Uma análise de desempenho de protocolos criptográficos na transferência de dados em Redes Sem Fio.

Henrique Valle de Lima[1]
Professor-Orientador: Mário Teixeira Lemes[2]

RESUMO. As redes sem fio apresentam-se cada vez mais presentes no cotidiano da vida moderna. Esta tecnologia agrega valores de mobilidade, rapidez de resposta, e extensões de trabalhos não mais limitados a ambientes físicos. Destarte, todo este conjunto de atributos confronta diretamente à questão da segurança. O objetivo deste artigo é apresentar uma explanação sobre a tecnologia de comunicação sem fio e realizar uma análise do impacto da adoção dos protocolos criptográficos WEP e WPA na transferência dos dados no enlace sem fio.

Palavras-chave: Redes Sem Fio, Segurança, Protocolos Criptográficos.

ABSTRACT. Wireless networks have become increasingly present in everyday modern life. This technology adds mobility values, responsiveness , and extensions work no longer limited to physical environments. Thus, all this set of attributes directly faces the question of security. The objective of this paper is to present an explanation of wireless communication technology and carry out an analysis of the impact of the adoption of cryptographic protocols WEP and WPA on the transfer of data in wireless link .

Key-words: Wireless Network, Security, Cryptographic Protocols.

1. INTRODUÇÃO

A crescente necessidade de manter-se conectado à internet tem levado ao surgimento e aperfeiçoamento de modos de transmissão e comunicação. A transparência e a mobilidade são fatores fundamentais na vivência da experiência. Em corroboro, as Redes sem Fio, ou Wireless, Wifi (*Wireless Fidelity*), ou ainda, WLANs (*Wireless Local Access Network*) ocupam um lugar importante nesta lista, devido aos fatores de mobilidade, flexibilidade, baixo custo e simplicidade de instalação [1]. Destarte, os processos de autenticação e transmissão não apresentem um nível de satisfabilidade confortável, o que acarreta inúmeras vulnerabilidades e riscos inerentes à própria tecnologia.

[1] Pós-graduando do curso Segurança em Redes de Computadores pela Faculdade de Tecnologia SENAI de Desenvolvimento Gerencial (FATESG). henrivalle@gmail.com.

[2] Mestre em Ciência da Computação pela Universidade Federal de Goiás (UFG). mario.lemes@ifg.edu.br.

Alguns sistemas de alta seguridade também enfrentam problemas relativos à tecnologia sem fio. De acordo com os resultados do trabalho conduzido em [2], um estudo de análise de segurança em redes sem fio evidenciou um ponto crítico nos aeroportos internacionais de *Denver* e *San Jose*. A empresa *American Airlines*, uma das maiores do mundo em número de operações aéreas, realizava a transmissão de dados como *check-in*, e tráfego aéreo por meio de uma rede Wifi completamente desprotegida. Durante o teste realizado foram obtidas todas as informações que trafegaram pela rede, resultados estes que deveriam ser de acesso exclusivo da empresa.

A grande vulnerabilidade das redes sem fio está atrelada diretamente atrelada ao próprio enlace sem fio. Uma vez que os dados são transmitidos através de ondas de rádio pelo espaço, qualquer um que tenha acesso físico ao espaço coberto pelas ondas tem a chance de interceptar o conteúdo trafegado [1].

Alguns tipos de sinais das redes sem fio podem alcançar um raio de transmissão de até 3 quilômetros [3, 4], excluindo-se barreiras físicas, e pode-se potencializar a leitura de dados por meio de uma antena de alto ganho [4]. Neste ponto evidencia-se outra característica de vulnerabilidade deste meio de transmissão: não é possível realizar o controle efetivo da amplitude da onda de rádio, tornando-se possível que qualquer pessoa debaixo da cobertura e um pouco de conhecimento técnico tenha acesso aos recursos da rede, ou até mesmo arquivos e processos nela instaurados [4].

A ampla necessidade de segurança neste meio impulsionou a criação de padrões de criptografia e implementação mínimos requeridos à tecnologia. As redes do tipo RFC 802.11 [7] contam com criptografias e modos de autenticação, que garantem que somente pessoas autorizadas tenham acesso ao conteúdo desta rede.

Por se tratarem de protocolos criptográficos, todos os dados que trafegam no meio, devem se submeter ao tipo de criptografia adotado. Este processo pode requerer a utilização de mais capacidade de processamento, uma vez que os dados passam por mais uma etapa antes de seu envio efetivo [5].

O objetivo deste artigo é explanar sobre alguns tipos de vulnerabilidades que cercam a tecnologia de redes sem fio, e ainda, analisar a carga que os processos criptográficos podem acarretar em uma rede do tipo infraestruturada [6]. Mais especificamente, analisar o desempenho de transmissão da rede diante da implementação de alguns processos de segurança específicos em utilização neste tipo de tecnologia.

2. CONCEITOS PRELIMINARES

Esta Seção trata diretamente das normas regulamentadas pelo IEEE (*Institute of Electrical and Electronics Engineers*) acerca da transmissão em redes sem fio, dos padrões, do histórico de desenvolvimento e o tipo de segurança envolta no processo.

2.1. A regulamentação do padrão IEEE 802.11

Todo o processo de gerenciamento de redes não seria efetivamente aplicado sem a presença de um órgão regulador. Neste cenário entra em cena a ANATEL (Agência Nacional de Telecomunicações). Este órgão é responsável por parametrizar e licenciar produtos e tecnologias em utilização no território brasileiro, visando uma unicidade entre as plataformas vigentes. Em corroboro a resolução n.° 506 de julho de 2008, estão licenciados para utilização no Brasil, como equipamentos de rádio comunicação em redes infraestruturadas, três faixas de frequências, sendo a primeira faixa variante de 902 a 928 MHz, a segunda de 2,4 a 2,5 GHz e a terceira dentro da faixa de 5,150 a 5,825 GHz. [7]

As redes do tipo 802.11 utilizam o padrão de transmissão de 2,4 a 2,5 GHz e 5,150 a 5,825 GHz. Nesta faixa de frequência estão contidos a maioria dos aparelhos de comunicação sem fio licenciados e em utilização no Brasil atualmente.

2.2. O padrão IEEE 802.11

Segundo [8], o início da utilização de redes sem fio data-se do início dos anos 90. Nesta época foram produzidos processadores que com maior capacidade possuíam suporte a execução deste tipo de aplicação. Destarte, as redes existentes na época eram patenteadas e incompatíveis, fato que fez que com o IEEE desenvolvesse o modelo de aplicação conhecido como 802.11.

De acordo com [9], a expansão deste tipo de tecnologia foi impulsionada pela facilidade de utilização, dando mobilidade para os utilizadores. Outro fator que impulsionou a tecnologia foi a extinção do antigo meio de trabalho por passagem de cabos de rede. O modo de implementação da tecnologia cabeada tornava-se então mais onerosa quando comparada a tecnologia sem fio.

No período de desenvolvimento da tecnologia três tipos de transmissão entraram em desenvolvimento: a transmissão via rádio frequência, via infravermelho e a laser. [6]

Na transmissão por meio de rádio frequência as ondas podem percorrer longas distancias e adentrar facilmente em meios com barreiras físicas, o que possibilitava que este tipo de comunicação fosse facilmente aplicada tanto em ambientes fechados como abertos. Destaca-se ainda como ponto de vantagem inerente a tecnologia, o fato da distribuição de sinal ocorrer de forma omnidirecionais, ou seja, as ondas viajam em qualquer direção, fazendo com que não haja a necessidade de alinhamento perfeito entre transmissor e receptor [6]. Devido a estes, e outros fatos, a tecnologia de transmissão por meio de rádio frequência sofreu uma maior expansão, em relação as outras duas metodologias propostas.

O padrão 802.11 estabelece normas para a criação e para o uso de redes sem fio. Como dito anteriormente, existem alguns segmentos de frequência que podem ser usados sem necessidade de aprovação direta de entidades apropriadas de cada governo: as faixas ISM (*Industrial, Scientific and Medical*), que podem operar, entre outros, com os seguintes intervalos: 902 MHz - 928 MHz; 2,4 GHz - 2,485 GHz e 5,15 GHz - 5,825 GHz. [6]

2.3. A segurança no padrão IEEE 802.11

O processo de evolução das tecnologias de comunicação resultou em uma única preocupação: como proteger os dados para que pessoas não autorizadas não tenham acesso? O processo de organização da tecnologia envolveu então a criação de métricas de segurança, visando a proteção das informações trefegadas no meio. Dessa forma surgiu o protocolo WEP (*Wired Equivalent Privacy*).

O WEP existe desde o padrão 802.11 *legacy* e consiste em um mecanismo de autenticação que funciona, basicamente, de forma aberta ou restrita por uso de chaves. Na forma aberta, a rede aceita qualquer dispositivo que solicita conexão, portanto, há apenas um processo de autorização. Na forma restrita, é necessário que cada dispositivo solicitante forneça uma chave (combinação de caracteres, como uma senha) pré-estabelecida. Esta mesma chave é utilizada para cifrar os dados trafegados pela rede. O WEP pode trabalhar com chaves de 64 bits e de 128 bits.

A utilização do WEP, no entanto, não é recomendada por causa de suas potenciais falhas de segurança [1, 4, 6, 8]. O WEP faz uso de vetores de inicialização que, com a aplicação de algumas técnicas, fazem com que a chave seja facilmente quebrada. Uma rede utilizando WEP de 64 bits, por exemplo, tem 24 bits como vetor de inicialização. Os 40 bits restantes formam uma chave muito fácil de ser vencida. Mesmo com o uso de uma combinação de 128 bits, é relativamente fácil quebrar todo o esquema de segurança.

Diante deste problema, a Wi-Fi *Alliance* aprovou e disponibilizou o *Wired Protected Access* (WPA). Tal como o WEP, o WPA também se baseia na autenticação e cifragem dos dados da rede, mas o faz de maneira muito mais segura e confiável. [9]

A base do WPA está em um protocolo chamado Temporal Key Integrity Protocol (TKIP), que ficou conhecido também como WEP2. [8] Nele, uma chave de 128 bits é utilizada pelos dispositivos da rede e combinada com o *MAC Address* (um código hexadecimal existente em cada dispositivo de rede) de cada estação. Como cada *MAC Address* é diferente do outro, acaba-se tendo uma sequência específica para cada dispositivo. A chave é trocada periodicamente (ao contrário do WEP, que é fixo), e a sequência definida na configuração da rede (o *passphrase*, que pode ser entendido como uma espécie de senha) é usada, basicamente, para o estabelecimento da conexão.

Apesar de o WPA ser bem mais seguro que o WEP, a Wi-Fi *Alliance* buscou um esquema de segurança ainda mais confiável. Foi aí que surgiu o *802.11i*, que em vez de ser um padrão de redes sem fio, é um conjunto de especificações de segurança, sendo também conhecido como WPA2.[6]

O WPA2 utiliza um padrão de criptografia denominado *Advanced Encryption Standard* (AES) que é muito seguro e eficiente, mas tem a desvantagem de exigir bastante processamento. O uso do WPA2 é recomendável para quem deseja alto grau de segurança, mas pode prejudicar o desempenho de equipamentos de redes não tão sofisticados (geralmente utilizados no ambiente doméstico). [8] É necessário considerar também que equipamentos mais antigos podem não ser compatíveis com o WPA2, portanto, sua utilização deve ser testada antes da implementação definitiva.

3. PROTOCOLOS DE SEGURANÇA

De acordo com [11], a integridade, a autenticidade, a confidencialidade, o não repúdio e a disponibilidade da informação são fatores primordiais para as empresas. Por isto se faz necessário a utilização de criptografia, especialmente quando se refere a um ambiente sem fio.

Em redes sem fio, existem vários métodos para se implementar a segurança. Neste caso, o estudo dirigido abrangerá os protocolos criptográficos WEP e WPA, que se fazem presentes na maioria dos equipamentos em utilização.

Perante a problemática da segurança de dados, necessário se fez, a criação de padrões de criptografia voltados para a computação. Estes padrões deveriam atender a necessidade de restrição de dados somente a pessoas autorizadas. Desta forma, foi proposto um sistema que utiliza chaves para a criptografia das mensagens que trafeguem pela rede, entre o transmissor e o receptor, garantindo que somente estes tenham posse da mensagem transmitida.

A criptografia é provavelmente a melhor ferramenta existente para a autenticação de usuários e transmissão de dados de forma segura. Com um bom nível de criptografia, pode-se garantir que somente pessoas autorizadas tenham acesso a rede, e mais, garantir a seguridade da rede, uma vez que os dados trafegados dificilmente serão interceptados, criando uma camada de privacidade, impedindo que terceiros tomem posse facilmente destes [10].

3.1. WEP

O protocolo WEP foi um dos primeiros métodos em utilização visando proteger o fluxo de dados trafegados pela rede sem fio. Segundo [12], o funcionamento do WEB baseia-se em criptografar os dados trafegados entre os equipamentos, fazendo uso de chaves de criptografia. O protocolo utiliza o conceito de chaves compartilhadas ou *SharedKey* e processa os dados utilizando a mesma chave em ambos os dispositivos. No processo de cifragem é utilizada uma chave de 64 ou 128 bits, dos quais 24 bits correspondem ao vetor de inicialização, que é alterado a cada pacote, de forma aleatória, visando-se um maior nível de proteção para as chaves [13].

O protocolo WEP conta ainda com uma função de detecção de erros, chamada CRC-32. Essa função é responsável por estabelecer uma reação de cálculo da mensagem enviada, também conhecido como ICV (*integrity Check Value*) [14]. Uma vez o receptor de posse da mensagem, o valor da função ICV é checado e comparado, o que permite averiguar se a mensagem sofreu alguma alteração durante sua transmissão.

3.2. WPA

De acordo com [1], o protocolo WPA é uma evolução do protocolo WEP. Segundo o autor, o protocolo WPA apresenta algumas modificações no que tange a possibilidade de autenticação do usuário, utilizando-se do padrão 802.11n e de EAP (*Extensible Authentication Protocol*), podendo ainda ser utilizado com chaves compartilhadas [15].

Como forma de verificação redundante de integridade, o WPA, além de fazer uso do já implementado ICV no WEP, utiliza-se de mais um campo de verificação, denominado MIC (*Message Integrity Check*), que é implementado pelo algoritmo chamado *Michael*.[11]

Diferentemente do WEP que utiliza apenas uma chave para autenticar o usuário e para realizar a criptografia de dados, o WPA apresenta dois grupos de chaves:

- *Pairwise key*: é utilizada para realizar a cominucação direta entre duas estações ou mesmo entre a estação e o *Access Point.* Este cenário caracteriza uma comunicação do tipo *unicast* e tem a necessidade que exista uma chave que seja conhecida apenas pelas duas partes da comunicação;
- *Group key*: é utilizada para comunicações do tipo *broadcast,* ou *multicast,* ou seja, em vias de comunicações onde todas, ou apenas um grupo de máquinas da rede deverão tomar conhecimento da mensagem. Neste tipo de comunicação é necessário que haja uma chave comum a ser conhecida por todos os destinatários da mensagem.

O protocolo WPA foi desenvolvido para trabalhos tanto corporativos quando residenciais. No modo residencial, o WPA-PSK utiliza-se de uma PMK (*Primary Master Key*) que será derivada da própria PSK (*Pre Shared Key),* ou seja, a chave primária (PMK) é derivada a partir da chave secreta (PSK) previamente configurada no Access Point.

Já em ambientes corporativos, a chave PMK sofre uma derivação da MSK (*Master Session Key),* que é uma chave compartilhada no momento da autenticação do 802.11. É importante ressaltar que a chave PMK nunca é utilizada para encripitação ou verificação de integridade de dados, sua finalidade é de gerar chaves temporárias, denominadas PTK (*Pariwise Transient Key).* A PTK baseia-se em um conjunto de chaves formado pelas chaves de criptografia de dados e as chaves de integridade de dados, sendo estas chaves geradas e dadas conhecimentos no processo de 4-*way-hadshake* em ambas as estações utilizantes. Note na Tabela 1 um quadro relacional entre os protocolos WEP e WPA.

Tabela 1. Comparativo de características WEP e WPA [16].

	WEP	WPA
Cifragem	Apresenta falhas; O processo de segurança já foi quebrado por cientistas;	Resolve as falhas apresentadas no WEP;
	Chaves de 64 e 128 bits estáticas, com 24 bits de Vetor de Inicialização;	Utiliza Chaves dinâmicas de 128 bits e uma combinação de sessão de logon;
	Apresenta distribuição manual de chaves;	Realiza distribuição automática de chaves;
Autenticação	Processo apresenta falhas; Autenticação possível somente por meio de dispositivos.	Autenticação baseada no usuário, através da arquitetura 802.11/EAP.

3.3. TKIP

Conhecendo-se a problemática de segurança envolta no padrão WEP, o Protocolo de Integridade de Chave Temporal foi a primeira tentativa de correção de vulnerabilidade do protocolo, e seus desenvolvedores esperavam que o TIKP proporcionasse um nível melhor de segurança ao WEP de maneira provisória, ate que outros métodos de quebras de chaves fossem implementados.

O WEP suporta ao mesmo tempo chaves de criptografia de 64 e 128 bits, enquanto que o TIKP utiliza somente chaves de 128 bits [15]. Tal fato fez que o algoritmo não acrescentasse nível se segurança relativo, uma vez que muitos ataques de criptografia no WEP 802.11 independem do tamanho da chave.

O acréscimo de segurança no TKIP acontece devido a mistura de chaves por pacote e rechaveamento automático. Durante este processo, cada estação recebe uma chave WEP estável, conhecida como chave temporária. De posse da chave, cada estação combina esta chave com seu endereço MAC de 6 bytes, gerando uma nova chave de criptografia, que será única para cada estação, uma vez que o MAC é único. Afim de favorecer o aumento do número de keystreams disponíveis, o TKIP utiliza um vetor de inicialização de 6 bytes, enquanto o WEP utiliza um vetor de 3 bytes [14].

Deste modo, o processo de rechaveamento garante que nenhuma estação tenha uma chave temporal por um período tão grande, capaz de estourar o keystream associado com esta chave e garante ainda que nenhuma estação utilize uma chave temporal por um período suficiente para que um invasor quebre a chave.

3.4. AES

O algoritmo AES, sigla de Padrão de Encriptação Avançado (do inglês "*Advanced Encryption Standard*"), é um algoritmo de criptografia simétrica de cifra de bloco (a entrada deve possuir um tamanho fixo).

O AES, na verdade, foi originalmente proposto por *Vincent Rijmen* e *Joan Daemen*, sendo conhecido como algoritmo Rijndael. Ele sofreu algumas modificações para comportar a encriptação apenas de palavras de 128, 192 e 256 bits [14]. Ele funciona em rodadas, nas quais ocorrem operações de permutações e combinações dos bits. Assim, o algoritmo é eficiente computacionalmente, podendo ser calculado rapidamente.

Em vias práticas, o AES funciona com um bloco fixo e com chaves de tamanho variável. A chave conta com expansão por meio da aplicação do escalonamento de chaves do *Rijndael*.

As operações de criptografia do AES envolvem o rearranjo bidimensional de bytes de 4x4 posições. De modo geral, o algoritmo trabalha com 4 turnos de criptografia:

1. *AddRoundKey*- cada byte do estado é combinado com a subchave própria do turno (RoundKey); cada subchave é derivada da chave principal usando o algoritmo de escalonamento de chaves.
2. *SubBytes*- consiste em uma etapa de substituição não linear onde cada byte é substituído por outro de acordo com uma tabela de referência.
3. *ShiftRows*- realiza uma etapa de transposição onde cada fileira do estado é deslocada de um determinado número de posições.
4. *MixColumns*- opera uma mescla entre os termos das colunas do estado e combina os quatro bytes de cada coluna usando uma transformação linear.

A figura 1 apresenta a esquematização de cifragem envolta no processo do algoritmo AES.

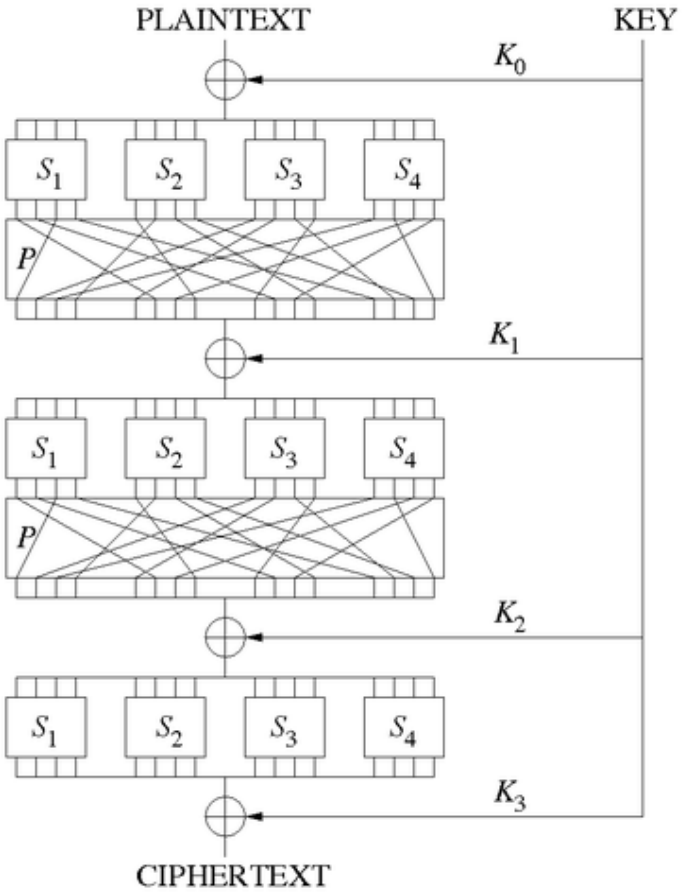

Figura 1. Rotinas de operações do algoritmo AES.

5. ANÁLISE DE DESEMPENHO EM TRANFERÊNCIA DE DADOS NA APLICAÇÃO DE CRIPTOGRAFIA

Esta Seção tem o objetivo de criar um comparativo, por meio de uma situação real de transmissão de dados com, e sem a aplicação de protocolos criptográficos. Tal processo permitirá realizar uma análise de desempenho e impacto na transmissão por meio do emprego das tecnologias de criptografia.

Para tal, realizar-se há a criação de um arquivo de tamanho específico (400 Mb), por meio do comando “dd if=/dev/zero of=/tmp/arquivo.img bs=400000 count=100”. Este comando criará o arquivo “arquivo.img”, que será usado para envio de uma estação a outra, por meio da rede sem fio.

Para a realização da análise de impacto na transmissão por meio da implementação de criptografia, utilizar-se-á dos parâmetros de velocidade de transmissão em consonância com o tempo gasto no decorrer da operação. Para o caso da aferição de de velocidade na transmissão dos dados, utilizar-se-á do gerenciador *Iperf*. Este gerenciador apresentará uma taxa média durante o processo de transmissão entre as estações, para cada um dos casos supracitados. A função de tempo será parametrizada pela funcionalidade *time* nativa do Ubuntu, apresentando como resultado final, o tempo decorrido em todo o processo de transferência de dados.

Deste modo estancia-se o seguinte cenário:

- **Computador 1:** Dell Inspiron – 1TB de disco rígido, 8 Gigabytes de memória RAM, Processador Intel Core i7 2.2GHz, Sistema Operacional Ubuntu 14.10 Live.
- **Computador 2:** Sony VAIO – 512 GB de disco rígido, 4 Gigabytes de memória RAM, Processador Intel Core i3 2.2GHz, Sistema Operacional Ubuntu 14.10 Live.
- **Modem WIFI:** TP-Link TL-WR740N.

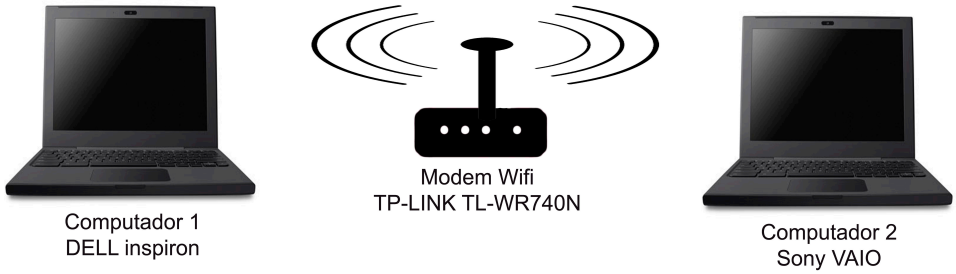

Figura 2. Cenário para transmissão dos dados.

Dando-se a execução dos testes, a Tabela 2 apresenta as tomatadas de velocidade de transmissão de dados.

Tabela 2. Taxa de transmissão de dados (Mb/s).

Taxa de velocidade de transmissão de dados			
	Rede Aberta	**Segurança WEP**	**Segurança WPA**
1	27,1	26,7	24,8
2	29,9	24,3	25,7
3	28,8	25,9	26,1
4	23,9	27,7	24,2
5	29,2	28,1	24,9
6	25,4	26,3	22,3
7	26,9	25,5	21,4
8	26,1	27,3	25,2
9	27,4	26,8	28,3
10	25,9	25,9	26,9
Média	**27,06**	**26,45**	**24,98**

A Figura 3 apresenta a análise gráfica da velocidade de transmissão de dados.

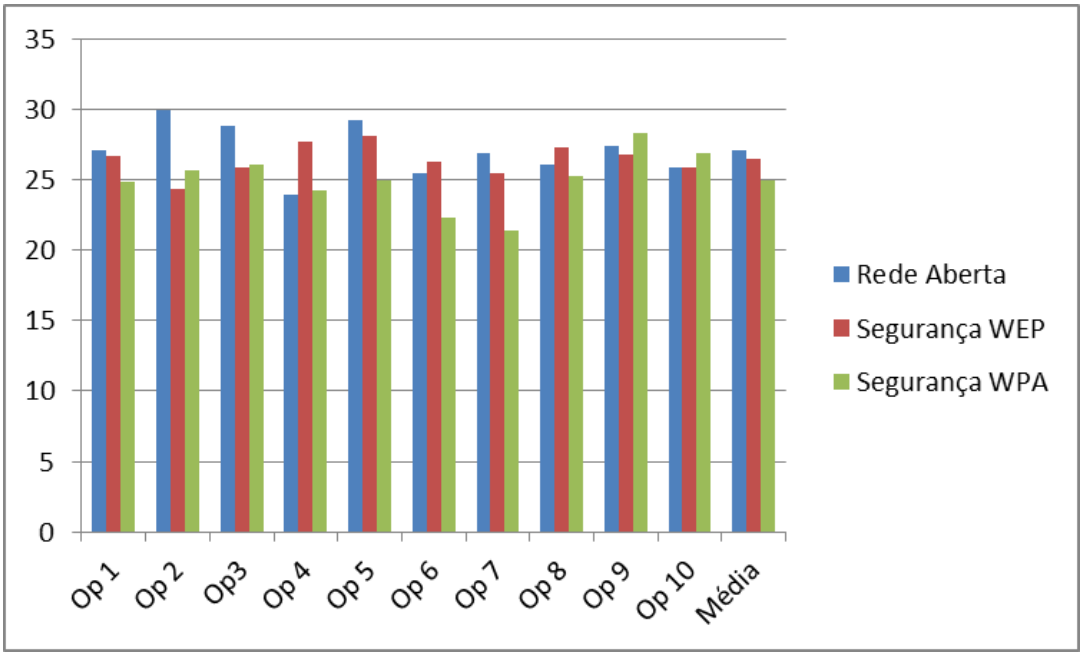

Figura 3. Gráfico comparativo de transmissão de dados.

A Tabela 3 apresenta a velocidade média (para as 10 vezes executadas) de transferência de arquivos para cada um dos 3 casos.

Tabela 3. Velocidade média de transferência do arquivo (s).

Velocidade média de transferência do arquivo			
	Rede Aberta	**Segurança WEP**	**Segurança WPA**
Média	15,1946141	15,49763061	16,4616

A Figura 4 apresenta a análise gráfica da média de tempo na transmissão do arquivo.

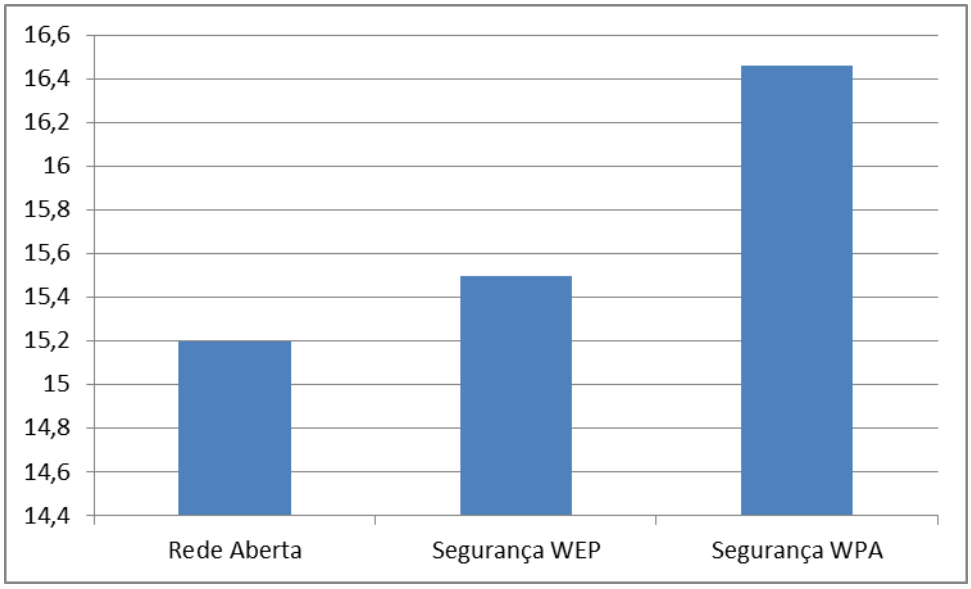

Figura 4. Gráfico comparativo de velocidade média de transmissão de dados.

A Tabela 4 apresenta a relação percentual de acréscimo, ou seja, o custo adicional de tempo quando comparado a Rede Aberta, para os modos de segurança WEP e WPA.

Tabela 4. Velocidade média de transferência do arquivo (s).

Velocidade média de transferência do arquivo		
	Segurança WEP	**Segurança WPA**
Rede Aberta	1,96%	7,70%

6. CONCLUSÃO

As redes Wireless vêm de encontro às necessidades essenciais de pessoas que visam realizar atividades com mobilidade aliada a produtividade. Entretanto, no que tange a segurança, a tecnologia apresenta alguns riscos, quando utilizada de forma indiscriminada.

Dentro do proposto, concluiu-se que o protocolo WEP foi uma solução que adotava os mesmos princípios utilizados na meio de transmissão cabeada, onde não se fazia de grande solicito o alto nível em recursos computacionais. Contudo, diversas falhas foram identificadas neste protocolo, tanto no aspecto de integridade, como no processo de autenticação.

Este nível de falhas impulsionou então os engenheiros do IEEE a apresentarem uma solução mais aceitável, por meio da implementação do protocolo WPA, que se apresentou corrigindo as principais falhas do seu antecessor. É notório o fato de que não existem redes wireless com total seguridade, mas os padrões em aplicação permitem a implementação de níveis aceitáveis de segurança no processo de transmissão de dados.

No quesito criptográfico, por meio de análise a Figura 3, pode-se concluir que os processos de criptografia aplicados trazem pouco, ou até mesmo quase nenhum impacto no desempenho da transferência de dados no quesito velocidade de transmissão de arquivos. Pode-se perceber que o uso de técnicas de segurança e criptografia como WEP ou WPA agregam valor a tecnologia, sem criar um peso de processamento computacional demasiadamente grande.

A figura 4 apresenta um comparativo entre os tempos médios requeridos para efetuar a operação. Por meio dela conclui-se que o impacto de tempo não se faz tão significativo para arquivos de pequeno e médio porte que transitem pela rede.

Por fim, a tabela 4 apresenta uma relação de acréscimo de desempenho com o uso da tecnologia em comparação a utilização de nenhuma métrica de segurança. Perante os testes efetuados, pode-se concluir que a utilização da tecnologia mais aceitável hoje, a WPA, acarreta em uma carga de apenas 7% em cima do desempenho da rede. Esta pequena porcentagem pode ser aceitável uma vez que dificilmente seriam percebida esta sobrecarga em utilizações cotidianas. Tal fato pode influenciar diretamente na tomada de decisões de uma pessoa que procure um modo de trabalho aceitável em associação dos quesitos de mobilidade aliada a segurança.

7. REFERÊNCIA BIBLIOGRÁFICA

[1] RUFINO, N. M. de O.; **Segurança em Redes sem Fio**; São Paulo; Novatec; 2ª ed.; 2005.

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

[3] ENGST, A. E.; FLEISHMAN, G.; **The Wireless Networking: Starter Kit**; – 2ª ed. Pearson Makron Books; 2003;

[4] MORIMOTO, C. E.; **Redes, Guia Prático**; Porto Alegre; Sul Editores; 2008.

[5] MORIMOTO, C. E.; **Servidores Linux, Guia Prático**; Porto Alegre; Sul Editores; 2008.

[6] TANENBAUM, A. S.; WETHERALL, D. J.; **Computer Networks**; 5ª ed.; Prentice Hall; 2008.

[7] http://www.anatel.gov.br/legislacao/resolucoes/2008/104-resolucao-506#art2. Acessado em agosto/2015.

[8] HAYKIN, S. E.; MOHER, M.; **Modern Wireless Communications**; New York; Always Learning; 2007.

[9] BROSKY, I.; **A Manager´s Guide to Wireless Networking. Wireless Computing**; New York; van Nostrand Reinhold; 1997.

[10] FLICKENGER, C.; et. Al.; **Redes Sem Fio no Mundo em Desenvolvimento: um Guia Prático para o Planejamento e a Construção de uma Infraestrutura de Telecomunicações**. 2 ed.; Grupo Central; 2007.

[11] MORENO, E. D.; PEREIRA, F. D.; CHIARAMONTE, R. B.; **Criptografia em Software e Hardware**; São Paulo; Novatec; 2005.

[12] BRAGA, R. R.; **Estudo e Análise dos Protocolos de Segurança em Redes Sem Fio 802.11 e suas Vulnerabilidades**; Parque Tecnológico de Itaiupú; Uberlândia; 2006.

[13] KABARA, J.; et al. **Information Assurance in Wireless Networks**; Department of Information Science and Telecomunications; University of Pittsburgh.

[14] SCHNEIER, B.; **Applied Cryptography. Second Edition: Protocols, Algorithms, and Source Code in C**; John Wiley & Sons Inc; 1996.

[15] BORISOV, N.; et. Al. **Security of the WEP Algorithm**; New York; Vostra; 2009;

[16] VACCA, J. R.; **Guide to Wireless Network Security**; New York; Springer Science Business Media; 2006.