Instituto Alberto Luiz Coimbra
de Pós-Graduação
e Pesquisa de Engenharia
Universidade Federal
do Rio de Janeiro

Programa de Engenharia de Sistemas e Computação

Segurança em Redes Ad Hoc

Orientador:

Luís Felipe M. de Moraes

moraes@ravel.ufrj.br

Aluno:

Luciano Renovato de Albuquerque

aluciano@ravel.ufrj.br

Junho de 2003

Resumo

A área de redes sem fio tem sido muito estudada atualmente. O grande potencial para possíveis aplicações, utilizando essa tecnologia, certamente tem sido um grande incentivo. Dentro dessa área, as redes Ad Hoc, foram relativamente pouco estudadas, havendo muito para ser desenvolvido e pesquisado.

Esse trabalho foi desenvolvido com o objetivo de entender a maneira como funciona uma rede Ad Hoc móvel, tendo como referência as questões de segurança. As possíveis falhas de segurança são estudadas, além de alternativas para solucionar ou pelo menos, amenizar os problemas que elas acarretam. No último capítulo uma proposta de melhoria para o funcionamento de um protocolo seguro é sugerida.

Conteúdo

Lista de Figuras

Capítulo 1

Redes Sem Fio

1.1 Introdução

As redes sem fio possuem características que as tornam mais suscetíveis a ataques. Isso ocorre principalmente pelo fato de seu meio de transmissão ser o ar.

Por se tratar de um meio de transmissão completamente aberto, técnicas que garantam a leitura dos dados apenas por seus respectivos destinatários são imprescindíveis. Em uma rede sem fio, basta que um dispositivo com capacidade de comunicação sem fio esteja dentro do raio de transmissão de outro, para que ele seja capaz de ouvir tudo que estiver sendo transmitido.

Tamanha facilidade de acesso indevido não ocorre em redes cabeadas, simplesmente pelo fato de ser necessário, antes de qualquer tentativa, que o atacante conecte seu dispositivo, por exemplo um notebook, à rede através de um hub ou roteador. Obviamente, ter acesso a um desses dispositivos que permitam acesso ao meio de transmissão da rede, não costuma ser tão fácil como simplesmente estar dentro do raio de transmissão de um dispositivo de comunicação sem fio.

Técnicas de criptografia são indispensáveis para garantir o mínimo de restrição no acesso aos dados sendo transmitidos através do ar. Um exemplo muito conhecido e já explorado é o protocolo WEP. Naturalmente, o objetivo desse protocolo é permitir que apenas os indivíduos realmente envolvidos numa determinada comunicação, tenham acesso aos dados sendo transmitidos relativos a mesma.

Esses comentários, sobre problemas relativos a redes sem fio, foram importantes

antes de entrarmos no ponto que realmente importa nesse trabalho. Quando imaginamos que um dos principais problemas de uma rede sem fio, é o fato de seu meio de transmissão ser facilmente acessado indevidamente, estamos levando em consideração redes infra-estruturadas, onde a instalação e configuração de mecanismos de segurança podem ser feitas baseadas em conhecimentos obtidos em redes cabeadas, certamente com as adaptações e melhorias necessárias.

O mais importante a ser notado nessa questão, é o fato de uma rede sem fio infra-estruturada possuir pontos em sua topologia, que permitem a implementação de mecanismos de segurança de forma análoga a redes cabeadas. Esses pontos centrais, como por exemplo roteadores, são extremamente importantes, pois sabemos que é através deles que os usuários terão seus dados transmitidos, permitindo observar cada um deles.

Nesse trabalho trataremos de questões relativas a segurança em redes sem fio, sem infra-estrutura e móveis. Veremos que a mobilidade da rede traz ao mesmo tempo inúmeras vantagens e desvantagens. Quanto a segurança da rede, perceberemos que a questão se torna ainda mais complicada, sendo a implantação de mecanismos de segurança mais complexa e custosa.

1.2 Redes Ad Hoc Móveis

As redes sem fio e sem infra-estrutura, são conhecidas como redes Ad Hoc. Nesse trabalho veremos os problemas de segurança encontrados nesse tipo de rede, levando em consideração um fator agravante em relação a segurança, a mobilidade que torna a topologia da rede dinâmica.

Podemos dizer que a principal característica de uma rede Ad Hoc, é a capacidade de comunicação entre qualquer um de seus membros sem a necessidade de uma infra-estrutura. Para tornar isso possível, cada um dos membros de uma rede Ad Hoc, deve ser capaz de encaminhar os pacotes de dados transmitidos pelos demais membros. Dessa forma, fazendo papel de roteador, garantindo a transmissão dos pacotes entre suas origens e destinos. Para o pleno funcionamento da rede, todos os seus nós devem ter a capacidade de roteamento de pacotes.

Os nós dessas redes, capazes de comunicarem-se diretamente, sem a necessidade de encaminhar seus pacotes através de nós intermediários, são considerados vizinhos.

Quando é necessário utilizar nós intermediários, por se tratar de uma rede onde seus membros são dispositivos móveis, é necessário realizar uma etapa conhecida como descoberta de rota. Onde uma nova rota entre a origem e o destino será descoberta, caso uma rota ainda não seja conhecida.

Esses são dois pontos de extrema importância para analisarmos uma rede Ad Hoc, levando em consideração características fundamentais:

- Predisposição de seus membros a colaborarem com o encaminhamento dos pacotes de todos os outros nós.
- Inexistência de um ponto central de controle.

Infelizmente, veremos que apesar dos pontos citados acima, serem os quais nos permitem imaginar aplicações para redes desse tipo, onde nenhuma outra rede, a princípio, seria mais adequada, também geram agravantes para a dificuldade encontrada em garantir algum nível de segurança para seus usuários.

Além de possíveis ataques, facilmente realizáveis pelo simples não encaminhamento de pacotes, existe a possibilidade da escassez de recursos impedir, sem que haja a intenção de um ataque, que um determinado nó encaminhe pacotes para os demais nós da rede. Quando falamos em escassez de recursos, estamos levando em consideração que os membros de redes Ad Hoc móveis seriam dispositivos de relativa baixa capacidade, onde o fornecimento de energia para os mesmos, é feito através de baterias de carga bastante limitadas.

Certamente, a predisposição à colaboração de cada um dos nós da rede, é um ponto extremamente frágil de uma rede desse tipo. Como citado no parágrafo anterior, ações muito simples, contrárias a essa importante característica, podem acarretar grandes problemas. Para amenizar ou simplesmente identificar, problemas relativos a segurança da rede, é necessária a implantação de mecanismos de segurança. Sendo assim, surge um outro desafio inerente a redes Ad Hoc, pois a não inexistência de um ponto central de controle na rede, inviabiliza a utilização de técnicas já conhecidas, como por exemplo firewalls e IDS (Intrusion Detection Systems), da mesma forma como são utilizadas em redes infra-estruturadas.

1.3 Roteamento

Na seção anterior vimos que pode ser necessário encaminhar pacotes através de nós intermediários, para que alcancem seu destino. Além disso, a rota necessária pode não ser conhecida, o que torna necessário a descoberta de uma rota apropriada.

Dentro desse contexto entram os protocolos de roteamento, foco principal no que diz respeito a segurança em redes Ad Hoc. Principalmente, por serem neles encontrados as principais falhas de segurança.

Os protocolos de roteamento são responsáveis por encontrar, estabelecer e manter rotas entre dois nós que desejam se comunicar.

Quando um nó deseja enviar uma mensagem para outro, ele pode optar por estabelecer uma rota completa, conhecendo cada nó da rota, ou então, enviar a mensagem para um nó vizinho que conheça uma rota para o destino desejado. Esse nó vizinho por sua vez, iria encaminhar a mensagem optando entre as duas possibilidades, da mesma forma que o nó origem.

É importante que esses protocolos, ao realizarem a manutenção das tabelas de roteamento em cada nó, gerem o mínimo de *overhead* possível e que a quantidade de banda consumida por eles também seja pequena. As atualizações das tabelas de roteamento podem ser realizadas de maneira isolada, distribuída, centralizada ou hierárquica.

A seguir, veremos dois tipos de protocolos de roteamento, os mais citados quando nos referimos a redes Ad Hoc. São classificados como pró-ativos e reativos [1,3,7].

1.3.1 Protocolos de roteamento pró-ativos

Pró-ativos são assim classificados, pelo fato de manterem informações sobre rotas para todos os nós da rede, mesmo que o nó onde o protocolo está sendo executado nunca tenha utilizado muitas dessas rotas, tanto para enviar seus próprios pacotes como para enviar pacotes de outros nós, fazendo papel de roteador.

São usadas mensagens periódicas, trocadas entre todos os nós da rede, para manter a tabela de rotas de cada um constantemente atualizada. Normalmente esse tipo de protocolo consegue ter um melhor desempenho, sendo mais veloz, no tempo de resposta para o nó origem que solicitou uma determinada rota do que protocolos

reativos. Dado que todas as rotas possíveis devem existir na tabela de roteamento de cada nó. O exemplo mais citado desse tipo de protocolo é o Destination-Sequenced Distance Vector (DSDV)[6].

1.3.2 Protocolos de roteamento reativos

São protocolos que realizam o estabelecimento de uma rota, apenas quando ela é solicitada pelo nó origem. Um processo de descoberta de rota é iniciado quando um determinado destino deve ser alcançado, e não existe rota estabelecida para o mesmo. As rotas são mantidas na tabela de roteamento, até que elas deixem de existir ou após um determinado tempo se passar sem serem utilizadas. Como o processo de descoberta de rota é realizado apenas quando uma origem qualquer faz uma requisição, esse tipo de protocolo, normalmente, gera menos overhead do que os pró-ativos, em detrimento do tempo de espera para ter a rota solicitada estabelecida.

Os protocolos Ad-Hoc On Demand Distance Vector (AODV) e o Dynamic Source Routing (DSR) são exemplos de protocolos reativos[2,8].

Após termos visto, brevemente, as possíveis técnicas para desenvolvimento de protocolos de roteamento, iremos conhecer algumas das possíveis técnicas utilizadas para realizar ataques em redes Ad Hoc móveis. Todas elas tendo como principal alvo, as falhas e fraquezas dos protocolos de roteamento, lembrando que inicialmente, esses protocolos foram desenvolvidos sem qualquer preocupação quanto a segurança.

1.4 Possíveis ataques

A natureza de uma rede Ad Hoc faz dela insegura. O grau de comprometimento entre seus membros é alto, já que todos dependem uns dos outros para o pleno funcionamento da rede. A qualidade conseguida depende do trabalho de cada nó. A partir desses comentários podemos perceber que o mau funcionamento de um único nó pode trazer grande prejuízo para toda a rede.

Os protocolos de roteamento desenvolvidos inicialmente não preocuparam-se com os aspectos de segurança, dessa maneira, as vulnerabilidades intrínsecas de uma rede Ad Hoc, devidas ao alto grau de dependência entre seus membros, tornaram-se falhas de segurança para os protocolos de roteamento.

Sendo assim, percebemos que a forma como uma rede desse tipo deve ser protegida não será a mesma adotada em redes cabeadas. Cada um de seus membros deverá estar preparado para enfrentar um adversário, garantindo indiretamente maior grau de segurança para toda a rede. Sabemos que em redes de outros tipos, onde o meio físico compartilhado não é o ar, a segurança total da rede depende, também, das ações preventivas tomadas por cada membro, porém em redes Ad Hoc essas ações têm um significado ainda mais forte.

Nós inimigos ou comprometidos podem participar do processo de descoberta de rotas e aproveitar-se disso. 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 [1,4,5,10].

Os pacotes usados pelos protocolos de roteamento quando sujeitos a ações como as citadas no parágrafo anterior podem causar:

- Rotas com loops
- *Timeouts* demorados
- Métricas falsas ou exageradas
- Repetição de *updates* antigos/desatualizados

Levando a negação de serviços (DoS).

Baseado no funcionamento de alguns protocolos de roteamento, veremos a seguir alguns ataques que podem ser realizados explorando suas falhas.

1.4.1 Alteração do campo destination sequence numbers

O campo *destination sequence numbers* utilizado pelo protocolo reativo AODV, pode ser alterado com o intuito de redirecionar o tráfego da rede e até mesmo impedi-lo de alcançar seu destino. Tomemos como exemplo a topologia de rede a seguir, onde o nó S deseja comunicar-se com o nó D, porém não possui uma rota para o respectivo destino. Nesse exemplo, o nó A seria o primeiro a receber a requisição, propagando-a pela rede até que alcançasse seu destino. Considerando o funcionamento normal da rede, onde o destino receberia corretamente a mensagem de requisição, uma outra mensagem, desta vez uma resposta, seria encaminha através da rede por D, tendo

como destino o nó S. Supondo a presença de um nó mal intencionado na rede, nesse exemplo o nó I, uma mensagem falsa poderia ser enviada para B passando-se por uma resposta de D à requisição recebida, fazendo então com que todo o tráfego enviado de S para D fosse transmitido de B para I. O ataque descrito, poderia ser conseguido simplesmente com a falsificação do campo *destination sequence numbers*, utilizando um valor maior do que o presente no pacote de resposta verdadeiro enviado por D.

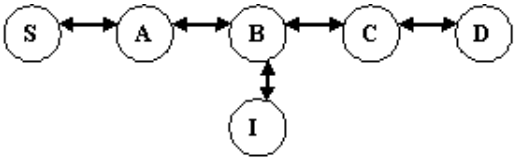

Figura 1.1: Rede Ad Hoc - Sequence Numbers

1.4.2 Alteração da quantidade de saltos

Quando a métrica utilizada por um protocolo de roteamento para escolha de rotas, é simplesmente a quantidade de saltos entre a origem e o destino, pode-se facilmente manipulá-los.

Um determinado nó pode forjar a quantidade de saltos de uma determinada rota, da qual ele deseja fazer parte, obrigando o tráfego a ser transmitido através dela. Também é possível para um atacante impedir que determinada rota passe por ele. Simplesmente, forjando um valor para a quantidade de saltos, maior para a rota que passa através dele, do que a quantidade saltos de pelo menos uma outra rota qualquer. Entretanto, não é apenas o valor de saltos correspondentes a rotas das quais fazem parte, que atacantes podem forjar. Também seria possível, além de forjar a quantidade de saltos, forjar o endereço de origem da mensagem, ou seja, realizar o *spoofing* no endereço de origem das mensagens. Dessa maneira, seria possível forçar a participação de um determinado nó em uma rota, ou até mesmo, impedir sua participação. Em suma, a manipulação do campo correspondente a quantidade de saltos de um protocolo, permite incluir ou retirar nós legítimos e ilegítimos de uma rota.

Vejamos a seguir, através de um exemplo, como a técnica de *spoofing* combinada com a alteração do campo que indica a quantidade de saltos poderia ser usada:

Consideremos a seguinte rede Ad Hoc:

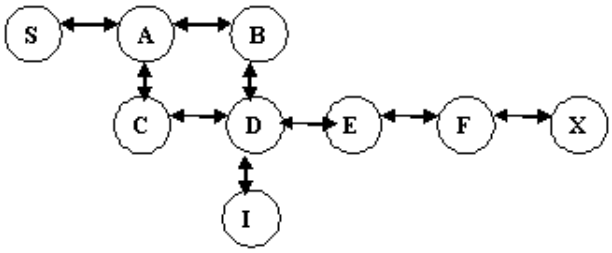

Figura 1.2: Rede Ad Hoc - Loop

Imaginado que o nó S quisesse comunicar-se com o nó X, rotas apropriadas seriam S - A - B - D - E - F - X ou S - A - C - D - E - F - X. Porém se um nó I enviasse mensagens forjadas para D, passando-se por C, ou seja, alterando o endereço de origem da mensagem para o endereço de C, e informando que possui uma rota para X menos custosa do que a rota oferecida pelo nó E, um loop se formaria. Dessa forma, toda informação enviada por S destinada a X, passaria pelos nós A - B - D - C, mas nunca alcançaria seu destino final, retornando sempre de D para C.

1.4.3 Mensagens de erro forjadas

Os protocolos de roteamento, implementam técnicas para manter atualizadas as informações sobre as rotas que possuem em suas tabelas de roteamento. Essas técnicas têm como objetivo perceber o mais rapidamente possível mudanças na topologia da rede.

Usando a figura 1.1 como exemplo, se o nó C, se mover para fora do alcance da transmissão de algum de seus vizinhos, digamos B, ele conseqüentemente deixaria de ser vizinho de B. Então, B teria que perceber essa mudança e atualizar sua tabela, mantendo a rota caso ela ainda estivesse sendo usada ou removendo-a caso ela não fosse mais necessária. Se uma rota alternativa não for encontrada, uma mensagem de erro deverá ser gerada por B, informando que o *link* entre ele e D não existe mais. Essa mensagem deveria ser propagada para os nós anteriores a B, nesse caso o nó A.

Um ataque poderia ser executado forjando mensagens de erro indicando que um determinado *link* teria se desfeito. Imaginemos que o *link* entre B e C, citado no parágrafo anterior nunca tivesse se desfeito. Um atacante, I, poderia enviar mensagens de erro para A usando o endereço do nó B, indicando a quebra do *link* entre

B e C que na realidade nunca teria acontecido. I, poderia fazer isso continuamente impedindo a comunicação entre os nós, realizando assim um ataque de negação de serviço.

1.4.4 Envenenando tabelas de rotas

Alguns protocolos, como por exemplo o *Dynamic Source Routing*, tentam aprender novas rotas observando os pacotes que trafegam na rede.

Quando recebe de maneira promíscua, um pacote que contém informações sobre uma determinada rota que não existe em sua tabela de roteamento, um nó executando esse tipo de protocolo é capaz de incluir essa nova rota em sua tabela.

Essa técnica garante um ganho na eficiência do protocolo de roteamento, porém abre mais uma brecha na segurança. Um atacante poderia se aproveitar dessa característica do protocolo, para forjar mensagens com rotas falsas, utilizando endereços também forjados. Quando os nós da rede recebessem esses pacotes e tentassem aprender com eles, estariam na verdade envenenado suas tabelas de roteamento com rotas falsificadas.

Essa característica do protocolo é opcional, podendo ser desativada sem que o protocolo deixe de funcionar. Mas a conseqüência disso pode ser uma perda considerável em sua eficiência

Capítulo 2

Propostas de Segurança

Segurança é um fator, considerado crítico em qualquer tipo de rede, porém em redes Ad Hoc móveis, trata-se de uma questão ainda mais delicada.

As características e limitações desse tipo de rede, obrigam a qualquer medida de segurança adota, preocupar-se com fatores inexistentes ou menos relevantes em outros tipos de redes. Sendo a maior divergência, a inexistência de uma infra-estrutura.

Obviamente, foi levando em consideração as características sobre as quais falamos nas seções anteriores, tendo como objetivo eliminar as falhas de segurança e os efeitos advindos dessas falhas, além daqueles inerentes a própria concepção de uma rede Ad Hoc móvel, que foram propostos alguns mecanismos de segurança.

Dentre os métodos que vêm sendo propostos e desenvolvidos, poderíamos identificar, basicamente, dois grupos distintos. Vale ressaltar, que mesmo os métodos classificados dentro do mesmo grupo, provavelmente utilizam técnicas distintas para alcançarem seus objetivos.

Assim, identificamos os dois grupos a seguir:

- Técnicas de avaliação de comportamento[13,14,19,27]
    - Modo promíscuo
- Protocolos Seguros[1,5,9,10,11]
    - Autenticação
    - Criptografia

2.1 Técnicas de avaliação de comportamento

2.1.1 A técnica Watchdog

A técnica chamada de *watchdog*, apresentada em [13], tem como objetivo identificar nós móveis que estejam apresentando um comportamento inadequado dentro da rede Ad Hoc. Através de observações feitas nas transmissões dos nós, é possível saber se um determinado nó esta deixando de encaminhar pacotes, e assim, prejudicando o desempenho de outros nós, ou até mesmo os impedindo de realizarem suas comunicações. Esse comportamento pode ser apresentado por nós maliciosos, com a intensão de prejudicar outro nó ou a rede como um todo, ou por um nó que simplesmente deseje economizar seus recursos. Necessariamente, nos dois casos a rede será influenciada, tendo uma queda no seu desempenho.

Para entender o funcionamento do *watchdog*, levemos em consideração o seguinte cenário:

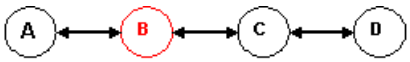

Figura 2.1: Nó B utilizando watchdog

Nesse cenário o nó A deseja comunicar-se com D, mas como os dois não estão perto o suficiente um do outro para fazerem isso diretamente, devem usar os nós intermediários B e C como roteadores. Supondo que o nó B esteja utilizando o *watchdog*, ao encaminhar os pacotes de A para C, o nó B permanece ouvindo o meio de transmissão, além de armazenar uma cópia dos pacotes enviados, em uma fila.

Os pacotes permanecem nessa fila, até um pacote igual seja transmitido pelo nó C ou até o tempo limite de permanência se esgote. Por se tratar de uma transmissão sem fio, todos os nós dentro do raio de alcance de C poderão ouvir a transmissão. Obviamente, a técnica de *watchdog* se baseia nessa característica relativa a forma de transmissão dos dados.

Quando um nó retira um pacote da fila referente ao *watchdog*, porque o tempo limite de permanência esgotou-se, ele incrementa uma pontuação indicativa da quantidade de vezes que seu nó vizinho, responsável por encaminhar determinado pacote, falhou. Através dessa pontuação, é possível acompanhar o comportamento dos vizinhos, e em determinado momento, caso o mau comportamento de algum dos nós

ultrapasse um limite indesejado, ou seja, sua pontuação ultrapasse um *threshold* pré estabelecido, uma mensagem de alerta é enviada para a origem que está utilizando a rota.

Certamente, a técnica de *watchdog* possui algumas limitações. Em alguns casos pode não ser possível detectar o mau comportamento de um nó. Tenhamos como referência a topologia apresentada na figura 2.1 e vejamos essas situações.

- Colisão incerta - supondo que o nó A estivesse observando o comportamento de B e presenciasse uma colisão, não seria possível afirmar se a colisão foi causada por B ou um outro vizinho qualquer, tornando impossível saber se B nesse momento encaminhou um pacote devidamente ou nunca o fez.
- Colisão no receptor - nesse caso, A conseguiria saber se B encaminhou corretamente um pacote para C, mas não seria capaz de saber se uma colisão impediu C de receber o pacote.
- Potência limitada para transmissão - um nó tentaria controlar sua potência de transmissão, de modo a controlar quais de seus vizinhos seria capaz de ouvi-lo.
- Alerta falso de mau comportamento - um nó poderia tentar propagar informações falsas sobre o comportamento de outro nó, com o objetivo de impedir sua participação na rede.
- Conspiração - nesse caso, dois nós ou mais, poderiam impedir que demais membros da rede soubessem de seu mau comportamento. Por exemplo, se os nós B e C fossem cúmplices, B poderiam encaminhar pacotes para C, mas C, por sua vez, nunca encaminhar esses pacotes. Por serem cúmplices, B nunca informaria A sobre o mau comportamento de C.
- Descarte parcial - um nó poderia descartar pacotes, de maneira a impedir sua classificação pelo *watchdog*, como mau comportado. Mantendo-se sempre dentro do limite estabelecido pela técnica de avaliação de comportamento. Mesmo assim, percebemos um limite mínimo para a transmissão dos nós, forçado pelo *watchdog*.

2.1.2 Evitando rotas

Além da utilização desse processo que permite acompanhar o comportamento de nós numa rede Ad Hoc, é preciso um mecanismo que saiba usar essa informação a

respeito dos nós, com o objetivo de impedi-los de continuar participando da rede.

Em [13], os autores apresentam o *pathrater* que realiza um trabalho complementar ao do *watchdog*. Esse outro mecanismo, baseia-se nas informações obtidas sobre o comportamento dos nós, e também, nas informações conseguidas através da camada de enlace. Assim, é possível avaliar as possíveis rotas entre uma origem e um destino, de acordo com sua disponibilidade. Dando maior prioridade para aquelas rotas que apresentarem melhores condições para utilização.

Um nó utilizando o *pathrater*, quando conhece um novo nó, podendo esse nó ter recentemente ingressado na rede, ou devido a mobilidade, somente agora ter se tornado um nó vizinho, o atribui uma taxa inicial de 0.5. Para si mesmo, o nó atribui uma taxa igual a 1.

Cada nó tem sua taxa incrementada de 0.01 a cada 200 ms, sendo a taxa atualizada em todas as rotas ativas. Uma rota deve ter tido pacotes encaminhados dentro dos últimos 200 ms, para que seja considerada ativa. Quando um link é perdido e um nó fica inacessível, sua taxa é decrementada de 0.05, podendo atingir o valor mínimo 0.

Os nós com taxas entre os limites 0.0 e 0.8, são considerados neutros. Ao ser informado pelo *watchdog* que determinado nó tem se comportado indevidamente, o *pathrater* atribui o valor negativo -100 para esse nó. Segundo os próprios autores, é aconselhável permitir o reingresso de um nó excluído à rede após um período adequado, apesar de não terem descrito uma maneira para isso.

2.2 Protocolos seguros

2.2.1 Authenticated Route for Ad Hoc Networks (ARAN)

Esse protocolo, o qual funciona de forma reativa, vem sendo desenvolvido com o objetivo de garantir a integridade das mensagens de roteamento, além de permitir a identificação da origem de cada mensagem, através da validação dos certificados de cada nó.

Para participar de uma rede Ad Hoc onde o ARAN está sendo utilizado, cada nó, antes de ser capaz de comunicar-se através da rede, deve obter um certificado. Para obtê-lo o nó precisa autenticar-se numa CA (Certification Authority), ou seja,

um Servidor de Certificados.

A necessidade de um Servidor de Certificados, dificulta bastante a utilização do protocolo em questão. Sendo assim, a forma como esses servidores devem estar dispostos na rede, ou até mesmo, se mais de um servidor deve realmente ser utilizado, são questões muito importantes à serem consideradas. A final, além de serem eles os responsáveis por autenticar os nós da rede, fornecendo certificados válidos, também são esses servidores os responsáveis por revogar os mesmo certificados. Dessa forma, percebemos que sua comunicação direta com a maior quantidade de nós da rede, garante maior segurança a medida em que os membros da rede obtêm essas informações, tão sensíveis, diretamente da origem.

Existem dois estágios que podem ser utilizados pelo protocolo ARAN. No primeiro estágio, a rota encontrada entre a origem e o destino, não tem garantia alguma de ser a menor rota possível, levando em consideração a quantidade de nós intermediários na rota. Já o segundo estágio, certamente sendo mais custoso, exigindo maior processamento e consumo de banda, garante que a rota utilizada é a menor possível. Entretanto, o segundo estágio é opcional, o que é perfeitamente compreensível quando lembramos que a rota encontrada no primeiro estágio, mesmo podendo não ser a menor, é a com menor tempo de retardo entre a origem e o destino.

Quando um nó origem necessita de uma rota para um destino qualquer, ele inicia o processo de descoberta de rota. Cria um pacote contendo seu certificado digital e o assina, encaminhando-o através da rede por *broadcast*. É importante frisar que apenas o nó destino da requisição poderá responder a mesma.

Os nós vizinhos a origem da requisição, receberão o pacote e validarão sua assinatura. Tratando-se de um pacote assinado devidamente, esse vizinho, por sua vez, assina o pacote e inclui seu certificado no mesmo, sem remover nenhum dado do pacote original.

Os próximos vizinhos a receberem o pacote de requisição, antes que ele chegue ao destino, seguirão o mesmo procedimento:

1. Validar o certificado do nó vizinho que enviou o pacote
2. Remover o certificado do nó vizinho que enviou o pacote
3. Incluir o próprio certificado no pacote
4. Encaminhar o pacote através da rede

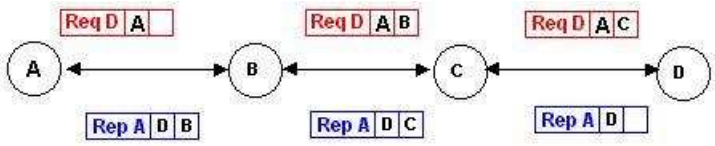

Figura 2.2: Processo de descoberta de rota - Primeiro estágio

Alcançando o no destino, a requisição é mais uma vez validada quanto a seu certificado, sendo que dessa vez, o certificado do nó origem também é validado. Sendo considerados válidos, o destino criará um pacote de resposta à requisição e o encaminhará de volta à origem da requisição. O pacote criado será assinado pelo destino e também deverá conter seu certificado.

No momento em que a origem da requisição recebe a resposta enviada pelo destino, ela verifica a autenticidade do pacote, tendo em vista que apenas o destino poderia ter respondido sua requisição, ou seja, nenhum nó intermediário, mesmo conhecendo uma rota para o destino desejado, poderia responder a requisição feita. Essa limitação do ARAN tem o objetivo de garantir maior segurança evitando, por exemplo, a formação de *loops* numa rota.

Além de uma possível perda na eficiência no processo de requisição de rotas, o protocolo obriga a criação de uma entrada na tabela de roteamento, para cada par origem-destino.

A grande diferença no funcionamento do primeiro estágio do protocolo ARAN, para seu segundo estágio, é a necessidade de que todos os nós intermediários, entre a origem e o destino da requisição, assinem o pacote antes de encaminhá-lo através da rede, porém sem remover a assinatura do pacote vizinho que o encaminhou anteriormente.

Sendo assim, ao alcançar o nó destino, o pacote de requisição conterá o caminho completo desde a origem.

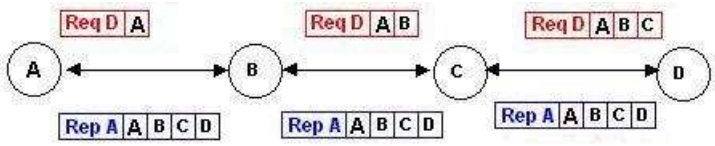

Figura 2.3: Processo de descoberta de rota - Segundo estágio

Durante a existência de uma rede Ad Hoc, um nó que tenha obtido um certificado, pode ter o mesmo revogado pelo Servidor de Certificados. Para isso, um mensagem de revogação é encaminhada através da rede, e todos os nós devem recebe-la, tomando conhecimento de que o nó referenciado nessa revogação, não deve ter seus pacotes encaminhados através da rede.

Obviamente, devido a própria mobilidade da rede Ad Hoc, esse processo pode encontrar problemas, existindo a possibilidade da revogação não se tornar conhecida por todos os membros da rede. Apesar disso, o fato de apenas alguns nós receberem a mensagem de revogação, já é um fator limitante para a participação desse nó.

A figura a seguir exemplifica um caso onde o nó que faz a ligação entre as duas partições da rede Ad Hoc, tem seu certificado revogado. Porém, sua posição estratégica o permite, pelo menos momentaneamente devido a mobilidade dos nós, impedir que todos os membros da rede saibam da revogação.

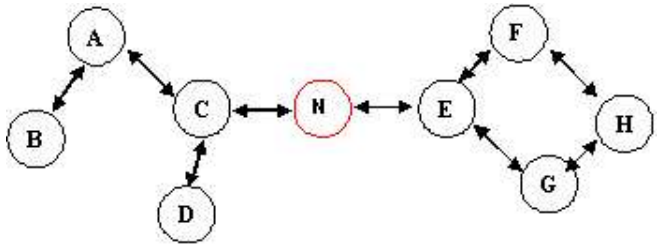

Figura 2.4: Nó N tem a possibilidade de impedir a propagação de sua revogação

2.2.2 Simulação do protocolo

Os gráficos a seguir mostram o desempenho de uma rede Ad Hoc móvel, obtidos a partir de simulações utilizando o simulador *Global Mobile Information* (GloMoSim).

Para as simulações, foram utilizados o protocolo 802.11 na camada MAC e tráfego de dados CBR sobre UDP. Utilizando uma configuração com 20 nós, numa área de 670m x 670m e outra com 50 nós, utilizando uma área de 1000m x 1000m. O posicionamento inicial dos nós foi obtido de forma aleatória e a mobilidade utilizando o modelo *waypoint*. A transmissão de cada nó possui o alcance de 250m. A taxa de transmissão dos nós é de 4 pacotes/segundo, sendo cada pacote do tamanho de 512 bytes.

Os gráficos nos permitem comparar os resultados obtidos para o protocolo seguro

ARAN e o protocolo AODV, o qual não implementa nenhuma técnica de segurança.

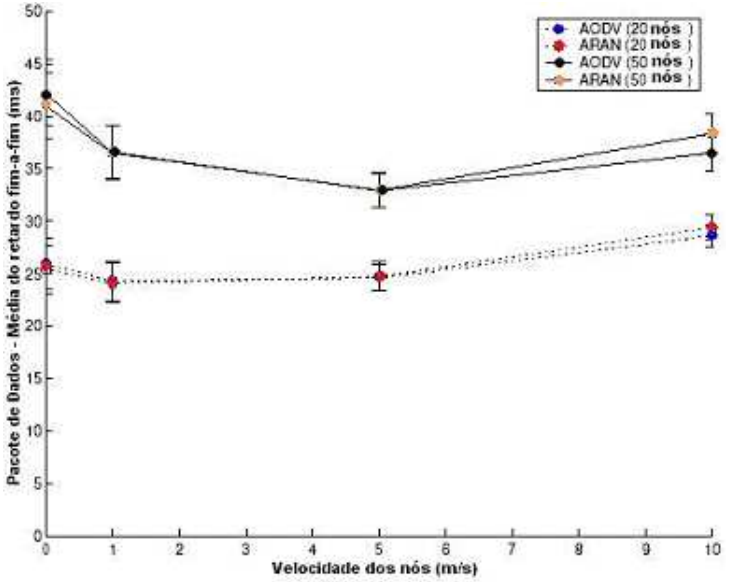

Figura 2.5: Retardo fim-a-fim para os pacotes de dados

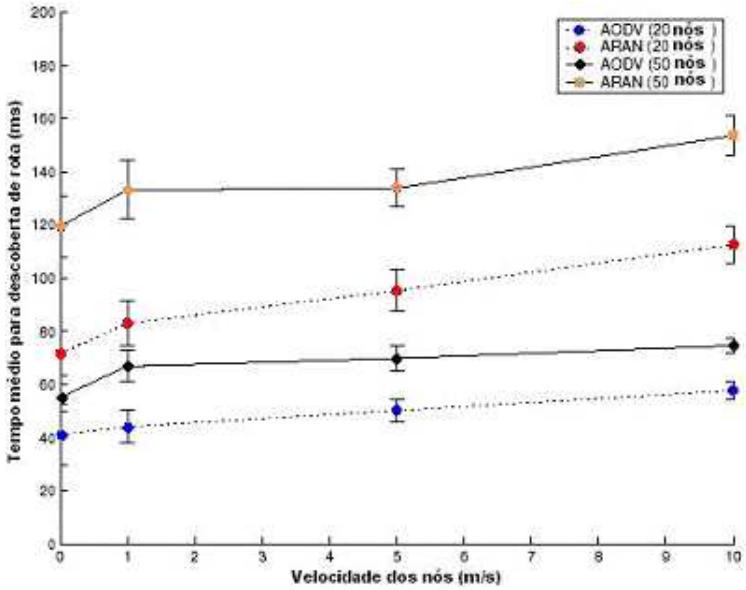

Figura 2.6: Tempo médio para Descoberta de rota

Podemos observar que o tempo médio de retardo fim-a-fim, é muito próximo para os dois protocolos, o que pode a princípio parecer estranho quando analisamos o gráfico da figura 2.6, onde vemos que o tempo médio para descoberta de rota do protocolo ARAN é bem maior que no AODV, nos dois cenários simulados.

Porém, é preciso lembrar que a quantidade de pacotes utilizados no processo de descoberta de rota, é muito inferior a quantidade de pacotes de dados transmitidos. Sendo assim, percebemos que o tempo de descoberta de rota, influenciou relativamente pouco no retardo fim-a-fim no gráfico da figura 2.5.

Capítulo 3

Técnica de Observação de Comportamento + Protocolo Seguro

3.1 Combinando as duas propostas

As duas técnicas sobre as quais falamos nas seções anteriores, tanto a implementação do protocolo seguro ARAN, quanto a observação de nós vizinhos através da utilização do *watchdog*, visam impedir ou minimizar a ação de nós comprometidos ou atacantes.

Analisando o protocolo ARAN, percebemos que seu funcionamento é semelhante ao do protocolo AODV, exceto por não permitir a resposta à uma requisição, durante o processo de descoberta de rota, ser feita por um nó intermediário, certamente, conhecedor de uma rota para o destino da requisição.

Essa característica, foi criada pelos autores do protocolo ARAN, com o objetivo de garantir maior segurança no processo de descoberta de novas rotas. Basicamente, impedindo a resposta de um nó intermediário à uma requisição para a qual ele possui a rota desejada, não permite que um nó qualquer, mesmo estando devidamente autenticado, tente forjar uma rota. Entretanto, o tempo de duração do processo de descoberta de rota deve ser o menor possível, um desejo natural em qualquer tipo de rede, sendo que numa rede Ad Hoc móvel, esse fator pode ter uma influência ainda mais determinante.

Dentro desse contexto, seria interessante criarmos condições para que um nó intermediário fosse capaz de responder a uma requisição, garantindo maior eficiência no processo sem diminuir o nível de segurança. Então, imaginamos que o *watchdog* e o protocolo ARAN, poderiam ser utilizados de forma complementar. Utilizando o *watchdog* de forma bastante específica, selecionando os nós onde ele deveria ser executado.

Os passos a seguir representam o funcionamento do protocolo seguro, adicionando a técnica de *watchdog*:

1. Nó S deseja comunicar-se com X, porém não conhece uma rota para o mesmo.
2. Nó S inicia o processo de descoberta de rota para X, encaminhando uma requisição através da rede.
3. Os nós vizinhos de S, A e B recebem a requisição e fazem a validação da mensagem.
4. Como não possuem a rota desejada, encaminham o pacote para seus vizinhos.
5. O nó D, conhece a rota desejada e responde a requisição, encaminhando uma mensagem para S.
6. Quando recebe a resposta, B deve perceber que a requisição não foi respondida pelo no destino, mas sim, por seu vizinho D.
7. B deve agora validar a assinatura de D e encaminhar a resposta através da rede, caso a validação seja verdadeira.
8. Além do passo anterior, por ser o nó vizinho do nó intermediário a responder a requisição, B deve iniciar o watchdog. Mantendo seu vizinho D em observação.
9. A mensagem de resposta sendo encaminha até S, seguirá o procedimento normal do protocolo seguro ARAN.

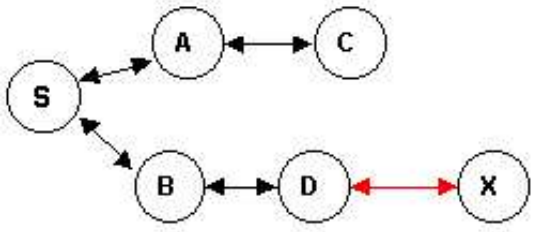

Figura 3.1: Nó intermediário respondendo requisição

Utilizando o *wotchdog*, no passo 8, foi possível permitir ao nó intermediário D responder a requisição, diminuindo o tempo de duração do processo de descoberta de rota. Assim, estabelecendo uma nova característica ao processo, a qual permitirá a avaliação da veracidade da informação emitida por D, ou seja, pacotes encaminhados através dessa nova rota, serão observados no momento em que estiverem sendo encaminhados através do nó D, assim sendo, B deverá ouvir todos os pacotes que encaminhar para D através da rota em questão.

Com a utilização dessa nova etapa, dentro do funcionamento do protocolo ARAN, esperamos uma diminuição do tempo médio de duração do processo de descoberta de novas rotas. Lembrando, que o fato de um nó intermediário responder à requisição de uma nova rota, certamente diminui a quantidade de saltos necessários para finalizar o processo de descoberta, o que leva a um menor número de nós participando desse processo.

3.2 Ganhos esperados

- Diminuição do tempo médio de duração do processo de descoberta de rota.
- Diminuição da quantidade de nós participantes do processo de descoberta de rota.

Além da melhora esperada no desempenho, pelo fato do tempo médio de duração do processo de descoberta de rota diminuir, esperamos reduzir as chances de um nó comprometido participar do processo, dado a diminuição na quantidade de nós participantes na requisição.

Capítulo 4

Considerações Finais

4.1 Conclusão

Esse trabalho permitiu identificar uma possível melhoria no funcionamento do protocolo seguro ARAN, através da utilização de uma outra técnica de segurança, o *watchdog*. Visando ganhos no desempenho de uma rede Ad Hoc.

No capítulo 1, vimos os dois tipos básicos de protocolos de roteamento, próativos e reativos, comentando o modo como funcionam. Então, vimos alguns dos problemas enfrentados em redes Ad Hoc, originários das falhas de segurança desses protocolos de roteamento.

No segundo capítulo, vimos duas propostas de segurança e as classificamos em dois grupos, técnicas de avaliação de comportamento e protocolos seguros. Dentro de cada grupo vimos um exemplo de proposta, o *watchdog* e o protocolo ARAN. Estudamos o funcionamento de cada um, para que pudéssemos entender como seria possível funcionarem de forma complementar, com o objetivo de melhorar o desempenho do protocolo sem aumentar a insegurança da rede, dados os problemas e falhas que pudemos observar anteriormente.

Dentro do capítulo 3, vimos como seria possível combinar o funcionamento do protocolo ARAN e a técnica *watchdog*, identificando onde e qual deveriam ser as mudanças dentro do protocolo seguro. Conhecendo o funcionamento de cada uma das técnicas, e entendendo onde e como elas poderiam ser combinadas, como feito nesse capítulo, é possível implementar a proposta em questão e obter resultados que permitam uma avaliação comparativa.

4.2 Trabalhos Futuros

Para uma avaliação concreta dos ganhos obtidos com a utilização da mudança proposta nesse trabalho, é necessária sua implementação. Por conseguinte, a simulação do seu comportamento e obtenção de dados que permitam avaliar, por exemplo, o retardo fim-a-fim, tempo médio para descoberta de rotas, vazão etc.

Bibliografia

[1] S. Yi, P. Naldurg, and R. Kravets. Security-Aware Ad-Hoc Routing for Wireless Networks. August 2001.

[2] Minicursos. *SBRC*, 2002.

[3] E. M. Royer and C. K. Toh. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. *IEEE Personal Communications*, 1999.

[4] Y. Zhang and W. Lee. Intrusion Detection in Wireless Ad Hoc Networks. *MobiCom'2000*, August 2000.

[5] B. Dahill, B. N. Levine, E. Royer, and C. Shields. A Secure Routing Protocol for Ad Hoc Networks. 2001.

[6] C. E. Perkins. Highly Dynamic Destination-Sequenced Distance-Vector Rounting(DSDV) for mobile computers.

[7] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark. Scenario-based Performance Analysis of Rounting Protocols for Mobile Ad-Hoc Networks. *Mobicom*, 1999.

[8] D. B. Johnson, D. A. Maltz, and J. Broch. DSR: The Dynamic Source Route Protocol for Multi-Hop Wireless Ad-Hoc Networks.

[9] Y. Hu, A. Perrig, and D. B. Johnson. Efficient Security Mechanismis for Routing Protocols. *NDSS*, 2003.

[10] Y. Hu, A. Perrig, and D. B Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. *Mobicom*, 2002.

[11] L. Zhou and Z. J. Haas. Securing Ad Hoc Networks. *IEEE Network Magazine 13(6)*, November/December 1999.

[12] S. Lee, B. Han, and M. Shin. Robust Routing in Wireless Ad Hoc Networks. *IWAHN*, 2002.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. *Mobile Computing and Networking*, pages 255–265, 2000.

[14] S. Zhong, J. Chen, and Y. R. Yang. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. *IEEE INFOCOM*, 2003.

[15] L. F. G. Soares, G. Lemos, and S. Colcher. Redes de computadores. 2**?** edição.

[16] J. Binkley and W. Trost. Authenticated ad hoc routing at the link layer for mobile. 1999.

[17] N. Asokan and P. Ginzboorg. Key Agreement in Ad-Hoc Networks. February 2000.

[18] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. On-demand secure routing protocol resilient to byzantine failures. *WiSe'02*, September 2002.

[19] D. Barreto, Y. Liu, J. Pann, and F. Wang. Reputation-based participation enforcement for ad hoc networks. *http://www.stanford.edu/ barretod/reputation.html*, 2002.

[20] P. Papadimitratos and Z. J. Haas. Secure Routing for Mobile Ad Hoc Networks. *CNDS*, 2002.

[21] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu. Adaptative Security for Multi-layer Ad-Hoc Networks. 2002.

[22] P. Papadimitratos and Z. J. Haas. Secure Link State Routing for Mobile Ad-Hoc Networks. 2003.

[23] P. Sinha, R. Sivakumar, and V. Bharghavan. Enhancing Ad Hoc Routing with Dynamic Virtual Infrastructures. *INFOCOM*, 2001.

[24] P. Papadimitratos, Z. J. Haas, and E. G. Sirer. Path Set Selection in Mobile Ad Hoc Networks. *MOBIHOC*, 2002.

[25] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks. 2001.

[26] W. Wang, Y. Lu, and B. K. Bhargava. On Security Study of Two Distance Vector Routing Protocols for Mobile Ad Hoc Networks. *PerCom*, 2003.

[27] S. Buchegger and J. Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. *IEEE Computer Society*, January 2002.

[28] M. G. Zapata. Secure Ad hoc On-Demand Distance Vector Routing. *ACM Mobile Computing and Communications Review (MC2R)*, pages 106–107, July 2002.

[29] S. Ghazizadeh, O. Ilghami, E. Sirin, and F. Yaman. *Security-Aware Adaptive Dynamic Source Routing Protocol*. The 27th Annual IEEE Conference on Local Computer Networks, November 2002.

[30] J. Kong, X. Hong, and M. Gerla. *ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-Hod Networks*. ACM MobiHoc'03, 2003.