Segurança na troca de informações em uma rede sem fio no modo Ad Hoc

Floriano Ferreira Dos Reis Filho[1], Héctor Dave Orrillo Ascama[1] e Sergio Takeo Kofuji[1]

[1]Laboratório de Sistemas Integráveis – Universidade de São Paulo (USP)

CEP: 05508-900 - São Paulo - SP – Brazil

{floriano,hector,kofuji}@pad.lsi.usp.br

Resumo. *Neste trabalho avalia-se um mecanismo de segurança sobre uma rede Ad Hoc com roteamento AODV (On Demand Distance Vector), este mecanismo é composto pelo protocolo WEP (Wired Equivalent Privacy) na camada de Enlace e o IPSec (IP Security) na camada de Rede. O IPSec é um protocolo das soluções não baseadas em padrões, utilizado na segurança de uma rede VPN (Virtual Private Network), realizou-se as devidas configurações e simulações em cenários reais para utilizá-lo em uma rede Ad Hoc. Pretende-se estimar como este mecanismo afeta o desempenho da rede Ad Hoc tendo-se como métrica a vazão de dados.*

1. Introdução

Na atualidade, as pessoas utilizam algum tipo de dispositivo portátil com capacidade de se comunicar com a parte fixa de uma rede sem fio ou até com outros computadores móveis. Basicamente, existem dois tipos de Redes Móveis sem fio: as redes *Ad Hoc* e as redes de infra-estrutura.

Nas redes de infra-estrutura, as estações móveis devem estar em permanente contato com uma estação de suporte a mobilidade, conhecida como ponto de acesso. Em uma rede *Ad Hoc*, as estações móveis são capazes de se comunicar diretamente entre si, sem a necessidade de um ponto de acesso.

O objetivo principal deste trabalho é implementar segurança ao protocolo do tipo on-demand *AODV* (*Ad Hoc On-Demand Distance Vector Routing*), utilizando o *WEP* (*Wired Equivalent Privacy*) e o *IPSec* (*IP Security*).

Este artigo está organizado como segue. A seção 2 apresenta os conceitos necessários para o entendimento do trabalho. A seção 3 contém a descrição do cenário experimental. A seção 4 descreve as simulações e os resultados alcançados. Finalmente, a seção 5 contém as conclusões do trabalho desenvolvido.

2. Falhas de segurança nos protocolos de roteamento

Em uma rede *Ad Hoc*, o grau de comprometimento entre os nós é alto, o desempenho da rede depende de cada um dos nós, por estas características uma rede *Ad Hoc* se faz insegura.

Os aspectos de segurança nos protocolos de roteamento são críticos, pois muitos foram desenvolvidos sem considerar esta característica.

Neste tipo de rede cada nó deverá estar preparado para enfrentar um adversário, garantindo indiretamente maior grau de segurança para toda a rede. O principal ataque dos adversários é comprometer o processo de descoberta de rotas e aproveitar-se disto. Os pacotes de route request (*RREQ*) e route reply (*RREP*) podem ser alterados enquanto trafegam, ou podem ser forjados causando diversas anomalias no funcionamento da rede [Dahill, Levine, Royer e Shields 2002].

Ataques feitos nos protocolos de roteamento podem causar um comportamento anormal do tráfego de rede, podendo-se levar a negação de serviços DoS (*Deny of Service*) [Y. Zhang e W. Lee 2003].

A seguir apresenta-se alguns conceitos utilizados na proposta.

2.1. Protocolo de roteamento *AODV*

O protocolo *AODV* permite o roteamento em uma topologia que muda constantemente. É um protocolo reativo, constrói as rotas somente quando necessário. Ele utiliza um processo de inundação para descobrir as rotas, tenta aumentar a largura de banda disponível, minimizando o uso de mensagens periódicas para atualização de rotas.

O *AODV* fornece descoberta dinâmica de rotas e manutenção das mesmas entre os nós, utilizando links simétricos e três tipos de mensagens [Kullberg 2004]. Ele minimiza o número de broadcasts solicitados, pois cria rotas sob demanda, não precisa manter uma lista completa de rotas para todos os destinos possíveis.

Escolheu-se o protocolo *AODV* para este trabalho, devido aos seus dois objetivos principais:

- ✓ Descoberta de rota entre o nó de origem e o de destino.
- ✓ Armazenamento e gerenciamento de rotas ativas. [Royer e Toh 1999].

Para a descoberta de rota, utiliza-se dois processos: Pedido de Rota e Recebimento de Rota. O primeiro ocorre quando a estação de origem deseja enviar uma mensagem para outra estação e não tem uma rota válida para este destino. O segundo acontece quando se tem uma resposta, da rota que a estação de origem deseja, para estabelecer um canal de comunicação com a estação de destino.

2.2 Protocolo de segurança *WEP* e *IPSec*

A segurança é questão importante nas redes sem fio, por este motivo procurou-se utilizar protocolos de segurança, abaixo descritos, que operam na camada de enlace de dados e na camada de rede.

O *WEP* (*Wired Equivalent Privacy*) é o método de criptografia utilizado nas redes *wireless* 802.11. Opera na camada de enlace de dados e fornece criptografia, entre

as estações conectadas no modo *Ad Hoc,* com base no método *RC4* (*Rivest Cipher*) da *RSA*, que usa um *IV* (*Initialization Vector*), vetor de inicialização de 24 bits e uma chave secreta compartilhada de 40 ou 104 bits. O *IV* é concatenado com a chave secreta compartilhada para formar uma chave de 64 ou 128 bits que é usada para criptografar os dados. O resultado serve de entrada para um gerador de números pseudo-aleatórios, *PRNG* (*Pseudo Random Number Generator*), que é baseado no algoritmo *RC4* [RSA Security Inc. 2003]. 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.

O *IPSec* agrega proteção ao pacote IP, fornece protocolos para a segurança de tráfego de dados na rede *Ad Hoc*, autenticação de cabeçalho *AH* (*Authentication Header*), segurança no encapsulamento do *payload*, conteúdo dos dados, *ESP* (*Encapsulating Security Payload*), bem como protocolos para a gerência de chaves. Tendo-se o *IPSec* como opção para implementar *VPN* (*Virtual Private Network*), a rede torna-se mais segura, pois os serviços podem ser utilizados por qualquer protocolo nas camadas superiores. Neste trabalho utilizou-se o *IPSec* para segurança das estações na rede *Ad Hoc* e não como ponte entre duas redes (*VPN*), como geralmente é utilizado, por possuir serviços para o controle de acesso, integridade, autenticação da origem dos dados e confidencialidade. No modo transporte, o cabeçalho ESP é inserido após o cabeçalho IP original, a criptografia do conteúdo dos dados é garantida. (fig.1).

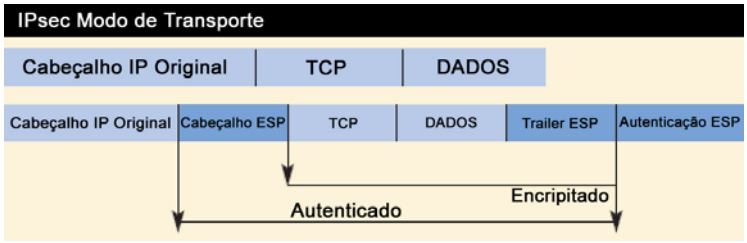

Figura 1. ESP após o cabeçalho IP original. [Meredith 2002]

3. Descrição do cenário para os testes

Criou-se um cenário prático de uma rede *Ad Hoc* de 2 nós. As simulações feitas com software não duplicam a realidade em um ambiente. Nele, fatores como taxa de sinal ruído varia e qualidade do *link* oscila devido à interferência de fatores climáticos, como a temperatura. Estas simulações ignoram as comunicações entre as camadas e não conseguem capturar os erros que ocorrem nas iterações entre o sistema operacional, o hardware e o ambiente sem fio [Sanghari, Brown e Doshi 2003].

Embora o protocolo de roteamento *AODV* tenha sido desenvolvido [Royer 2003], não se teve um teste do mesmo na plataforma Windows, utilizando os protocolos da camada de enlace de dados e rede com um nível de segurança atribuído para suporte ao protocolo de roteamento.

3.1. Hardware e software utilizados

Para a realização do experimento, utilizou-se duas estações com a seguinte configuração: 1) D*esktop* com processador Intel Pentium 4 de 1.80 GHz e 768 MB de RAM. 2) Placas padrão IEEE 802.11b 11 Mbps *Wireless LAN* da 3Com, modelo 3CRDW696, pois fornecem conexão *Ad Hoc* segura e suporte 802.1x para *Windows XP*. 3) Sistema Operacional *Windows XP Professional* com *Service Pack 1*.

Para geração do tráfego em uma rede sem fio escolheu-se a ferramenta *Netperf* [Hewlett-Packard Company 2003], que permite gerar, receber e coletar dados, com o objetivo de fazer uma análise estatística da rede.

3.2. Configuração do cenário

Realizaram-se os testes em uma sala com 42 m^2, com um espaço de 1 metro entre as estações. Definiu-se um canal de comunicação 6, pois este canal trabalha na faixa de freqüência compatível, entre 2426 a 2448 MHz, das interfaces *wireless* (2.4 GHz). A rede foi composta por duas estações, com endereços *IP* (*Internet Protocol*) privados, pois eles fazem parte de uma rede que será criada apenas para fins específicos em um cenário *Ad Hoc*.

O tamanho das mensagens transmitidas pela rede *Ad Hoc* varia entre 8 até 65.536 bytes. Para gerar o tráfego na rede utilizou-se a ferramenta Netperf. Cada nó atua primeiro como emissor e depois como receptor.

4. Resultados das experiências

Na fig. 2 mostra-se como os mecanismos de segurança *WEP* e *IPSec* afetam a vazão de dados. Os testes foram feitos da máquina A para a máquina B e vice-versa. Os resultados de cada um deles são apresentados nos gráficos.

Para estes testes, os parâmetros de vazão de dados e o tamanho das mensagens foram especificados para se evidenciar qual o ponto máximo onde pode-se ter a maior taxa de dados na transferência de uma mensagem.

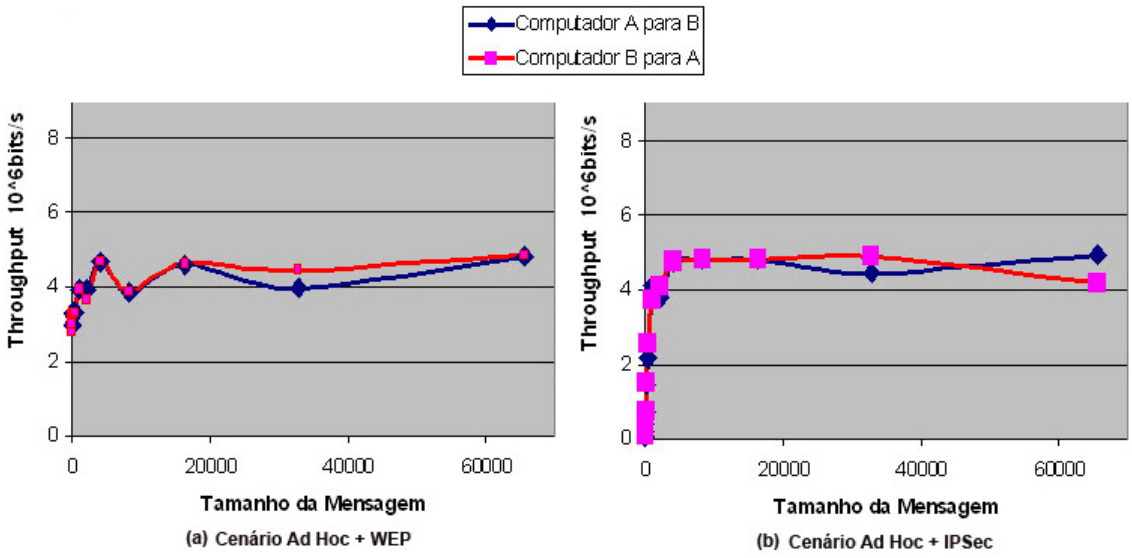

Figura 2. Vazão de dados no cenário sem fio.

A fig. 2a mostra que o nível maior para taxa de transferência foi 4,65 Mbps para tamanhos de mensagens de 16.384 bytes, para as duas estações. Quanto maior o tamanho da mensagem, maior a taxa de transferência de dados. Neste caso, com tamanho de mensagem de 65.536 bytes as duas estações alcançam a taxa máxima de transmissão no meio sem fio.

Na fig. 2b, o nível maior para taxa de transferência para as duas máquinas foi de 4,8 Mbps. Ambos os computadores depois de enviarem mensagens com o tamanho de 16.384 bytes tendem a diminuir a vazão de dados. Do computador B para o A, a taxa diminui para 4,19 Mbps com mensagem de 65.536 bytes. Do computador A para o B a taxa diminui para 4,48 Mbps. Com tamanho de mensagem até 16.384 bytes, a rede entra em um estado estável, aumentando-se o tamanho das mensagens a rede tem variações devido à sobrecarga para criptografia do conteúdo do pacote IP.

As linhas da fig. 3 correspondem à transmissão das mensagens entre o computador A e o computador B. Segue abaixo os cenários testados:

Cenário 1. *Ad Hoc Puro*

Cenário 2. *Ad Hoc* com *WEP*

Cenário 3. *Ad Hoc* com *IPSec*

Cenário 4. *Ad Hoc* com *AODV*

Cenário 5. *Ad Hoc* com *IPSec* e *AODV*

Cenário 6. *Ad Hoc* com *IPSec*, *AODV* e *WEP*

Consolidando-se os cenários, testados entre as duas máquinas, percebe-se o comportamento de uma rede *Ad Hoc* sem mecanismos de segurança e o efeito dos mecanismos que foram implementados.

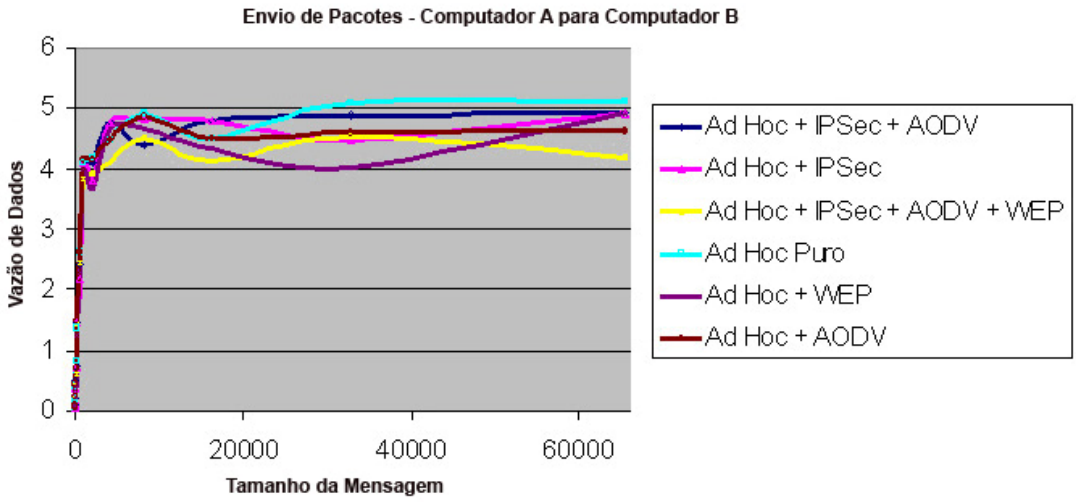

Figura 3. Vazão de dados nos seis cenários implementados.

Verifica-se que a sobrecarga do *IPSec* é maior que a do protocolo *WEP*. Este fato é devido aos mecanismos de segurança do *IPSec* (método de autenticação, confidencialidade do *ESP* e integridade do *SHA1*) serem mais sofisticados. Ambos, os protocolos, juntamente com o *AODV* degradam o desempenho da rede.

5. Conclusões

Neste trabalho apresentou-se um estudo sobre a influência da sobrecarga introduzida nas redes 802.11b pelos mecanismos de segurança *WEP* e *IPSec* sobre uma rede *Ad Hoc*. Os resultados obtidos mostraram que esses mecanismos introduzem informações adicionais de controle na rede que reduziram a vazão de dados se comparamos com o primeiro cenário, onde configurou-se apenas uma rede *Ad Hoc*, sem mecanismos de segurança.

Vê-se que os pontos máximos atingidos pelas transmissões são quase iguais, menos no caso da transmissão com o nível de segurança utilizando-se o protocolo *WEP*

e o *IPSec*. 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 criptografia e decriptografia, os quadros da camada de enlace possuem 8 bytes de informações adicionais, compostas pelo *IV* e pelo *ICV*. A sobrecarga se demonstra quando vemos a linha que corresponde ao cenário seis (*Ad Hoc* com *IPSec*, *AODV* e *WEP*) onde a vazão de dados diminui de forma significativa.

Para *WLANs* (*Wireless Local Area Network*) que não necessitam de um alto nível de segurança, recomenda-se utilizar o protocolo de criptografia *WEP* com 128 bits. Já em ambientes que a confidencialidade dos dados é uma prioridade, recomenda-se a utilização de *VPNs* (*Virtual Private Network*). Entretanto, se introduzirmos os protocolos *WEP* e *IPSec*, percebe-se na prática que a segurança não afeta de maneira eficiente a vazão de dados.

Observando-se as tecnologias de segurança, percebe-se, por outro lado, que há um legado de componentes, para rede sem fio com padrões antigos de tecnologias, utilizados no mercado. Em trabalhos futuros pode-se implementar novas simulações práticas e analisar o impacto dos novos mecanismos de segurança para redes sem fio (802.11i). Além disso, pode-se inserir mais dispositivos para possibilitar o roteamento de pacotes, com mais rotas disponíveis, na rede sem fio.

Referências

B. Dahill, B. N. Levine, E. Royer e C. Shields. (2002) "A Secure Routing Protocol for Ad Hoc Networks", Conference on Network Protocols (ICNP), pp. 2.

Y. Zhang e W. Lee.(2003.) "Intrusion Detection in Wireless Ad Hoc Networks", ACM Wireless Network Journal.

Kullberg, Tuulia. (2004) "Performance of Ad-hoc On-Demand Distance Vector Routing", Seminar on Internetworking, Helsinki University of Technology, pp. 1.

RSA Security Inc. (2003), "RC4: Encrypty Algoritm of RSA Security", http://www.rsasecurity.com

E. M. Royer, Chai-Keong Toh, (1999) "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, Vol. 6, No. 2, pp. 46-55.

M. P. Joseph, Corson. M. Scott. (1998) "Móbile Ad Hoc Networking and the IETF". Mobile Computing and Communications Review, vol. 2, número 4.

S. Sanghari, T. Brown, S. Bhandare. S. Doshi, (2003) "Ewant: The Emulated Wireless Ad Hoc Network Testbed". Universidade do Colorado, pp 5, IEEE.

E. M. Royer. (2003) "Ad Hoc On-Demand Distance Vector Routing", Request for Comment RFC 3561.

Hewlett-Packard Company, (2003) "Public Netperf Homepage",

http://www.netperf.org/netperf/NetperfPage.html

Meredith, Gail. (2002) "Decoding IPSec, Understanding the Protocols of Virtual Private Networks". Second Quarter. Cisco Systems.