ANÁLISE DE DESEMPENHO DE REDES SEM FIO COM DIFERENTES PROTOCOLOS DE CRIPTOGRAFIA

Douglas Pegoraro Stangarlin, Walter Priesnitz Filho
UFSM
{douglas, walter}@redes.ufsm.br

***Resumo*—Este trabalho apresenta o estudo e desenvolvimento de uma análise de desempenho de redes sem fio IEEE 802.11, também conhecida como WiFi, levando em consideração os diferentes padrões de segurança existentes comercialmente para esta tecnologia. O trabalho foi desenvolvido em um ambiente controlado, em uma rede do tipo infraestrutura, considerando a análise dos padrões de segurança em diferentes tempos de testes. Os testes foram executados, sobre o protocolo de transporte UDP, a fim de comparar o desempenho conforme os diferentes padrões de segurança são utilizados.**

I. 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.

As questões de desempenho e segurança são vitais em redes de computadores. Em se tratando de redes sem fio estas questões são ainda mais importantes, 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 com fio. Uma vez 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.

Para tentar solucionar esta fragilidade é necessário o uso de mecanismos de segurança como cifragem e criptografia. Segundo Stallings [1] a cifragem é a transformação dos dados em um formato que não seja prontamente decifrável através de algoritmos matemáticos, tais procedimentos (transformação e recuperação dos dados) dependem de um algoritmo e zero ou mais chaves criptográficas. Em seu trabalho/estudo Stallings [1] enfatiza que a ferramenta automatizada mais importante em segurança de redes e comunicações é a criptografia.

A criptografia em uma rede de computadores requer utilização da largura de banda da mesma e processamento extra. Como descrito em Stallings [1], 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 este processo que o pacote é considerado transmitido com sucesso.

Existem trabalhos relacionados que comprovam que a criptografia interfere no desempenho dos sistemas computacionais e das redes sem fio, podemos citar o traballho de Suzin [2], o qual traz uma análise de desempenho em redes sem fio com o padrão de segurança OPEN até o WPA (*WiFi Protect Access*). Através dos testes realizados, Suzin [2] constatou que a utilização de um protocolo de criptografia mais robusto, como o WPA, demanda um maior poder de processamento e largura de banda da rede, em função do nível de segurança requerido. Já no trabalho de Barka e Boulmalf [3] são analisados os impactos do uso de criptografia em uma rede de infraestrutura 802.11g, demonstrando que a utilização do padrão de segurança WEP utilizando a criptografia RC4 interfere na vazão da rede em comparação a não utilização de criptografia.

Neste trabalho é feita uma análise e apresentação de quanto os protocolos de criptografia interferem no desempenho de uma rede sem fio, demonstrando estudos sobre o desempenho com os diferentes protocolos de criptografia disponíveis comercialmente na atualidade.

Este trabalho está estruturado como descrito a seguir: Na seção II são apresentados os padrões de segurança existentes atualmente e suas comparações. A seção III traz a metodologia utilizada para a realização dos testes deste trabalho, trazendo o ambiente de testes utilizado, os tipos de testes efetuados e apresentando as métricas de desempenho utilizadas para medir desempenho da rede. A seção IV traz os resultados dos testes efetuados, já a seção V traz as conclusões referentes ao trabalho.

II. REVISÃO TEÓRICA

Para solucionar problemas de segurança em redes sem fio o IEEE (*Institute of Electrical and Electronics Engineers*), comitê responsável por padronizar as redes sem fio 802.11, definiu alguns padrões de segurança para serem utilizados nesta tecnologia.

A seguir são apresentados os padrões de segurança existentes e comercialmente disponíveis no Brasil.

A. Padrão de Segurança WEP

O *Wired Equivalent Privacy* (WEP) 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. Segundo Thomas [4] o WEP foi desenvolvido com objetivo de tornar os dados trafegados tão seguros como se estivessem em uma rede Ethernet cabeada.

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.

B. Padrão de Segurança WPA

O *Wi-Fi Protected Access* (WPA) 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.

Segundo Suzin [2] o WPA incorpora um esquema de criptografia denominado TKIP (*Temporal Key Integrity Protocol*), este embaralha os *frames* utilizando um algoritmo de *hash* que modifica a chave criptográfica a cada 10 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 política de IV mais inteligente. O WPA pode ser utilizado com uma chave secreta entre 32 e 512 *bits*.

C. Padrão de Segurança 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 [5] o WPA2 foi desenvolvido para a obtenção de um nível de segurança ainda maior que no padrão WPA.

Caixeta [5] afirma que uma grande inovação do WPA2 é a substituição do método criptográfico do WPA pelo método AES-CCMP (*Advanced Encryption Standard*). 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.

D. Comparação entre os Padrões de Segurança para Redes Sem Fio

Segundo Amaral e Maestrelli [6] 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 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 [6] o TKIP não provê o mesmo nível de segurança do AES, e a especificação da IEEE 802.11 descreve que o TKIP é recomendado para atualizações de equipamentos fabricados antes da publicação do padrão WPA2 (equipamentos pré-RSN - *Robust Security Network*), ou seja, utilizar o WPA como atualização para o WEP, principalmente por deficiência de equipamentos que não suportam o AES, e que necessita de maior poder de processamento.

O trabalho de Amaral e Maestrelli [6] traz um comparativo entre as diferenças nos padrões de segurança para redes *wireless*, demostrando a evolução da segurança, o que se pode observar na Figura 1.

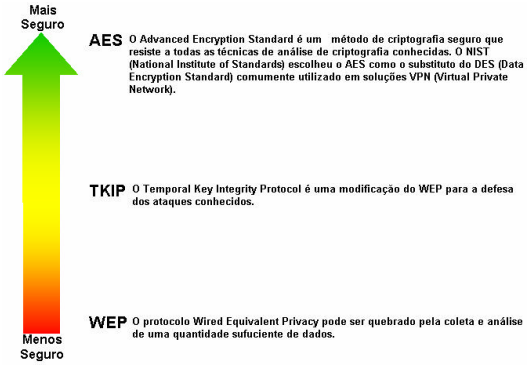


Figura 1. Comparativo entre os padrões de segurança em redes *wireless*

III. METODOLOGIA

Para o desenvolvimento deste trabalho foi configurado um ambiente de testes para realização de experimentos que objetivavam a aquisição de informações referentes ao desempenho da rede. Através das informações adquiridas com os testes efetuou-se uma análise para medir o desempenho da rede com os diferentes padrões de segurança existentes na atualidade.

A. Ambiente de Testes

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).

O *software* utilizado para geração de tráfego de rede para os testes foi o Rude e Crude Versão 0.62 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 e coleta das informações dos pacotes na outra extremidade da rede.

Nos microcomputadores realizou-se uma nova instalação do sistema operacional Linux Ubuntu 10.04 LTS 32 *bits*, ambos configurados igualmente.

Foi utilizada a topologia do tipo infraestrutura para a realização dos testes, a qual necessita de um concentrador central (*Access Point* - AP), sendo que o roteador *wireless* foi posicionado entre os dois microcomputadores distante 1 metro, conforme Figura 2.

Foram realizados testes para a rede sem segurança (*OPEN*) e para os padrões de segurança WEP, WPA e WPA2 em 1, 2, 4 e 8 minutos, os quais foram realizados três coletas para cada um dos tempos de testes realizados. Sendo que foram utilizadas chaves de maior tamanho

Figura 2. Estrutura da Rede do Ambiente de Testes

possível para obter a maior utilização de recursos de *hardware*, pois quanto maior a chave de criptografia maior será a utilização de *hardware* no processo de criptografia como um todo. Os tempos de testes foram acrescidos desta maneira para indicar possíveis discrepâncias nos testes. Sendo que todos os testes foram realizados dentro da mesma sala para obter as características desejadas sem interferências diferentes.

B. Desempenho em Redes sem Fio

Para análise do desempenho na rede experimental foram utilizadas métricas para representar o desempenho da rede.

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.

2) Delay: É a medida de quanto tempo irá demorar para um pacote 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.

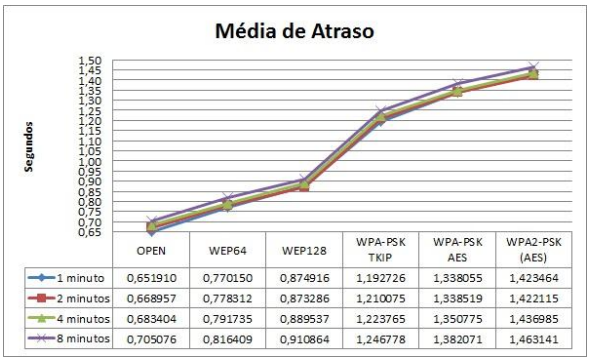
3) Jitter: O *jitter* em uma rede de computadores pode ser definido como o tempo entre a chegada dos pacotes. O *jitter* médio de uma rede de computadores é a variação do tempo entre a chegada de uma série de pacotes.

IV. Resultados

A média de atraso está representada pelo gráfico da Figura 3, através desta pode-se observar que a média de atraso aumenta conforme aumenta o padrão de segurança. Pode-se observar também que a maior diferença destas médias, considerando os padrões de segurança disponibilizados, está entre o padrão WEP128 para o padrão WPA-PSK TKIP, com aumento cerca de 25% (24,67%) em média para os quatro tempos de teste.

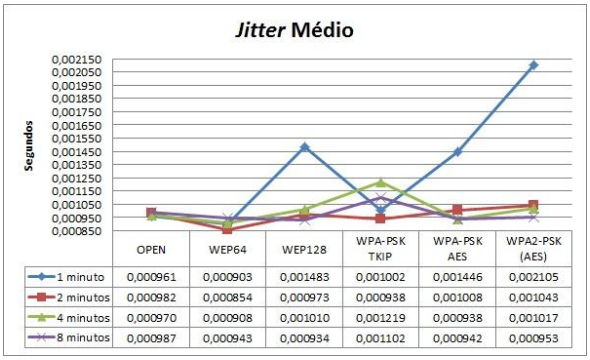
A Figura 4 mostra o *jitter* médio em função do tempo de coleta para cada padrão de segurança nos diferentes tempos dos testes efetuados. Através da figura pode-se observar que o *jitter* médio nos testes de 1 minuto apresentaram um valor elevado em comparação ao tempo de 2 minutos, em todos os padrões de segurança com exceção da rede sem segurança (*OPEN*), isto ocorre devido a instabilidade inicial da rede, pois a mesma necessita de alguns instantes para estabilizar.

Através da Figura 5 pode-se observar o *jitter* máximo para os padrões de segurança em cada teste. Através dos resultados obtidos pode-se perceber que esta métrica de



	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

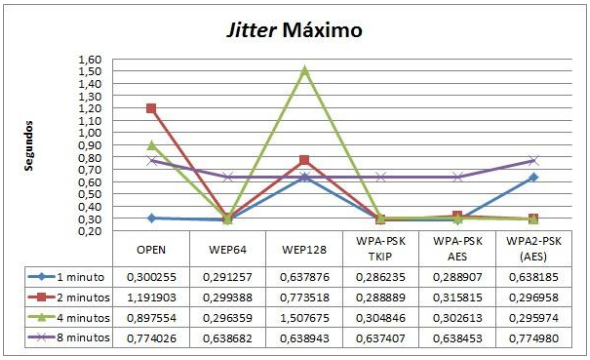
Figura 3. Média de atraso para os padrões de segurança em função do tempo de coleta



	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 4. *Jitter* médio para os padrões de segurança em função do tempo de coleta

desempenho em redes de computadores é bem instável, pois em certos momentos da conexão a rede pode sofrer degradação, uma vez que em se tratando de redes sem fio diversos fatores podem interferir na estabilidade da rede, causando com isso picos no *jitter*, e a métrica do *jitter* máximo traz os maiores valores obtidos em termos de atraso na chegada dos pacotes (*jitter*).

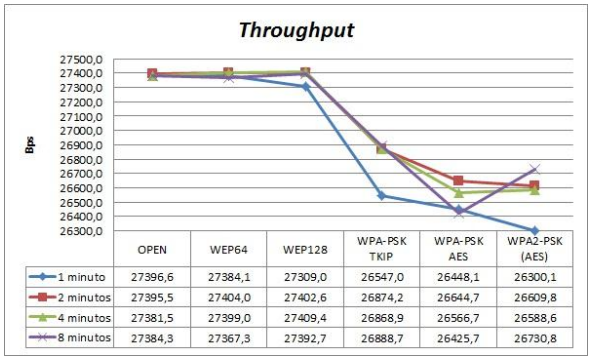


	OPEN	WEP64	WEP128	WPA-PSK TKIP	WPA-PSK AES	WPA2-PSK (AES)
1 minuto	0,300255	0,291257	0,637876	0,286235	0,288907	0,638185
2 minutos	1,191903	0,299388	0,773518	0,288889	0,315815	0,296958
4 minutos	0,897554	0,296359	1,507675	0,304846	0,302613	0,295974
8 minutos	0,774026	0,638682	0,638943	0,637407	0,638453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

Figura 5. *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 a Figura 6. Através da figura também é possível concluir

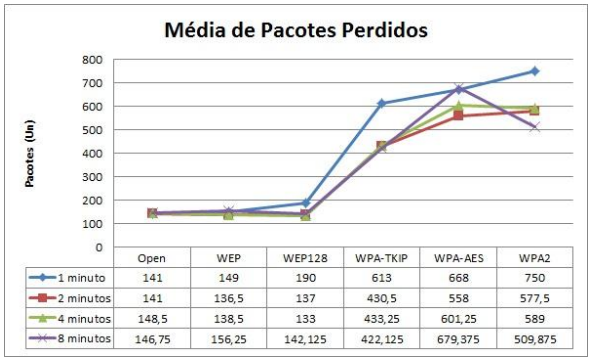
que a vazão na rede no tempo de testes de 1 minuto é inferior a tempos de testes maiores. Isto acontece pelo mesmo motivo descrito anteriormente na análise do *jitter* médio, que a rede é muito instável no começo de sua transmissão.



	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 6. Throughput para os padrões de segurança em função do tempo de coleta

Na Figura 7 pode-se observar a média dos pacotes perdidos por minuto para todos os tempos de testes. Através destes dados pode-se comprovar a instabilidade da rede no inicio da transmissão, pois aumentando o tempo dos testes percebe-se que a quantidade de pacotes perdidos por minuto diminui para praticamente todos os padrões de segurança.



	Open	WEP	WEP128	WPA-TKIP	WPA-AES	WPA2
1 minuto	141	149	190	613	668	750
2 minutos	141	136,5	137	430,5	558	577,5
4 minutos	148,5	138,5	133	433,25	601,25	589
8 minutos	146,75	156,25	142,125	422,125	679,375	509,875

Figura 7. Média de pacotes perdidos em função do tempo de coleta

V. Conclusões

Através dos experimentos e análises efetuadas neste trabalho pode-se verificar que a criptografia AES e o padrão WPA2-PSK possuem menor desempenho e maior segurança, conforme Amaral e Maestrelli [6] enfatiza, para a rede. Podem ser utilizados em redes com um alto requisito de confiabilidade, as quais necessitem transferir informações críticas. Pode-se, também, avaliar que os padrões de segurança OPEN, e WEP, com suas derivações, são as melhores opções em redes que necessitem um alto desempenho, sem requisitos significativos quanto a segurança.

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 em função dos algoritmos de criptografia utilizados. Isto deve-se ao fato de o padrão WEP e WPA-PSK TKIP utilizarem como algoritmo de criptografia o RC4, sendo que segundo Amaral e Maestrelli [6] estes padrões de segurança foram desenvolvidos para os equipamentos ja existentes. Já no padrão WPA-PSK AES e WPA2 utiliza-se como algoritmo de criptografia o AES, segundo Amaral e Maestrelli [6] a incorporação do AES foi devido a seu alto nível de segurança, sendo que o padrão WPA2 foi desenvolvido pensando na maior segurança possível para as redes sem fio 802.11. Com base nestas informações, é possível determinar a configuração mais adequada aos requisitos no momento da implantação de uma rede.

Também através deste trabalho pode-se comprovar o que foi descrito na subseção D da seção II, 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 na seção dos Resultados (Seção IV), pode-se detectar um aumento da média de atraso e diminuição da vazão da rede.

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 ou ainda comparar equipamentos com diferentes *hardwares* para determinar o quanto isto influencia na transmissão. Outro trabalho interessante é analisar o desempenho com diferentes padrões de redes 802.11x. Para estes trabalhos sugere-se a utilização de tempos de testes superiores a dois minutos, uma vez que a rede apresenta bastante instabilidade em intervalos de tempos de até dois minutos.

Referências

[1] W. Stallings, *Criptografia e Segurança de redes: Princípios e Práticas*, 4th ed. São Paulo: Pearson Prentice Hall, 2008.

[2] C. Suzin, "Análise de desempenho de protocolos de criptografia em redes sem fio," *Monografia (Graduação em Sistemas de Informação) - Universidade de Caxias do Sul*, p. 70 f., 2007.

[3] E. Barka and M. Boulmalf, "Impact of encryption on the throughput of infrastructure wlan ieee 802.11g," *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, pp. 2693–2697, 2007, disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4224745&isnumber=4224245>. Acesso em: 29 Ago. 2012.

[4] T. Thomas, *Segurança de Redes: Primeiros Passos*. Rio de Janeiro: Editora Moderna Ltda, 2007.

[5] T. F. G. Caixeta, *Entendendo a Segurança nas Redes sem Fio. Revista Segurança Digital*, 4th ed., 2012, disponível em: <http://segurancadigital.info/>. Acesso em: 10 jun. 2012.

[6] B. M. Amaral and M. Maestrelli, *Segurança em Redes Wireless 802.11*, 2004, disponível em: <http://www.docstoc.com/docs/27567161/Segurança-em-Redes-Wireless-80211>. Acesso em: 30 jun. 2012.