Avaliando a Sobrecarga Introduzida nas Redes 802.11 pelos Mecanismos de Segurança WEP e VPN/IPSec*

Paulo Ditarso Maciel Júnior, Bruno Astuto Arouche Nunes,
Carlos Alberto Vieira Campos, Luís Felipe Magalhães de Moraes

Laboratório de Redes de Alta Velocidade – RAVEL
Programa de Engenharia de Sistemas e Computação – COPPE/UFRJ
Caixa Postal: 68.511 – 21941-972 – Rio de Janeiro, RJ

{pdmjr,bastuto,carlosvc,moraes}@cos.ufrj.br

Resumo. *Apresenta-se neste artigo uma análise comparativa da sobrecarga introduzida nas Redes 802.11b pelos mecanismos de segurança WEP e VPN/IPSec. É analisado o comportamento dos tráfegos TCP e UDP, sob alguns cenários de redes locais sem fio em função do número de conexões ativas e da solução de segurança utilizada. De posse desta análise, pode-se estimar de maneira mais adequada, a aplicação destes mecanismos no ambiente de rede sem fio desejado, tomando como base o protocolo da camada de transporte utilizado e o nível de segurança pretendido.*

Abstract. *This paper presents a comparative analysis of the overhead introduced in IEEE 802.11b networks, by the security mechanisms WEP and VPN/IPSec. TCP and UDP traffic behavior are analysed under different local wireless environments, as a function of the number of active connections and the security solution implemented. Through this analysis, it is possible to estimate the most appropriate security mechanism to be applied in the intended wireless environment, in terms of the transport layer protocol utilized and the wanted security level.*

1. Introdução

O padrão IEEE 802.11b [1] é uma das soluções mais adotadas para redes locais sem fio (*Wireless Local Area Networks - WLANs*). Esse padrão está cada vez mais presente nas empresas, hotéis, fábricas e lugares públicos como aeroportos, universidades, hospitais e centros comerciais, oferecendo a possibilidade de acesso à rede com suporte à mobilidade.

O problema desta tecnologia emergente, está na sua falta de segurança, devido à particularidades do meio físico de transmissão. Como os dados são transmitidos pelo ar, não existem limites definidos como no caso das redes cabeadas. Dessa forma, é possível interceptar informações mesmo que a longas distâncias, sem necessariamente estar no mesmo ambiente ou prédio da WLAN.

As redes sem fio, geralmente, estão conectadas a infra-estrutura da rede cabeada, tornando-se assim, mais fácil para o invasor ganhar acesso a toda base de dados da empresa. Por isso, é extremamente importante a implementação de mecanismos e sistemas de segurança às WLANs. Todavia, a escolha destes mecanismos e sistemas deve ser criteriosa, devido à sua

*Esse trabalho foi realizado com recursos da CAPES e da FAPERJ.

sobrecarga adicional inserida no tráfego da rede. Dentro desse contexto, este trabalho apresenta uma avaliação dessa sobrecarga em alguns cenários de utilização do padrão IEEE 802.11b.

O presente artigo está organizado da seguinte forma. Na seção 2, são apresentados os principais mecanismos de segurança utilizados em redes sem fio. Na seção 3, são descritos os cenários onde as medições foram realizadas em função do tipo de tráfego, número de conexões e o protocolo de transporte utilizado. A avaliação dos resultados obtidos é mostrada na seção 4. Por fim, as conclusões e trabalhos futuros são apresentados na seção 5.

2. Mecanismos de Segurança utilizados nas WLANs

Existem várias propostas para implementar segurança em WLANs como por exemplo, a utilização de Firewalls [2], mecanismos de autenticação como o Kerberos e o RADIUS [3], implementação de novos protocolos para garantir privacidade e autenticação no padrão IEEE 802.11 [1], propostas baseadas no padrão IEEE 802.1x [4] e a utilização de Redes Virtuais Privadas (*Virtual Private Network - VPNs*).

Em [5], as soluções de segurança são classificadas em: baseadas e não-baseadas em padrões. Dentre as baseadas em padrões, destaca-se o algoritmo de criptografia *Wired Equivalent Privacy - WEP* [1], por fazer parte da especificação padrão do IEEE 802.11. Das soluções não-baseadas em padrões, as VPNs através do Protocolo IP Seguro (*IP Security Protocol - IPSec*) [6, 7] são as mais utilizadas e possuem um alto nível de segurança. Por outro lado, quanto maior for esse nível de segurança, maior será a sobrecarga no sistema, como mostrado na seção 4. Nas seções abaixo, serão descritos os mecanismos WEP e VPN/IPSec.

2.1. O Mecanismo *Wired Equivalent Privacy - WEP*

O padrão IEEE 802.11 utiliza o protocolo WEP na camada de enlace para autenticar e criptografar os dados que serão transmitidos na rede sem fio. A figura 1 mostra como o WEP funciona:

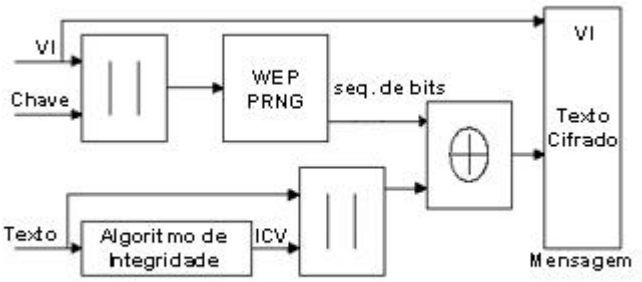


Figura 1: O funcionamento do WEP

O Vetor de Inicialização - VI de 24 bits é concatenado com a chave secreta, que pode ser de 40 ou 104 bits, resultando em uma chave composta de 64 ou 128 bits. Esta, por sua vez, serve de entrada para um gerador de números pseudo-aleatórios (PRNG) que é baseado no algoritmo RC4 [8].

A saída do PRNG é uma seqüência pseudo-aleatória de bits baseada na chave composta e com o mesmo tamanho do texto a ser criptografado. Esse texto é obtido através da concatenação do texto puro com o resultado do processo para checagem de integridade (*Integrity Check Value* - ICV) que utiliza o algoritmo de checagem de redundância CRC-32 (*Cyclic Redundancy Check*).

A seqüência de bits pseudo-aleatória é utilizada para criptografar o texto através de uma operação binária XOR. O resultado do XOR é concatenado com o VI e enviado pelo emissor através do meio de transmissão.

O receptor usa o VI que vêm no início do pacote e a chave secreta compartilhada para gerar a mesma seqüência criada pelo PRNG e decriptografar o texto cifrado. Então, aplica-se o CRC-32 e compara-o com o ICV concatenado ao texto puro para checar a integridade da mensagem recebida.

O IEEE 802.11 define dois métodos de autenticação:

- Autenticação com sistema aberto (*Open System Authentication*): a estação pode associar-se com qualquer ponto de acesso e escutar todos os dados que são transmitidos sem criptografia. Este método baseia-se na transmissão da identidade da estação que quer ser autenticada para a estação que realizará a autenticação;
- Autenticação com chave pré-compartilhada (*Pre-Shared Key Authentication*): método baseado no mecanismo desafio-resposta (*challenge-response*).

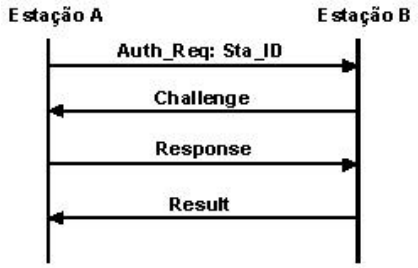


Figura 2: A autenticação no protocolo WEP

A figura 2 ilustra este processo de autenticação. A estação A envia uma requisição e a sua identificação (Auth_Req; Sta_ID) para a estação B. B responde com uma mensagem contendo um desafio de 128 bits (*Challenge*). A estação A copia o desafio em uma nova mensagem, criptografa com a chave WEP pré-compartilhada e reenvia para B (*Response*). A estação B checa a resposta de A e responde com o resultado do procedimento de autenticação (*Result*).

2.2. O Mecanismo *Virtual Private Network* - VPN com *IP Secure* - IPSec

Foi utilizado o IPSec para estabelecer a VPN entre o ponto de acesso e as estações sem fio. O IPSec provê segurança através de criptografia e/ou autenticação na camada IP.

Dentre várias propriedades desejáveis em comunicação de dados segura, pode-se citar: a confidencialidade, a integridade e a autenticidade, como as mais comuns. O IPSec fornece estas características na utilização de dois protocolos: Cabeçalho de Autenticação (*Authentication Header - AH*) [9] e o Encapsulamento Seguro do Campo de Dados (*Encapsulating Security Payload - ESP*) [10]. O AH e o ESP suportam dois modos de operação: transporte e túnel.

Modo Transporte: O modo transporte provê proteção para os protocolos da camada superior (TCP e UDP, por exemplo). É usado, geralmente, em comunicações fim-a-fim entre estações. Neste modo o ESP criptografa e, opcionalmente, autentica o campo de dados do pacote IP. O AH autentica o campo de dados IP e campos do cabeçalho IP. A Figura 3(b) ilustra o ESP e o AH no modo transporte.

Modo Túnel: Tipicamente utilizado para estabelecer VPNs, provê proteção ao pacote IP completo. Os campos do AH e ESP são adicionados ao pacote IP e tudo passa a ser tratado como

o campo de dados do pacote IP de um novo pacote, inclusive com um novo cabeçalho IP. A Figura 3(c) mostra o funcionamento do IPSec em modo túnel. O ESP criptografa e, opcionalmente, autentica todo o pacote IP interno. O AH autentica o pacote IP interno e partes do cabeçalho externo.

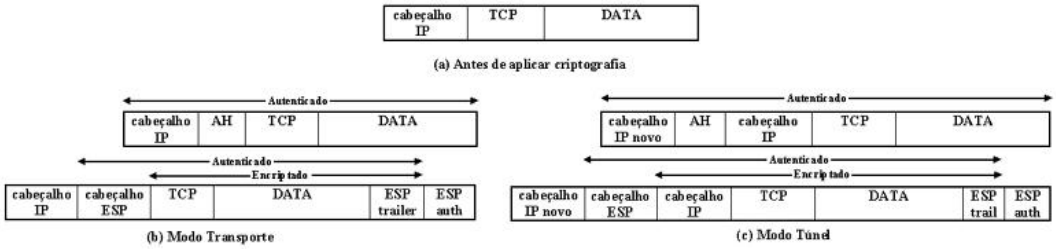


Figura 3: Formato do pacote IPSec.

3. Ambientes dos Testes

Nesta seção, serão descritas as características e a configuração do ambiente que foram realizados os testes.

3.1. Equipamentos

Foram utilizados quatro equipamentos para a realização dos experimentos com a seguinte configuração:

- Pentium 166MHz, 16MB de RAM, placa WLAN PCMCIA 11Mbps, placa Ethernet 100Mbps (ponto de acesso);
- Pentium III 1GHz, 256MB de RAM, placa WLAN PCMCIA 11Mbps (estação sem fio);
- Pentium III 700MHz, 256MB de RAM, placa Ethernet 100Mbps (estação com fio);
- Pentium IV 1.8GHz, 256MB de RAM, placa WLAN PCMCIA 11Mbps (estação móvel).

As interfaces de rede sem fio estão de acordo com o padrão IEEE 802.11b, cujo protocolo de acesso ao meio é o CSMA/CA e o a banda passante nominal é de 11 Mbps.

3.2. Programas Necessários

O sistema operacional no ponto de acesso é o OpenBSD 3.2 e as demais estações utilizam o Windows XP. Foi estabelecida uma VPN através do protocolo ESP com autenticação do IPSec funcionando em modo túnel. Para isto, utiliza-se o *daemon* ISAKMP [11] no ponto de acesso e o programa SSH Sentinel [12] como cliente VPN nas estações sem fio. A VPN utiliza uma chave pré-compartilhada para a autenticação e o algoritmo 3DES-CBC (168 bits) para criptografia. O outro mecanismo de segurança utilizado foi o protocolo WEP com a chave composta no tamanho de 128 bits.

Foi utilizado o programa IP *Traffic* [13] para geração do tráfego TCP e UDP, e para monitorar a rede. Com ele pode-se exportar as estatísticas do tráfego monitorado para uma posterior análise.

3.3. Configuração dos Cenários de Testes

Os testes foram realizados em uma sala de 35 m^2, sem nenhum obstáculo físico entre os equipamentos. O mesmo conjunto de testes foram executados sob dois cenários diferentes:

Cenário 1: comunicação entre uma estação sem fio e uma estação com fio, como pode ser visto na figura 4(a).

Cenário 2: comunicação entre duas estções sem fio, como pode ser visto na figura 4(b).

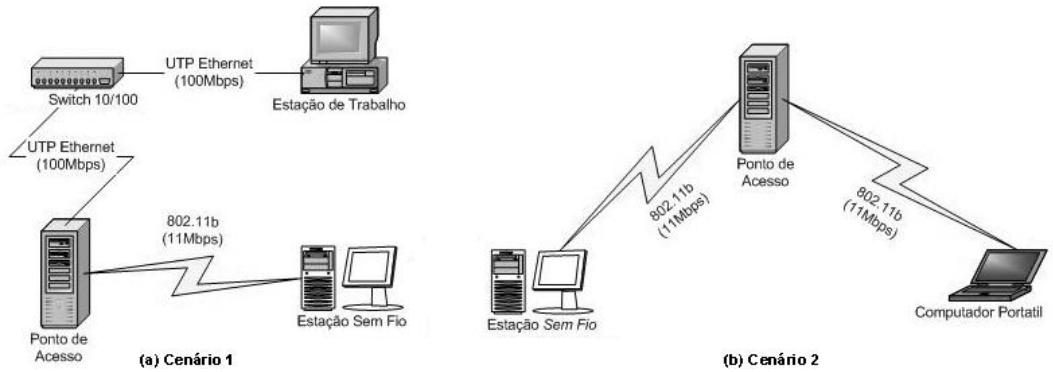


Figura 4: Cenários de realização dos testes

Utiliza-se o IP *Traffic* para gerar um tráfego CBR com o tamanho de pacote IP de 1500 bytes, para evitar fragmentação, e um intervalo entre pacotes de 1 milisegundo para saturar o canal. Para cada cenário, foi avaliado o comportamento do tráfego TCP e UDP tanto para uma única conexão, quanto para oito conexões simultâneas. Através de testes realizados com a ferramenta IP *Traffic*, percebeu-se que com mais de oito conexões o aumento na vazão não foi significante. Com isso, os testes foram realizados com uma e com oito conexões.

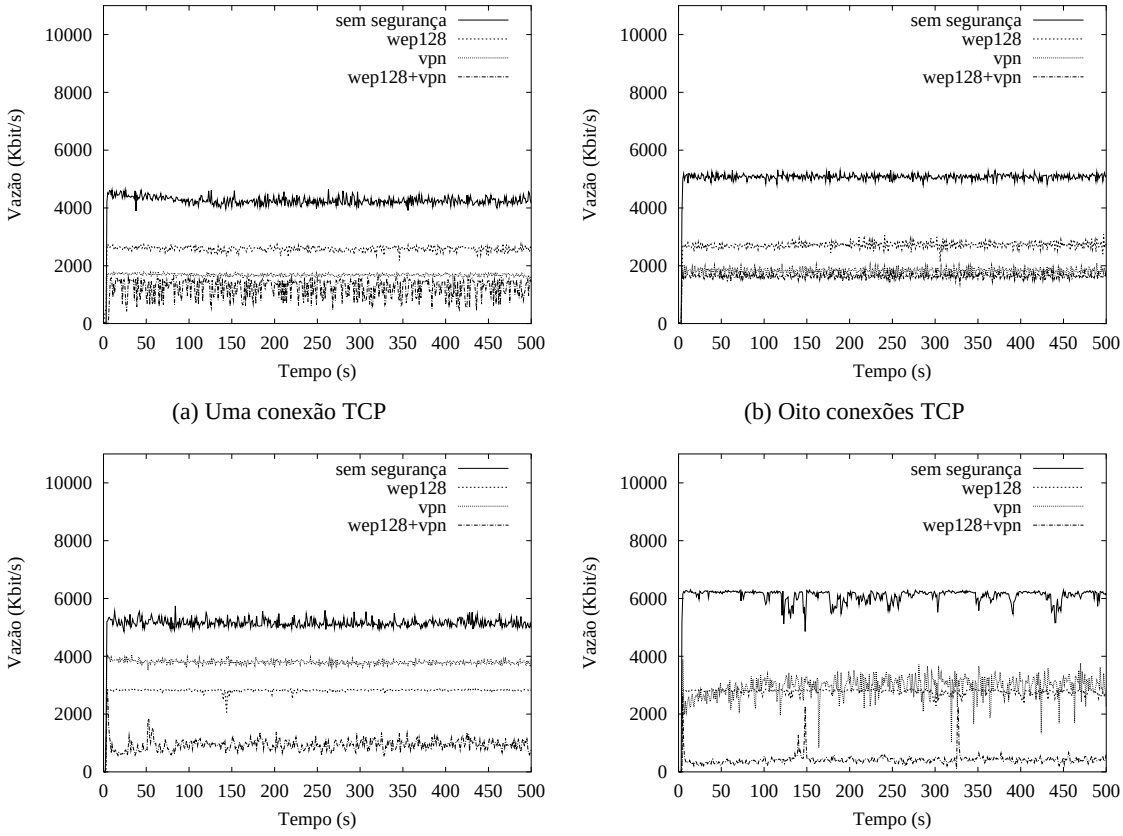
Em cada configuração dos testes descritos acima, variou-se o nível de segurança. Primeiro, foi monitorado o tráfego sem nenhum mecanismo de segurança. Depois, observou-se o comportamento do mesmo tráfego sob a criptografia do WEP com 128 bits. Em seguida, foi medido o tráfego passando por uma VPN. Por fim, o monitoramento do tráfego passando pelo mais alto nível de segurança alcançado com estas tecnologias que é a aplicação da criptografia tanto na camada de enlace, como o WEP de 128 bits, quanto na camada de rede com a VPN.

4. Avaliação dos Resultados Obtidos

As figuras 5(a) e 5(b) apresentam o tráfego TCP, sob diferentes níveis de segurança, para uma e para oito conexões ativas respectivamente. Ambas comportam-se de maneira semelhante, com um pequeno ganho na vazão no tráfego com oito conexões devido o aumento da carga no canal, atingindo assim a vazão máxima. É importante observar a grande perda ocorrida na vazão do canal devido ao aumento no grau de segurança da comunicação.

Para 8 conexões ativas, o tráfego sem segurança atinge uma vazão média de aproximadamente 5 Mbps. O tráfego criptografado com o algoritmo WEP de 128 bits apresenta-se com uma vazão média próxima de 2,7 Mbps. Uma perda de aproximadamente 46% em relação à vazão máxima obtida. Quando é estabelecida a VPN a vazão cai ainda mais. Com o nível máximo de segurança, atingido com o WEP e VPN ao mesmo tempo, a vazão média cai para 1,6 Mbps. Cerca de 33% da vazão atingida pelo tráfego sem segurança, ou seja, uma queda de aproximadamente 67%. A mesma análise aplica-se aos tráfegos com uma conexão ativa, porém, com uma pequena redução nos valores médios obtidos.

Este comportamento é devido à sobrecarga introduzida na rede pelos mecanismos de segurança adotados. No WEP, além do tempo computacional requerido para as operações de



(a) Uma conexão TCP

(b) Oito conexões TCP

(c) Uma conexão UDP

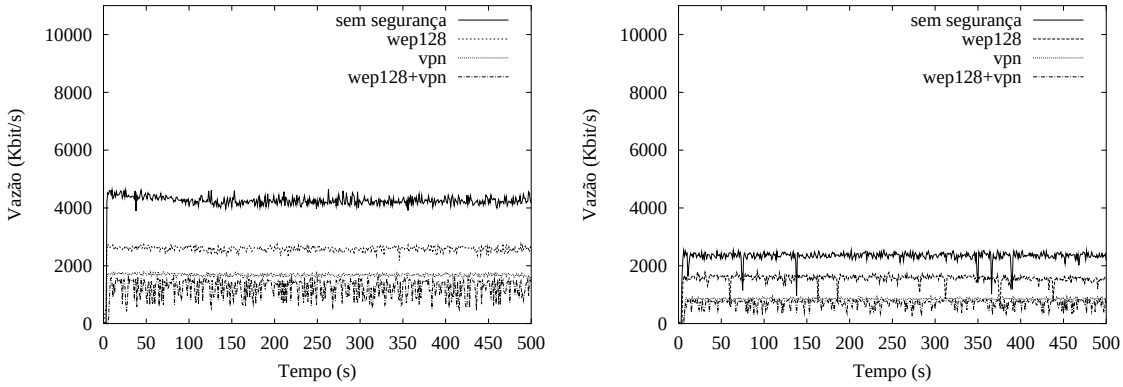
(d) Oito conexões UDP

Figura 5: A vazão da rede no cenário 1 em função do número de conexões e do protocolo de transporte

criptografia e decriptografia, os quadros da camada de enlace possuem 8 bytes de informações adicionais, compostas pelo VI e pelo ICV. A VPN no modo túnel protege todo o pacote IP através de criptografia, encapsula o cabeçalho ESP ao pacote, aplica o algoritmo de autenticação, e por fim, adiciona um novo cabeçalho IP ao pacote gerado. Isso significa que, além do tempo gasto nas operações de criptografia e autenticação, são inseridos ainda mais dados de controle na rede do que com o WEP. Ao mesmo tempo que são inseridos dados de controle no tráfego da rede, existe ainda o processo de fragmentação e defragmentação dos pacotes que ultrapassam o tamanho da unidade máxima de transferência (*Maximum Transfer Unit - MTU*).

As figuras 5(c) e 5(d) representam as mesmas medições apresentadas acima, agora no protocolo UDP. Verificou-se novamente o mesmo comportamento de queda na vazão com relação as implementações de segurança, com uma perda ainda mais acentuada quando utiliza-se VPN. Comparando os resultados com os obtidos para o tráfego TCP, verifica-se uma vazão ligeiramente maior no UDP, já que não existe tráfego de controle para este protocolo.

A figura 6 ilustra o tráfego TCP para uma conexão ativa nos dois cenários apresentados. O cenário 1, figura 6(a), com a comunicação entre uma estação sem fio e outra com fio, e na figura 6(b), o cenário 2 com a comunicação entre uma estação sem fio e um computador portátil. No cenário 2, notou-se a redução nas vazões encontradas em relação ao cenário 1, pelo fato de existirem duas estações disputando o meio de transmissão através do protocolo CSMA/CA. Diferente do cenário 1 onde tem-se apenas uma única estação disputando o meio sem fio, e toda comunicação entre o ponto de acesso e a estação com fio é através do padrão Ethernet que é baseado no protocolo de acesso ao meio CSMA/CD. Além disso, o padrão Ethernet utilizado tem uma taxa de



(a) Cenário 1 com uma conexão TCP

(b) Cenário 2 com uma conexão TCP

Figura 6: A vazão em diferentes cenários

transmissão nominal de 100 Mbps, enquanto no padrão 802.11b é de 11 Mbps.

A figura 7 apresenta todos os resultados obtidos dos experimentos descritos acima e aplicados no cenário 2. Foi constatada mais uma vez a influência na vazão da rede devido à aplicação de uma comunicação com diferentes níveis de segurança.

5. Conclusões e Trabalhos Futuros

Neste trabalho foi apresentado um estudo sobre a influência da sobrecarga introduzida nas redes 802.11b pelos mecanismos de segurança WEP e VPN/IPSec. Os resultados obtidos mostraram que esses mecanismos introduzem informações adicionais de controle na rede que reduziram a vazão da rede. Constatou-se que a utilização de VPN provendo segurança em ambientes sem fio, adiciona uma alta sobrecarga no sistema diminuindo a vazão efetiva, média em aproximadamente 60%, conforme o esperado. Com o protocolo WEP, a redução média foi de aproximadamente 34%.

Para WLANs que não necessitam de um alto nível de segurança, recomenda-se a utilização do protocolo de criptografia WEP com 128 bits. Já em ambientes que a confidencialidade dos dados é uma prioridade, recomenda-se a utilização de VPNs. Entretanto, como a redução da vazão pode chegar a 60%, algumas aplicações que necessitem de um requisito mínimo de qualidade de serviço podem ser prejudicadas, como por exemplo, aplicações multimídias.

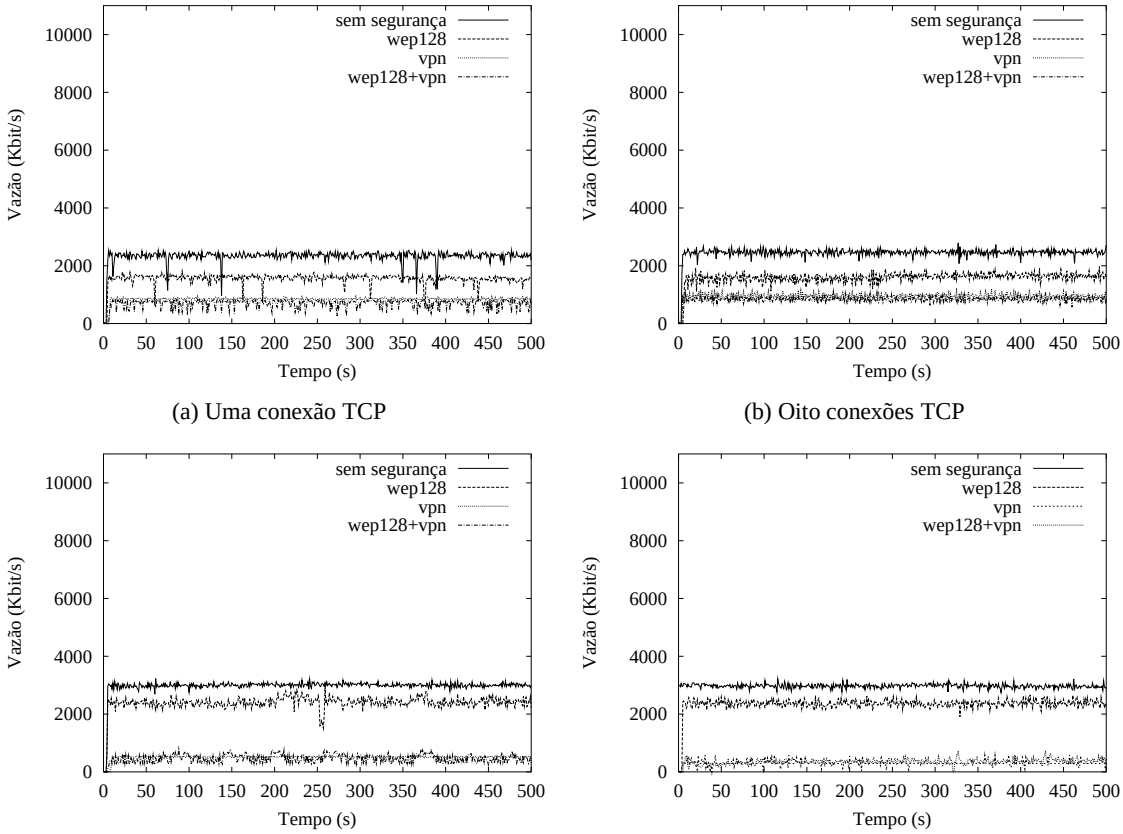
Como trabalhos futuros, pretende-se estender a avaliação realizada à outras métricas de desempenho, como retardo fim-a-fim, variação do atraso *jitter* e taxa de perda. Além disso, deseja-se avaliar outros mecanismos de segurança tais como, 802.1x, DHCP Seguro e sistemas de autenticação como RADIUS e Kerberos. Por fim, pretende-se modelar analiticamente a sobrecarga adicionada pelos mecanismos de segurança citados acima.

Referências

[1] 802.11b, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification: Higher-Speed Physical Layer Extension in the 2.4 GHz Band*. IEEE Std 802.11b, 1999.

[2] W. W. U. Murthy, O. Bukhres and E. Vanderdez, "Firewalls for Security in Wireless Networks," in *Thisty-First Annual Hawaii International Conference on System Scicens*, jan 1998.

[3] H. M. A. Prasad and J. Kruys, "Security Architecture for Wireless LANs: Corporate & Public Environment," *IEEE VTC2000*, 2000.



(a) Uma conexão TCP

(b) Oito conexões TCP

(c) Uma conexão UDP

(d) Oito conexões UDP

Figura 7: A vazão da rede no cenário 2 em função do número de conexões e do protocolo de transporte

[4] 802.1x, *Standard for Port Based Network Access Control*. IEEE Std 802.11b, 2000.

[5] M. Casole, "WLAN Security - Status, Problems and Perspective," in *European Wireless 2002*, feb 2002.

[6] R. A. S. Kent, "Security Architecture for the Internet Protocol," *IETF RFC 2401*, nov 1998.

[7] N. D. R. Thayer and R. Glenn, "IP Security Document Roadmap," *IETF RFC 2411*, nov 1998.

[8] *RC4: Encrypty Algoritm of RSA Security*, 2003. http://www.rsasecurity.com.

[9] R. A. S. Kent, "IP Authentication Header," *IETF RFC 2402*, nov 1998.

[10] R. A. S. Kent, "IP Encapsulating Security Payload (ESP)," *IETF RFC 2406*, nov 1998.

[11] M. S. D. Maughan, M. Schertler and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," *IETF RFC 2408*, nov 1998.

[12] *SSH Sentinel: Client Software for VPN/IPSec*, 2003. http://www.ssh.com.

[13] *IP Traffic: a Tool for Generation and Monitoring of Traffic*, 2003. http://www.zti-telecom.com.