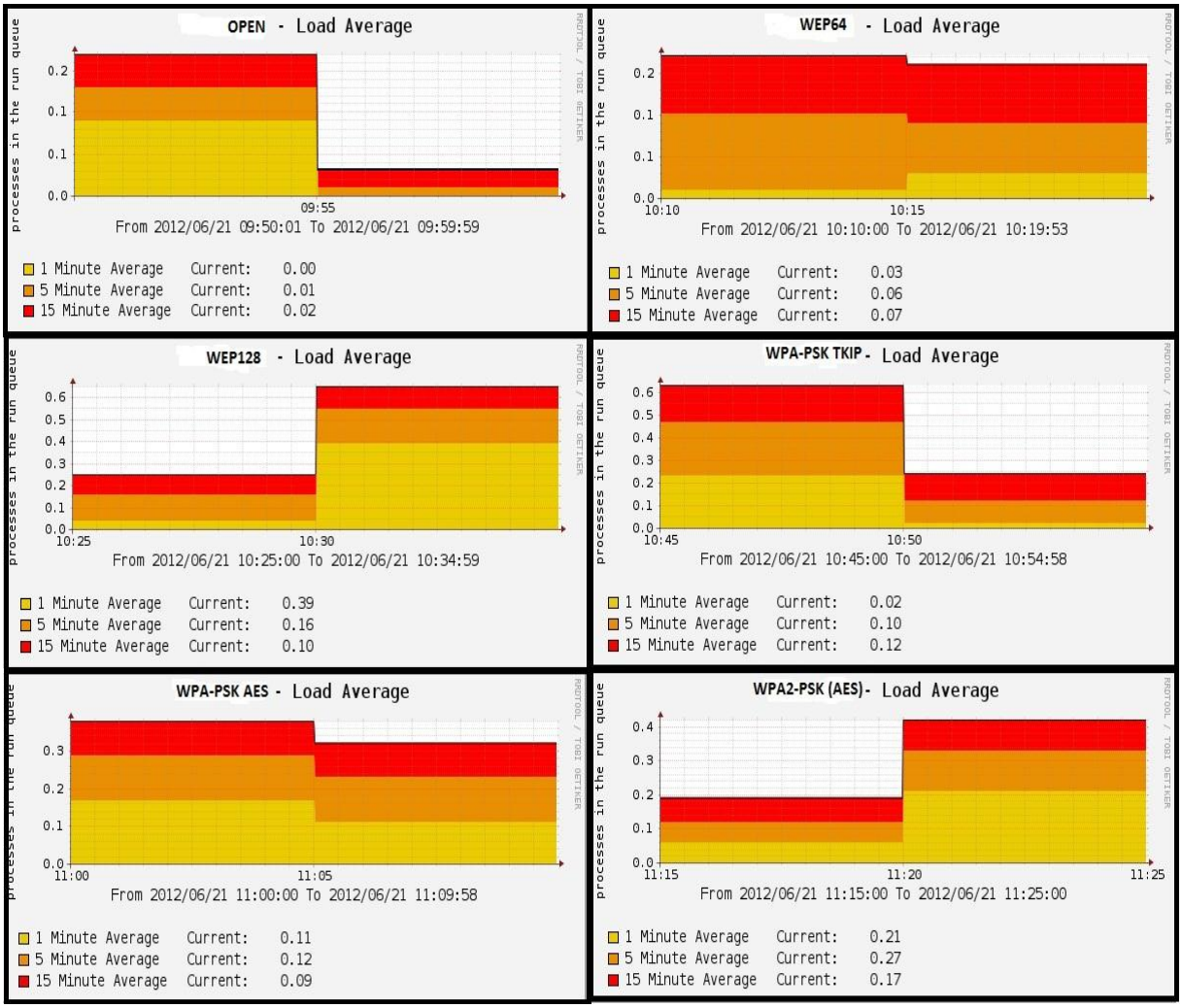


Figura 22 - Carga média para os diferentes padrões de segurança no computador receptor de tráfego.

Em relação ao computador gerador de tráfego, nota-se que praticamente todos os testes dos diferentes padrões de segurança tiveram uma utilização de carga de processamento similar, conforme Figura 23.

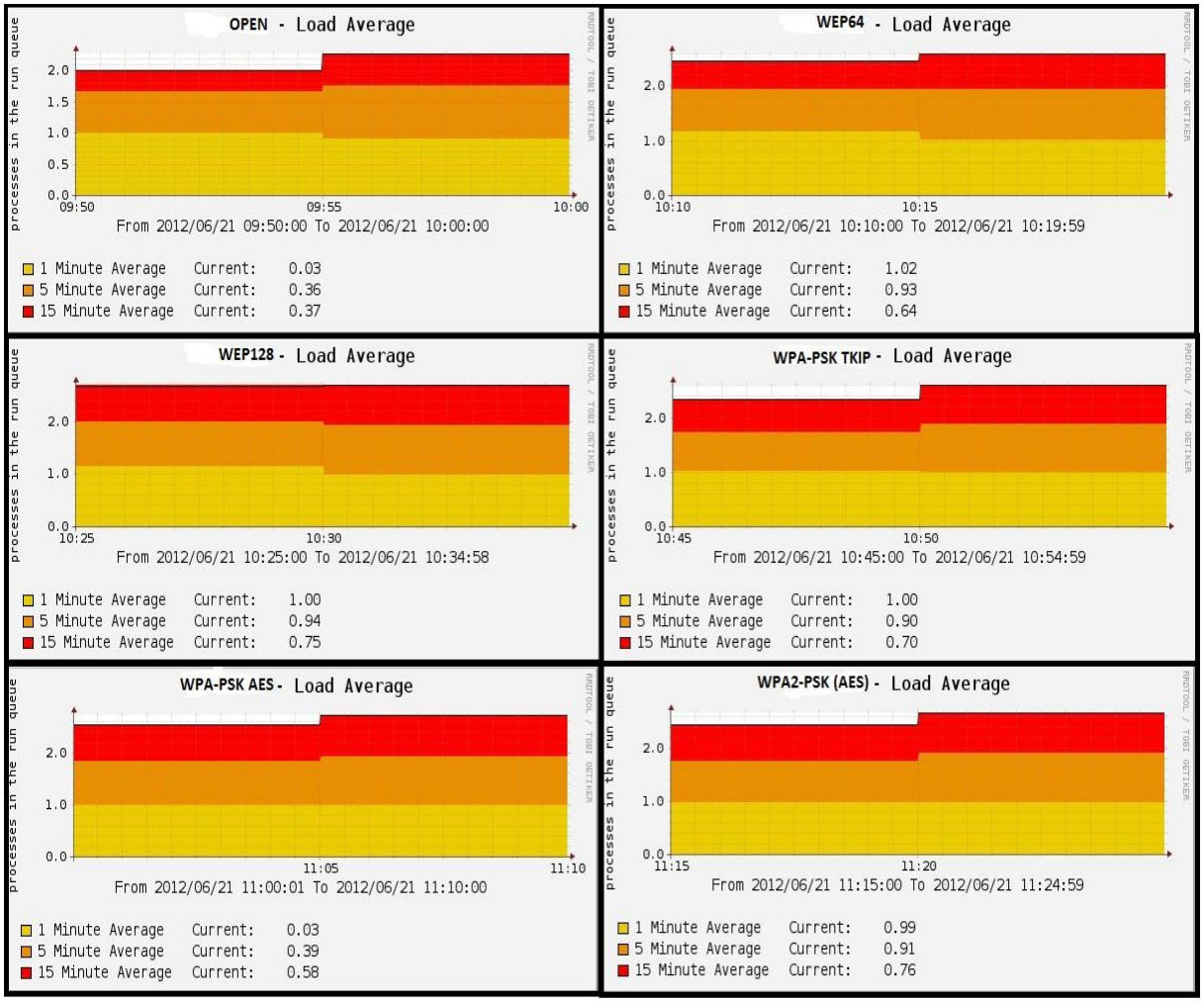


Figura 23 - Carga média para os diferentes padrões de segurança no computador transmissor de tráfego.

Outras métricas referentes ao uso de *hardware*, como memória, não teve alterações significativas em relação aos diferentes padrões de segurança. Infelizmente não foi possível adquirir essas informações referentes ao *Access Point*, pois o mesmo não possuía suporte para coletar informações referentes à utilização de *hardware*.

9 CONSIDERAÇÕES FINAIS

As redes sem fio cada vez mais estão se tornando essenciais para organizações e uso doméstico, visto que a facilidade de mobilidade e conectividade quase que instantânea facilitam o desenvolvimento do trabalho requerido com base em comunicação entre os dispositivos, ou acesso a Internet.

O IEEE vem trabalhado juntamente com fabricantes para desenvolver padrões cada vez mais robustos, aumentando a velocidade e alcance das redes sem fio, sem esquecer da segurança, que é de fundamental importância para a continuidade de adoção deste tipo de tecnologia. Com base em segurança e desempenho destas tecnologias, este trabalho tem fundamental importância para avaliar qual é a melhor solução comercialmente disponível para a melhor adoção.

Este trabalho demonstrou que as redes sem fio com maior segurança tendem a ter um desempenho inferior as redes abertas ou com pouca segurança, pois as mesmas necessitam de um maior poder de processamento para seus algoritmos. Com base nesta informação, os interessados poderão configurar suas redes sem fio, com a configuração que mais se enquadra em seus requisitos para a rede.

Através deste trabalho pode-se comprovar o que foi descrito na seção 5.2, sobre a necessidade de maior processamento nos padrões de segurança que utilizam a criptografia AES, para os padrões que utilizam TKIP e o padrão WEP, visto que através da análise desenvolvida nas seções 7 e 8, pode-se detectar um maior aumento nas métricas de desempenho de redes.

Para trabalhos futuros, poderá ser analisado o desempenho em redes *Ad hoc*, ou fazer variações na rede de infraestrutura, podendo também obter as informações de *hardware* do *Access Point*, ou dos equipamentos presentes na rede. Outro trabalho interessante é analisar o desempenho com diferentes padrões de redes 802.11x, bem como analisar o desempenho do novo padrão que está surgindo, o 802.11ac, e os padrões que irão surgir, pois o IEEE está trabalhando para evoluir as redes sem fio.

10 REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, B. M.; MAESTRELLI, M. **Segurança em Redes Wireless 802.11.** 2004. Disponível em: <http://cbpfindex.cbpf.br/publication_pdfs/nt00204.2006_01_30_22_51_07.pdf>. Acesso em: 30 jun. 2012.

AUGUSTO, M. E. **Avaliação Experimental de Ferramentas para Medição de Largura de Banda**. 2002. 72 f. Dissertação (Mestrado em Informática) – Universidade Federal do Paraná, Curitiba, 2002.

CACTI. **Cacti The Complete rrdtool-based graphing solution.** 2012. Versão 0.8.8. Disponível em: <www.cacti.net>. Acesso em: 20 mai. 2012.

CAIXETA, T. F. G. **Entendendo a Segurança nas Redes sem Fio.** Revista segurança Digital. 4 ed., 2012. Disponível em: < http://segurancadigital.info/>. Acesso em: 10 jun. 2012.

CARISSIMI, A. da S.; ROCHOL, J.; GRANVILLE, L. Z. **Redes de Computadores**. Porto Alegre, Bookman, 2009.

CERT.br. **Estatísticas dos Incidentes Reportados ao CERT.br**. 2012. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 15 mai. 2012.

FARIAS, D. D. de; MONKS, E. M. **Análise de Desempenho versus Segurança em Diferentes Criptografias de Redes sem Fios**. 2010. Disponível em: <http://187.7.106.14/wiki/lib/exe/fetch.php?media=projeto3:dartagnan_projeto5.pdf>. Acesso em: 25 mai. 2012.

IEEE. ***Oficial IEEE 802.11 Working Grupo Project Timelines***. 2012. Disponível em: <http://www.ieee802.org/11/Reports/802.11_Timelines.htm>. Acesso em: 10 mai. 2012.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet:** Uma abordagem Top-Down. 5 ed., São Paulo. Addison Wesley, 2010.

MOONBLINK. **802.11b WiFi Channels**. 2012. Disponível em: <http://www.moonblinkwifi.com/2point4freq.cfm>. Acesso em: 25 abr. 2012.

MORAES, A. F. de. **Redes de computadores:** Fundamentos. 7 ed., São Paulo. Érica, 2010.

NAKAMURA, E. T.; GEUS, P. L. de. **Segurança de Redes em Ambientes Cooperativos.** São Paulo. Novatec Editora, 2007.

NETGEAR. **802.11ac - The next generation WiFi Standard.** 2011. Disponível em: http://www.netgear.com/landing/80211ac/. Acesso em: 23 jun. 2012.

OLIVEIRA, R. R. **Criptografia simétrica e assimétrica (parte 1).** Revista segurança Digital. 5 ed., 2012a. Disponível em: <http://segurancadigital.info/>. Acesso em: 19 jun. 2012.

OLIVEIRA, R. R. **Criptografia simétrica e assimétrica (parte 2).** Revista segurança Digital. 6 ed., 2012b. Disponível em: <http://segurancadigital.info/>. Acesso em: 19 jun. 2012.

RSA *Security*. ***RSA Laboratories' Frequently Asked Questions About Today's Cryptography.*** **Version 4.1**. RSA Security Inc., 2000. Disponível em: http://www.rsasecurity.com/rsalabs/node.asp?id=2152. Acesso em: 16 mai. 2012.

RUDE & CRUDE. Versão 0.62. Disponível em: <http://rude.sourceforge.net/>. Acesso em: 10 mai. 2012.

STALLINGS, W. **Criptografia e segurança de redes:** Princípios e práticas. 4 ed., São Paulo: Pearson Prentice Hall, 2008.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados:** Teoria e aplicações corporativas. 5 ed., Rio de Janeiro. Elsevier, 2005.

SUZIN, C. **Análise de desempenho de protocolos de criptografia em redes sem fio**. 2007. 70 f. Monografia (Graduação em Sistemas de Informação) – Universidade de Caxias do Sul, Vacaria, 2007.

TANENBAUM, A. S. **Redes de Computadores.** 4 ed., Rio de Janeiro: Elsevier, 2003.

TERADA, R. **Segurança de Dados:** Criptografia em rede de computador. 2 ed., São Paulo. Blucher, 2008.

THOMAS, T. **Segurança de Redes:** Primeiros Passos. Rio de Janeiro: Editora Moderna Ltda, 2007.

VAUGHAN-NICHOLS, S. J. **Gigabit Wi-Fi is on Its Way.** 2010. In: IEEE. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05632027>. Acesso em: 12 jun. 2012.