UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CURSO DE SISTEMAS DE INFORMAÇÃO

DALTON HEIDEMANN

SIMULAÇÃO DE ATAQUES DE ANÁLISE DE TRÁFEGO EM REDES SEM FIO AD HOC MÓVEIS

FLORIANÓPOLIS - SC, 2010

UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CURSO DE SISTEMAS DE INFORMAÇÃO

DALTON HEIDEMANN

SIMULAÇÃO DE ATAQUES DE ANÁLISE DE TRÁFEGO EM REDES SEM FIO AD HOC MÓVEIS

Trabalho de conclusão de curso apresentado como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador:

Prof. Dr. João Bosco Mangueira Sobral

Membros da Banca:

Prof. Dr. Fernando Augusto da Silva Cruz

Prof. Dr. Bernardo Gonçalves Riso

Prof. Dr. Ricardo Felipe Custódio

Urian Kramer Bardemaker

FLORIANÓPOLIS - SC, 2010

Dalton Heidemann

SIMULÇÃO DE ATAQUES DE ANÁLISE DE TRÁFEGO EM REDES SEM FIO AD HOC MÓVEIS

Trabalho de conclusão de curso apresentado como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: _____

Prof. Dr. João Bosco Mangueira Sobral

Banca examinadora

_____

Prof. Fernando Augusto da Silva Cruz

_____

Prof. Dr. Bernardo Gonçalves Riso

_____

Prof. Dr. Ricardo Felipe Custódio

_____

Urian Kramer Bardemaker

"*Uma mente que se abre a uma nova idéia*
jamais retorna ao seu tamanho original."
Albert Einstein

AGRADECIMENTOS

A minha família, que sempre me deu força em todos os momentos.

Ao meu irmão Diego que sempre esteve presente.

Aos colegas de trabalho.

Por fim, ao meu orientador, fundamental para o devido trabalho.

RESUMO

Redes sem fio ad hoc móveis (MANET – *Mobile Ad Hoc Network*), são inerentemente vulneráveis a diversos ataques, como monitoramento e análise de tráfego, que podem comprometer sua privacidade, devido ao meio compartilhado e à ausência de infra-instrutora fixa,. A fim de evitar a revelação de informações relevantes através dos pacotes de roteamento, pesquisadores propuseram protocolos de roteamento anônimo, ANODR, SDAR, ASR, ANDSR, MASK, ASRP, AnonDSR, CARP e ODAR, e os avalia, quanto a anonimato de identidade, venue, localização, padrão de movimento e rota. Através deste estudo comparativo informal, descobriram-se possíveis vulnerabilidades e obtiveram-se indicações de quais protocolos são mais seguros, anônimo. Esse estudo procurou levantar alguns aspectos de segurança e simular discretamente um dos protocolos descritos e comparados por Tamashiro (2007). Em termos gerais, a pesquisa consistiu em estudar o funcionamento do protocolo anônimo ANODR, simular ataques de análise de tráfego e verificar as propriedades de anonimato, utilizando o simulador de redes QualNet.

PALAVRAS-CHAVE: *Redes Ad hoc, Anonimato, MANET, ANODR.*

ABSTRACT

Mobile Ad Hoc Networks (MANET), are inherently vulnerable to various attacks, such as monitoring and traffic analysis, which can compromise your privacy, due to shared environment and lack of infrastructure, instructor sets,. To avoid disclosure of information through the packet routing, researchers proposed routing protocols anonymous, ANODR, SDAR, ASR, ANDSR, MASK, ASRP, AnonDSR, CARP and ODAR, and evaluate, as anonymity of identity, venue, location, route and pattern of movement. Through this informal comparative study, it was possible vulnerabilities and there were indications of what protocols are more secure. anonymous. This study sought to raise some issues of safety and discreetly simulate one of the protocols described and compared by Tamashiro (2007). Overall, the research was to study the operation of the anonymous ANODR protocol and check the properties of anonymity using the QualNet network simulator.
KEY WORDS: ad hoc networks, anonymity, MANET, ANODR.

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE ABREVIATURAS E ACRÔNIMOS

AD HOC – Do latim, “para isto”

SDAR – Secure Distributed Routing Protocol

ANODR – Anonymous On Demand Routing

AODV – Ad-hoc On demand Distance Vector

CARP – Certificate Free Routing Protocol

CDMA – Code Division Multiple Access

DSR – Dynamic Source Routing

IP – Internet Protocol

MANET – Mobile Ad-Hoc Network

ODAR – On-Demand Anonymous Routing

TCP – Transmission Control Protocol

TDMA – Time Division Multiple Access

TORA – Temporally Ordered Routing Algorithm

UDP – User Datagram Protocol

WLAN – Wireless Local Area Network

WPAN – Wireless Personal Area Network

SUMÁRIO

1. INTRODUÇÃO

Redes sem fio ad hoc móveis são redes constituídas por dispositivos sem fio móveis, chamados nós, que se comunicam diretamente ou através uns dos outros, sem o gerenciamento centralizado de qualquer infra-estrutura. Outras características relevantes são: topologia dinâmica, roteamento distribuído, recursos computacionais e segurança física limitados. Características que as tornam úteis também dificultam a utilização de mecanismos de segurança utilizados em redes estruturadas e as tornam inerentemente vulneráveis a ataques. Um dos mais perigosos é a análise de tráfego, um ataque passivo, difícil de detectar, em que o adversário monitora a rede, a fim de obter e inferir informações relevantes sobre os nós, através da detecção de sinais e análise dos pacotes. Um dos métodos propostos para proteger as redes contra esse ataque são os protocolos de roteamento anônimo.

Com base no estudo comparativo de diversos protocolos apresentado por TAMASHIRO (2007), pretende-se realizar simulações de ataques com intuito de validar as comparações teóricas apresentadas no estudo. A escolha do protocolo foi definida principalmente pela combinação positiva dos aspectos de segurança. Assim, o protocolo escolhido foi o ANODR (KONG & HONG, 2003). Este foi incorporado ao simulador de redes Qualnet (SNT, 2010), onde foi possível utilizar componentes móveis de rede sem-fio para criar um cenário de simulação. Ainda referente aos aspectos de segurança, será apresentada uma fundamentação teórica das redes propostas e suas aplicações. Por fim, será possível fazer um estudo comparativo entre a proposta teórica e o resultado das simulações de ataque.

1.1 Objetivos

1.1.1 Objetivos Gerais

Pesquisas sobre segurança em redes ad hoc têm sido intensificadas nos últimos anos; detecção de intrusão e segurança dos protocolos são alguns dos tópicos. Dentre as propriedades de segurança pesquisadas, tais como integridade, autenticação e confidencialidade, este trabalho enfoca privacidade e anonimato. Mais especificamente, protocolos de roteamento anônimo, cujo objetivo é impedir ou, no mínimo, dificultar a obtenção e inferência de informações, através da captura e da análise de pacotes de roteamento.

Efetuar um estudo teórico e pratico a fim de avaliar os protocolos de comunicação para rede ad hoc.

1.1.2 Objetivos Específicos

- Apresentar com detalhes um protocolo de roteamento anônimo.
- Simular ataques ao protocolo usando uma ferramenta de simulação discreta.
- Analisar os resultados da simulação dos ataques.
- Apresentar uma contextualização teórica das redes ad-hoc móveis e dos protocolos de roteamento anônimo.

1.2 Delimitação do Escopo

De forma geral, esse trabalho será baseado no estudo comparativo dos protocolos de roteamento anônimo realizado por TAMASHIRO (2007). Existe uma limitação quanto ao tipo de ataque, sendo que a análise realizada leva em conta apenas ataques passivos. Pretende-se ainda analisar e simular apenas um protocolo avaliado, assim sua escolha pode não ser a melhor entre as disponíveis (pelo menos não necessariamente). Ainda com relação aos aspectos de segurança, o estudo não irá questionar possíveis ataques ou falhas de segurança em outras camadas (enlace, transporte e aplicação), já que o foco é a camada de rede (roteamento).

1.3 Metodologia

Para a realização desse trabalho, procurou-se seguir a seguinte metodologia:

- ✓ Pesquisar conceitos e aplicações referentes às redes MANET;
- ✓ Apresentar os conceitos e os detalhes de funcionamento do protocolo escolhido;
- ✓ Estudar a ferramenta para simulação e apresentar conceitos relacionados;
- ✓ Simular os ataques a um protocolo previamente definido;
- ✓ Apresentar os resultados.

2. REDES SEM FIO AD HOC MÓVEIS

Este capítulo apresenta um estudo teórico de algumas definições relevantes para a compreensão das redes sem fio ad-hoc móveis. É feita uma breve caracterização dessas redes, relacionando tais aspectos com as aplicações e implicações de segurança. Por fim, alguns protocolos tradicionais de redes ad-hoc móveis são brevemente caracterizados.

2.1 Visão geral

Redes sem fio ad hoc móveis (MANET – *Mobile ad-hoc Networks*) é um termo empregado para designar o tipo de rede que não possui um nó ou terminal especial para o qual todas as comunicações convergem e que as encaminha para os respectivos destinos (este terminal é geralmente designado por ponto de acesso). Desta forma, uma Rede de computadores Ad-hoc é aquela na qual todos os terminais funcionam como roteadores, encaminhando de forma comunitária as comunicações advindas de seus terminais vizinhos.

No modo Ad-Hoc o usuário se comunica diretamente com outro(s). Pensado para conexões pontuais, só recentemente este modelo passou a prover mecanismos robustos de segurança, por conta do fechamento de padrões mais modernos (802.11i). Porém, estes novos padrões exigem placas também mais modernas e que ainda não são a maioria no mercado.

Geralmente, numa rede ad hoc não há topologia predeterminada, e nem controle centralizado. Redes ad hoc não requerem uma infra-estrutura tal como backbone, ou pontos de acesso configurados antecipadamente. Os nós ou nodos numa rede ad hoc se comunicam sem conexão física entre eles criando uma rede “on the fly”, na qual alguns dos dispositivos da rede fazem parte da rede de fato apenas durante a duração da sessão de comunicação, ou, no caso de dispositivos móveis ou portáteis, por enquanto que estão a uma certa proximidade do restante da rede.

Uma rede ad hoc móvel, manet é um conjunto de nós móveis (MNs) formando redes dinâmicas autônomas independentes de qualquer infra-estrutura, uma vez que os nós são móveis, a topologia da rede pode mudar rapidamente e de forma inesperada de uma hora para outra. MNs se comunicam umas com as outras sem a intervenção de uma estação base ou ponto de acesso centralizado. Devido ao raio de transmissão das redes sem fio, múltiplos saltos (hops) podem ser necessários para efetuar a troca de dados entre os nós da rede, daí o

termo “rede multi-hop”. Nessa rede, cada MN atua tanto como roteador quanto como um host. Dessa forma, cada MN participa da descoberta e manutenção de rotas para outros nós.

O conceito de uma rede ad hoc do início da década de 70, quando a U.S DARPA (United States Defense Advanced Research Projects Agency) iniciou o projeto PRNET (Packet Radio Network), para explorar o uso de redes de pacote de rádio num ambiente tático para comunicação de dados. Mais tarde, em 1983, a DARPA lançou o programa SURAN (Survivable Adaptive Network) para expandir a tecnologia desenvolvida no projeto PRNET para suportar grandes redes, e para desenvolver protocolos de rede adaptativos os quais pudessem adaptar-se às rápidas mudanças de condições em um ambiente tático. O último da série dos programas iniciados pela DARPA para satisfazer os requisitos de defesa para sistemas de informações robustos e rapidamente expansíveis foi o GloMo (Global Mobile Information Systems), que teve início em 1994. Enquanto as comunicações táticas militares permaneciam a principal aplicação das redes ad hoc, havia um número crescente de aplicações não militares, tais como conferência e busca e salvamento.

Uma das características que mais distinguem as redes ad hoc é a ausência de infra-estrutura fixa. Outras características incluem um modo de operação ponto a ponto distribuído, roteamento multi-hop, e mudanças relativamente freqüentes na concentração dos nós da rede. A responsabilidade por organizar e controlar a rede é distribuída entre os próprios terminais. Em redes ad hoc, alguns pares de terminais não são capazes de se comunicar diretamente entre si, então alguma forma de re-transmissão de mensagens é necessária, para que assim estes pacotes sejam entregues ao seu destino. Com base nessas características, redes celulares padrão e redes totalmente conectadas não se qualificam como redes ad hoc.

Os nós então são responsáveis por descobrir, dinamicamente, com quais podem se comunicar diretamente e por encaminhar pacotes, cujos destinos não estão no raio de alcance de suas origens (TAMASHIRO, 2007 *apud* HAAS *etal.,* 1999). Na figura 1 é possível perceber essa idéia. Enquanto que os nós A, B e C podem se comunicar diretamente, a comunicação com D depende do roteamento através de C.

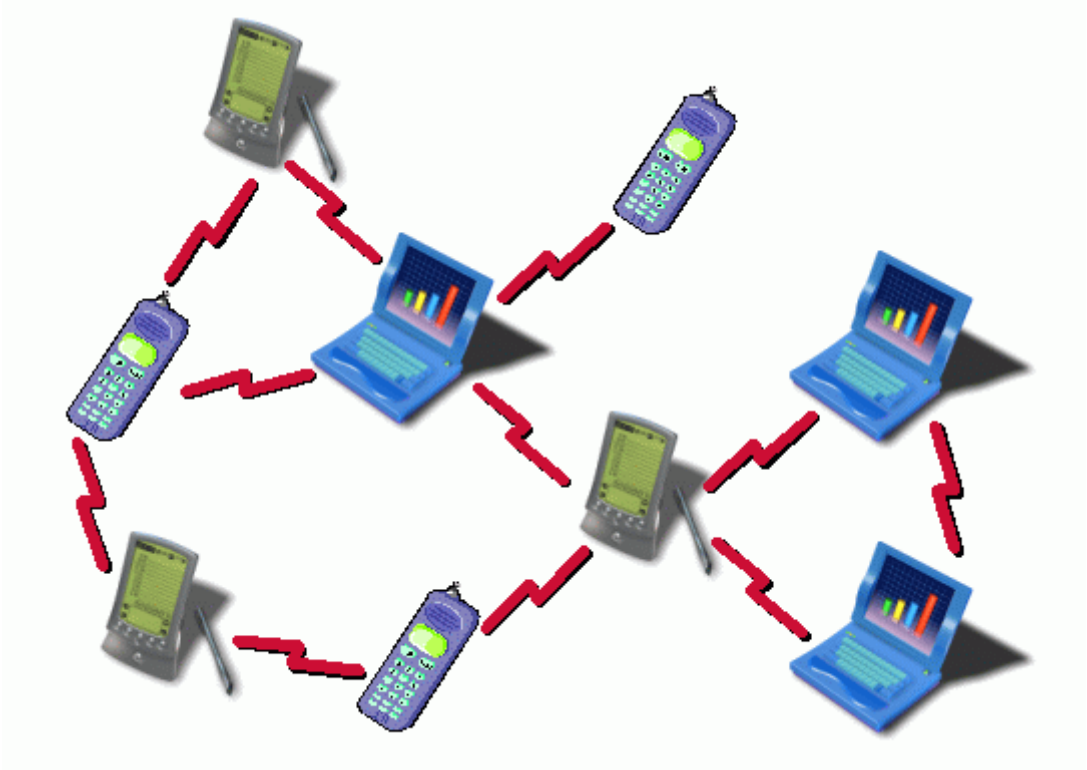

Figura 1: Rede Sem Fio Ad Hoc Móvel

Ainda em relação à natureza de operação da rede, pode-se dizer que o modelo é um sistema autônomo de nós móveis. Segundo CORSON & MACKER (1999), "*uma rede MANET é constituída por nós que são livres para mover-se arbitrariamente*", e ainda que "*o sistema pode operar isoladamente, ou pode ter gateways ou interfaces com uma rede fixa*".

2.2 Característica e Aplicações

As principais características e aplicações, segundo CORSON & MACKER (1999), estão relacionadas com a capacidade de mobilidade e dinamismo da topologia. Os nós são equipados com transmissores e receptores variados, o que caracteriza um modelo altamente dentro de uma mesma área de alcance. Isso indica que um nó A poderia comunicar-se diretamente com C, mas o nó C, devido ao seu transmissor de curto alcance, necessitaria de um nó intermediário para fazer o roteamento.

Esse conjunto de características habilita uma grande variedade de aplicações. Inicialmente o propósito eram as operações militares, estendo-se um pouco depois às de

resgate. A própria tecnologia das redes sem fio ad hoc móveis, segundo CORSON & MACKER (1999), é de alguma forma associada com o termo *Mobile Packet Radio Networking* (PRNet), referente às pesquisas militares nos Estados Unidos nas décadas de 70 e 80, e com as redes WMN (Wireless Mesh Networks), organizadas conforme uma topologia MESH (WIKIPEDIA – MESH NETWORKS, 2008).

Com a popularização das redes sem fio, alguns novos propósitos incluem aplicações de cunho industrial e comercial. O amadurecimento do padrão 802.11 (IEEE 802.11, 2009) contribuiu de forma significativa para essa ampliação comercial. De certa forma pode-se estender sua utilidade para incontáveis novos propósitos (principalmente devido a sua flexibilidade), ou para melhorias em operações de resgate usando satélites e outras topologias autônomas de comunicação.

Em [TAMASHIRO, 2007] é apresentado um quadro que categoriza alguns cenários atuais e futuros das aplicações. O quadro é apresentado na tabela 1.

Tabela 1: Aplicações das Redes Sem Fio Ad Hoc Móveis

Aplicações	Descrição
Redes Táticas	Comunicação em operações militares Batalhas automatizadas
Redes de Sensores	Monitoramento de residências Medição de parâmetros (radiação, calor, etc.) Monitoramento de dados (ex. atividade sísmica)
Emergência	Operações de busca e resgate
Ambientes comerciais	Comércio eletrônico: serviços como pagamento em qualquer lugar Negócios: acesso dinâmico a arquivos armazendos em uma localização central, escritório móvel Veículos: transmissão de notícias, condição das estradas, tempo e música, formação de redes entre veículos próximos
Redes caseiras e corporativas	Redes sem fio locais (WLAN) Redes sem fio pessoais (WPAN)
Aplicações educacionais	Configuração de salas virtuas e de videoconferência Criação de uma rede para comunicação rápida em conferências, encontros e palestras
Redes Mesh	Zonas residenciais: acesso à Internet Auto-estradas: comunicação para os automóveis Zonas comerciais: alternativa à rede de celulares Campus universitário: rede de baixo custo
Entretenimento	Acesso à Internet em ambientes abertos Jogos entre múltiplos jogadores
Localização de serviços	Serviços de informação: localização de serviços como postos de gasolina

Apesar do conjunto de aplicações ser potencialmente infinito, os problemas com segurança podem retardar ou até impedir que certas características das redes ad hoc sejam

realizadas na prática. Uma nova abordagem deve levar em conta requisitos fundamentais de segurança. Uma delas é o anonimato, que garante que nós participantes no roteamento não são capazes de identificar as partes envolvidas. Contudo, as pesquisas nessa área vêm crescendo significativamente nos últimos anos, e até o momento várias propostas foram apresentadas no meio acadêmico. Com a popularização de dispositivos móveis, a adoção de um padrão seguro de roteamento será necessária para estender essas funcionalidades para outras áreas, como redes interligadas de rodovias e carros, e comunicação entre eletrodomésticos.

3. PROTOCOLOS ANÔNIMOS AD HOC MÓVEIS

Esse capítulo tem como propósito apresentar conceitos gerais de segurança de redes computacionais relativas ao anonimato no roteamento dos pacotes. Apresenta ainda algumas propostas teóricas de anonimato para redes estruturadas, que são usadas – na maioria dos casos – como base no processo de roteamento de pacotes e descoberta/manutenção de rotas nas redes ad-hoc móveis. Mais adiante o anonimato em redes ad-hoc móveis é abordado.

3.1 VISÃO GERAL DOS PROTOCOLOS

Algumas soluções para anonimato em redes sem fio ad-hoc móveis foram desenvolvidas ao longo dos últimos anos, sem que nenhuma tenha conseguido obter completo sucesso. Ainda que muitas dessas soluções sejam parecidas na utilização de mecanismos de encriptação e roteamento, alguns detalhes tornam algumas mais apropriadas para certos dispositivos ou não. A tabela 2 mostra um resumo comparativo entre os protocolos apresentados a seguir, levando em conta o anonimato de identidade, localização e padrão de movimento, de rota e de venue (se os nós sabem a sua distância em relação aos nós origem e destino, ou seja, se os pacotes possuem contadores de saltos ou se o seu tamanho indica o número de saltos percorridos; se os pacotes podem ser seguidos até o nó origem ou destino (TAMASHIRO, 2007)).

3.1.1 ANODR ANonymous On Demand Routing [Kong and Hong 2003]

Possui três fases: descoberta, encaminhamento e manutenção. A origem difunde um acote de requisição com um onion (estrutura formada por diversas camadas de criptografia) e um trapdoor, através do qual, somente o destino sabe que é o destinatário final; contém a sua identidade e uma chave de confiança, cifrados com uma chave previamente compartilhada por ele e pelo nó origem, e a sua identidade cifrada com a chave de confiança (é revelada a nós na rota pelo pacote de resposta e, é usada para confirmar a abertura do trapdoor). Cada nó intermediário armazena a chave pública de uso único do nó emissor, contida na requisição, e a substitui pela sua, acrescenta um nonce ao onion e cifra com uma chave simétrica aleatória (o onion gerado pela origem contém a sua identidade cifrada com uma chave simétrica). Quando a requisição chega ao destino, este difunde um pacote de resposta com o onion da requisição, através do qual, os nós verificam se pertencem à rota. Cada nó, na rota reversa, remove uma

camada do onion, cifra-o com uma chave secreta e a cifra com a chave pública recebida na requisição; aquela chave é usada para cifrar salto a salto a carga útil dos pacotes de dados e para gerar uma seqüência de pseudônimos de rota. Quando se detecta a perda de um enlace, um pacote de erro com o pseudônimo do próximo nó na rota é difundido localmente. Para proteger os pacotes de resposta e de dados, utiliza técnicas mixing. Para esconder o tamanho real da requisição e da resposta, cada nó acrescenta um padding aleatório ao onion, de modo que sempre tenha um tamanho fixo.

3.1.2 SDAR - Secure Distributed Anonymous Routing [Boukerche etal. 2004]

Provê um sistema de gerenciamento de confiança, responsável por estabelecer e atualizar níveis de confiança entre nós vizinhos, e possui três fases: descoberta de rota, rota reversa e transferência. A origem difunde um pacote de requisição com o seu hash assinado, um trapdoor (identidade do destino, chave de sessão e tamanho do padding inserido no pacote, cifrados com a chave pública do destino), o nível de confiança desejado e uma chave pública temporária (a chave privada correspondente e a identidade da origem são cifrados com a chave de sessão). Essa chave pública é usada por cada intermediário para cifrar sua identidade, uma chave e um identificador de sessão. As duas últimas informações e a chave de sessão gerada pela origem são usadas pelo destino para criar um onion, que contém um padding também. Através do onion, cada nó, ao receber o pacote de resposta, verifica se pertence à rota. Com a chave de sessão estabelecida com o destino e as chaves dos intermediários, a origem gera um onion dos dados; estes pacotes são enviados por unicast, uma vez que cada nó sabe a identidade do anterior e a do próximo nó.

3.1.3 ASR - Anonymous Secure Routing [Zhu et al. 2004]

É similar ao ANODR [Kong et al. 2005]. As diferenças são: a segunda parte do trapdoor não contém a identidade do destino; a requisição possui um contador de saltos, projetado para ser secreto; as chaves estabelecidas entre nós consecutivos não são usadas para gerar uma seqüência de pseudônimos, mas para cifrar identificadores dos pacotes de dados e de erro; ao invés de um onion, utiliza-se o número de seqüência da requisição no pacote de resposta para os nós verificarem se pertencem à rota.

3.1.4 MASK [Zhang et al. 2005]

Provê processos de pré-configuração e de autenticação de vizinhos e possui três fases: requisição, resposta e encaminhamento. Uma autoridade confiável provê a cada nó um conjunto secreto de pseudônimos e pontos. Quando um nó se move, escolhe um novo pseudônimo e estabelece chaves secretas e identificadores de enlace com seus vizinhos, através de mapeamento bilinear e funções hash. A origem difunde um pacote de requisição com seu pseudônimo ativo e a identidade do destino. Cada nó intermediário armazena o pseudônimo e o substitui pelo seu. Quando a requisição chega ao destino ou a intermediários que conhecem rotas válidas, difunde-se um pacote de resposta, que contém o próximo identificador de enlace compartilhado com o nó anterior e a identidade do destino cifrada com a chave secreta correspondente. Estes identificadores e chaves são utilizados também nos pacotes de dados para identificar o próximo salto e cifrar salto a salto sua carga útil, respectivamente; mudam a cada pacote encaminhado. Utiliza técnicas mixing em situações de pouco tráfego, e intermediários acrescentam paddings aleatórios `a carga útil dos dados.

3.1.5 ANDSR - Anonymous Dynamic Source Routing[de Araujo 2005]

Acrescenta um processo de descoberta de misturadores (responsáveis pelo roteamento) ao protocolo DSR. Antes de iniciar a descoberta de rota, a origem precisa encontrar um misturador vizinho a ele. Após encontrá-lo, envia um pacote de requisição, que contém o seu endereço e o do destino cifrados, respectivamente, com a chave pública do destino e a dos misturadores, e um campo ao qual estes acrescentam seus endereços e que contém o seu endereço cifrado com sua chave pública. O pacote de resposta contém os endereços da origem e do destino, cifrados com a chave pública do primeiro e os endereços de todos os misturadores na rota. Nos pacotes de dados, a carga útil e o endereço da origem são cifrados com a chave pública do destino, e o endereço deste com a chave dos misturadores. No caso de detecção de quebra de enlace, é difundido um pacote de erro.

3.1.6 ASRP - Anonymous Secure Routing Protocol [Cheng and Agrawal 2005]

Possui três fases: requisição, resposta e transmissão. A origem difunde um pacote de requisição com um trapdoor (sua identidade e a do destino e uma chave de sessão, cifrados com a chave pública do destino), uma chave pública e um pseudônimo (temporários). Essas duas últimas informações são armazenadas e substituídas por cada nó intermediário e são utilizadas no pacote de resposta para, respectivamente, identificar o próximo nó e cifrar uma

chave secreta e um novo pseudônimo, que são usados na transmissão de dados. A carga útil dos dados é cifrada com a chave de sessão dos nós finais e salto a salto com as chaves compartilhadas pelos nós consecutivos.

3.1.7 AnonDSR - Anonymous Dynamic Source Routing [Song et al. 2005]

Possui três fases: requisição, resposta e transferência. Antes de iniciar uma comunicação, a origem estabelece parâmetros de segurança (índice e chave secreta, algoritmos criptográficos) com o destino. Os processos de roteamento e de encaminhamento são semelhantes aos processos de ANODR e SDAR. Na requisição, há uma chave pública temporária, um trapdoor (identidade do destino e chave privada, cifrados com a chave compartilhada por eles, e o índice correspondente) e um onion. A chave pública é usada pelos intermediários para inserirem pseudônimos e chaves de sessão no onion, que são usados na resposta para identificar o próximo nó e para gerar um onion. Do mesmo modo, são usados nos pacotes de dados; é gerado um onion da carga útil de dados com essas chaves e a chave compartilhada pelos nós finais. Para evitar análise de tráfego, são enviados pacotes de resposta e de dados falsos; origem e destino inserem paddings nos onions.

3.1.8 CARP - Certificate-free Anonymous Routing [Banerjee et al. 2006]

Possui quarto fases: descoberta e resposta de rota, transferência e manutenção. A origem difunde um pacote de requisição com um trapdoor (sua identidade e a do destino, um nonce e um vetor de inicialização, cifrados com uma chave gerada através de criptografia baseada em identidades) e um campo ao qual os intermediários acrescentam pseudônimos temporários. Com o vetor de inicialização e o nonce como chave, o destino cifra a prova de que abriu o trapdoor (a sua identidade e a da origem, e um nonce) e envia um pacote de resposta, que contém também a lista de pseudônimos. Os pacotes de dados também possuem essa lista e os dados são cifrados com uma chave, gerada através do hash dos nonces e das identidades dos nós origem e destino. Para todos os pacotes encaminhados, espera-se confirmação; caso não seja recebida, um pacote de erro é enviado.

3.1.9 ODAR - On-Demand Anonymous Routing [Sy et al. 2006]

Possui quatro fases: requisição do valor público do destino (Diffie-Hellmann), requisição e resposta de rota, e transferência. Antes de estabelecer uma comunicação, a origem solicita o valor público do destino para o servidor de chaves e calcula uma chave secreta; periodicamente, este envia um pacote que contém a rota dele para todo nó. Depois, difunde um pacote de requisição com um trapdoor (HMAC - Hashed Message Authentication Code da identidade do destino com a chave estabelecida por Diffie-Hellmann), seu valor público temporário e um Bloom Filter (vetor de bits, constituído por m posições, das quais k são modificadas para 1 de acordo com o resultado de k funções hash aplicadas ao elemento a ser inserido no filtro). Intermediários inserem o HMAC de suas identidades no Bloom Filter. O destino, com o valor público da origem e seu valor privado, calcula a chave gerada pela origem, abre o trapdoor e envia a resposta com o Bloom Filter. Através deste filtro, os nós verificam se pertencem à rota e encaminham os dados. Cita a possibilidade de utilização de técnicas mixing para proteger os pacotes de dados.edes ad hoc podem ser classificadas utilizando-se vários parâmetros.

3.2 Aspectos de Segurança e Anonimato

Ainda que o foco do estudo não se refira diretamente aos aspectos de segurança em si e no anonimato nas camadas de enlace, transporte e aplicação, é importante apresentar de forma rápida alguns conceitos.

Segundo TAMASHIRO (2007), *"segurança em redes sem fio ad hoc móveis consiste em: disponibilidade, autenticidade, confidencialidade, integridade, não-repúdio, privacidade, anonimato, robustez, entre outros requisitos*". Assim, tais redes são mais vulneráveis a ataques, devido a sua topologia dinâmica, vulnerabilidade dos nós e dos enlaces, ausência de gerenciamento e monitoramento centralizado e limitação de recursos.

Por anonimato, segundo a especificação ISO/IEC 15408 (TAMASHIRO, 2007), são apontados quatro requisitos relacionados com a privacidade: *Anonimato*, que assegura a não revelação da identidade do usuário; *Pseudo-anonimato*, que assegura Anonimato, porém associa a identidade ao serviço; *Não-correlação*, que assegura a não correlação de um ou mais serviços ao usuário; e *Não-observação*, que assegura o uso de um serviço sem que outros usuários percebam que o serviço está sendo usado.

Outras definições foram aperfeiçoadas no sentido de detalhar e preencher uma eventual falta de entendimento. PFITZMANN & HANSEN (2008) vem trabalhando desde o ano de 2000 com propostas de adotar conceitos relativos ao anonimato e privacidade. É

indicado ainda que a adoção de uma terminologia padrão pode contribuir para o avanço das pesquisas, evitando que cada novo pesquisador invente sua própria definição. Nesse sentido, esse estudo propõe conceitos mais amplos para definir privacidade, sendo que o anonimato não está ligado somente ao usuário, mas a qualquer *entidade* – definida como alguém ou algo que executa uma ação. Na definição de não-correlação o atacante não consegue saber se um *item de interessente* (sob a perspectiva do atacante, sendo mais abrangente que usuário e serviço) está relacionado ou não. Um item de interesse, dessa forma, pode ser qualquer componente de interesse no ataque (pessoas, processos, mensagens, etc.). O anonimato pode ainda ser qualificado e relacionado com a não-correlação, apresentando assim: *Anonimato de origem*, quando a mensagem não pode ser associada com a origem, e vice-versa; e *Anonimato de destino*, quando a mensagem não pode ser associada com o destino, e vice-versa.

3.3 Comparativo dos Protocolos

Esta seção analisa os protocolos informalmente, em relação às propriedades de anonimato. Considera-se que o anonimato é parcial quando as propriedades não são verdadeiras, sob determinadas condições ou quando se consideram pacotes que não pertencem aos processos de roteamento e de encaminhamento.

Tabela 2: Anonimato de Identidade

	Nó origem	Nó destino	Nós intermediários
ANODR	√	X	√
SDAR	P	√	X
ASR	√	√	√
ANDSR	P	X	X
MASK	√	X	√
ASRP	√	√	√
AnonDSR	P	P	P
CARP	√	√	√
ODAR	√	√	P

Nota: √ - provê, X - não provê, P - provê parcialmente

Em SDAR, a requisição possui as identidades da origem e do destino, mas cifradas com uma chave conhecida somente por eles e a chave pública do segundo, respectivamente.

Porém, atacantes globais presentes em toda a rede podem descobrir a requisição original, través do ataque de conteúdo, e identificar a origem, porque não há anonimato da identidade do emissor. As identidades dos nós emissor e destinatário estão em todos os pacotes; o destino abe as identidades dos intermediários, porque eles as inserem na requisição.

Tabela 3: Anonimato de Venue

	Nó origem	Nó destino
ANODR	X	√
SDAR	P	P
ASR	X	P
ANDSR	X	X
MASK	P	√
ASRP	P	P
AnonDSR	P	√
CARP	X	X
ODAR	X	X

Nota: √ - provê, X - não provê, P - provê parcialmente

Em SDAR e ASRP, atacantes globais ou presentes em toda a rede podem descobrir os venues da origem e do destino. O pacote de requisição original pode ser descoberto, através do ataque de conteúdo. Além disso, em situações de pouco tráfego, os pacotes de dados podem ser localizados, porque são vulneráveis aos ataques de análise de tempo e de volume, e se há somente uma requisição, é possível seguir o pacote de resposta do destino até a origem.

Tabela 4: Privacidade de Localização e de Padrão de Movimento

	Localização	Padrão de movimento
ANODR	forte	forte
SDAR	não há	não há
ASR	forte	forte
ANDSR	não há	não há
MASK	fraca	forte
ASRP	fraca	fraca
AnonDSR	parcialmente fraca	parcialmente fraca
CARP	forte	fraca
ODAR	parcialmente fraca	parcialmente fraca

Em SDAR e ANDSR, é possível relacionar a identidade de um nó (misturador, no caso de ANDSR) a todos os pacotes que encaminha ou recebe, porque não há anonimato do emissor e do destinatário. Além disso, em SDAR, todo nó conhece seus vizinhos, e em ANDSR, nós comuns revelam suas identidades ao requisitarem misturadores. Os pacotes pertencentes a uma rota, encaminhados por um nó (SDAR) ou por todos os nós (ANDSR), podem ser correlacionados através do ataque de reconhecimento de fluxo.

Tabela 5: Anonimato de Rota

	Em relação a nós que não pertencem à rota	Em relação a nós que pertencem à rota
ANODR	√	P
SDAR	X	X
ASR	P	P
ANDSR	X	X
MASK	P	P
ASRP	P	P
AnonDSR	P	P
CARP	X	X
ODAR	X	X

Nota: √ - provê, X - não provê, P - provê parcialmente

Em SDAR, qualquer nó pode correlacionar os nós pertencentes a cada rota, porque não há anonimato das identidades dos nós emissor e destinatário, e os pacotes são vulneráveis aos ataques de análise de tempo e de volume. Os pacotes de resposta e de dados podem ser seguidos em certas circunstâncias. Além disso, o destino sabe a identidade de todos os intermediários. Pelo tamanho dos pacotes de requisição e de resposta, nós na rota sabem a distância relativa entre eles.

4. SIMULAÇÃO DOS ATAQUES

Nesse capítulo será apresentada a ferramenta utilizada durante a simulação, o detalhamento do protocolo selecionado, a metodologia utilizada e os resultados da simulação

4.1 Escolha do simulador de redes

Para realizar a simulação do protocolo optou-se pelo simulador de rede *QualNet 4.5.1*, desenvolvido pela empresa *Scalable Networks* (SNT, 2009). Antes, entretanto, outros simuladores foram analisados em termos de facilidade de uso e incorporação do código do protocolo. Entre as opções disponíveis, o simulador OPNET e o Network-Simulator (ns-2) foram amplamente estudados.

A ferramenta OPNET é uma solução completa para simulação de redes, sendo possível, através dos editores, criar rapidamente novos pacotes, nós, camadas de rede, processos, etc. Entretanto, o software mostrou-se um pouco complexo na hora de implementar a especificação informal dos protocolos, devido a ausência de suporte e documentação fornecida pelo fabricante. Com uma licensa comercial e com o suporte adequado, possivelmente essa ferramenta possui o conjunto mais completo de opções para simulação.

O simulador de redes *Network Simulator* (ns-2) é um simnulador de eventos discretos para pesquisa na área de redes. Suporta desde componentes básicos, como TCP e UDP, até mecanismos mais complexos em redes wireless e via satélite. Ainda assim, por ser gratuito e código-fonte aberto, possui uma boa documentação e contribuição de códigos. É escrito em conjunto da linguagem C++ com uma versão orientada a objetos de TCL (WIKIPEDIA TCL, 2009): OTCL (OTCL, 2009). Apesar dos recursos visuais serem infinitamente inferiores ao OPNET, o simulador *ns-2* é capaz de representar desde redes locais simples até redes mais complexas. Além disso, uma grande vantagem desse simulador é sua integração nativa com biobliotecas C++. Seria, portanto, uma ótima escolha para simular o protocolo e verificar suas propriedades.

O simulador *QualNet* apresentou uma boa documentação, uma licensa educacional e, principalmente, uma implementação do protocolo anônimo ANODR. Assim, optou-se por adaptar essa implementação para verificar as propriedades deste protocolo. Na próxima seção são apresentados alguns conceitos técnicos relativos ao simulador escolhido para o trabalho.

4.1.1 Simulador QualNet 4.5.1

O simulador *QualNet* foi utilizado na versão 4.5.1, disponibilizado para testes com uma licensa educacional. Em termos gerais, é um simulador simples de usar que procura avaliar o desempenho de redes wireless, cabeadas e mistas. Ele é dividido em módulos, cada um responsável por agrupar diferentes características de redes. Alguns deles são: Wireless, Multimídia, Celular e Satélite, Segurança e Rede de Sensores. Além das bibliotecas, o simulador é divido em componentes de simulação.

O Editor de Cenários permite que o usuário configure distribuições geográficas, modelos de mobilidade, conexões físicas e os parâmetros de funcionamento dos nós e da rede. Todos os parâmetros são facilmente configurados em uma estrutura hierárquica.

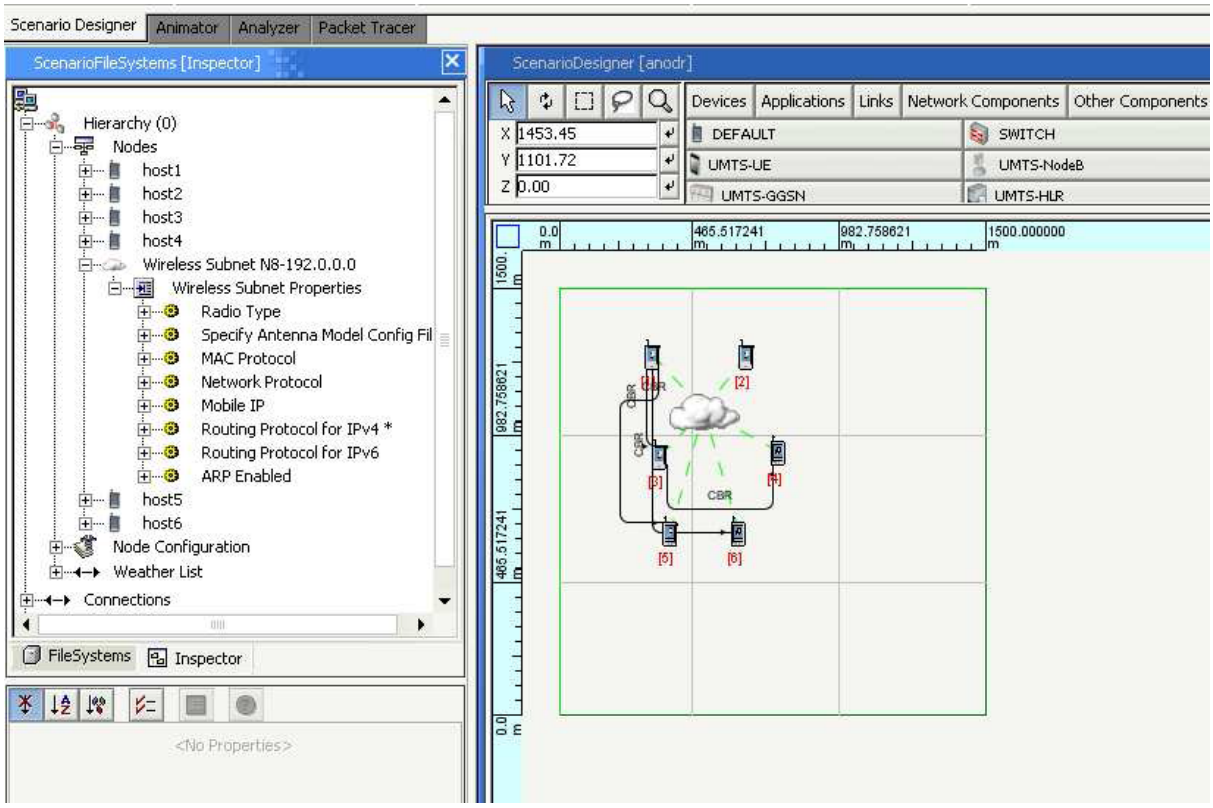

Figura 2: QualNet - Editor de Cenários do Simulador

4.2 Escolha do Protocolo

O protocolo escolhido para avaliação e simulação é o ANODR – *Anonymous On Demand Routing*. A escolha do protocolo foi fundamentada na disponiblidade dentro do

simulador e nas características apresentadas, onde se observou que alguns outros protocolos posteriores a esse são apenas modificações para proteger outros ataques, ou para melhorar o desempenho quando se trata de equipamentos móveis de pouco poder computacional. Será apresentada uma visão geral do protocolo e os detalhes específicos de funcionamento.

4.2.1 Visão Geral do Protocolo

O protocolo ANODR, proposto por KONG & HONG (2003), foi o primeiro protocolo para roteamento anônimo em redes ad-hoc móveis. Em termos gerais, procura prover anonimato de rota e privacidade de localização, garantindo que os adversários não possam descobrir a identidade real das partes envolvidas em uma transmissão de rede. O planejamento do protocolo é baseado em *broadcast* com informações de *trapdoor*.

O propósito do protocolo é desenvolver um esquema de rotas que não possam ser traçadas, dentro de um ambiente de roteamento sob demanda. Esse objetivo é, substancialmente, diferente de outras propostas de roteamento seguro, onde procura-se prevenir outros tipos de ataque, como o de negação de serviço. Dentro do ambiente que o protocolo é projetado, os atacantes tentam agir passivamente em silêncio, procurando ficar o mais invisível possível.

Dessa forma, a contribuição do trabalho é tentar apresentar um protocolo de roteamento que previne um atacante associar os participantes da rede com suas identidades, e impedir que o fluxo de um pacote possa ser seguido no destino ou origem. E embora os adversários possam detectar a existência de transmissões de rede sem fio, fica difícil saber o número de participantes e os padrões de transmissão. O anonimato não é referenciado, pois, em termos de não-observância.

O protocolo é constituído por três fases: descoberta de rota, encaminhamento de dados e manutenção de rota.

4.2.2 Funcionamento do Protocolo

Algumas propostas são utilizadas como base para a definição posterior dos componentes de funcionamento:

- ✓ **Broadcasting com trapdoor**: Ao enviar o broadcast para a rede, a informação de trapdoor conhecida apenas pelo destino é associada à mensagem.
- ✓ **Privacidade de localização e não rastreabilidade**: Normalmente o roteamento de

mensagens em uma rede ad-hoc móvel ocorre através de múltiplos saltos, passando por vários nós intermediários até atingir o destino. Objetiva-se, assim, garantir privacidade de localização para cada nó responsável por encaminhar mensagens, e ainda entre os nós origem/destino.

O protocolo divide o processo de roteamento em duas partes principais: Descoberta de rota, manutenção de rota e encaminhamento de dados.

4.2.2.1 Descoberta de Rota

A descoberta anônima de rota é um processo que ocorre no momento que um determinado nó na rede deseja enviar dados para outro nó. As rotas não são conhecidas previamente, por esse motivo o roteamento é chamado sob demanda. Durante a fase inicial da requisição o seguinte pacote é criado no nó de origem:

{ RREQ, *seqnum, trdest, onion* }

O primeiro campo indica o tipo de pacote que será criado. O campo *seqnum* é um identificador global único do pacote. O terceiro campo é a chave criptográfica de *trapdoor*, que pode ser aberta somente pelo destinatário. O campo *onion* representa as camadas criptográficas (*onion routing*) utilizadas pelos nós intermediários, garantindo dessa forma a rota anônima de pseudônimos. Esse campo é essencial no funcionamento do protocolo, e sua arquitetura influencia decisivamente no desempenho e garantia de anonimato. Para tal, o autor propõe três abordagens, partindo de um esquema simples de misturadores (Mix-NET), e finalmente chegando ao modelo final mais eficiente.

O primeiro modelo utiliza uma simples adaptação do esquema da rede de misturadores e chaves assimétricas. É chamado, por isso, de ANODR-PO (*Public key Onion*).

Durante a fase de requisição (RREQ), cada nó na rota adiciona uma camada referente ao nó anterior e envia por *broadcast* a mensagem. O resultado da mensagem encaminhada é sempre encriptado com a chave pública do nó. Ao chegar no destino (sabe-se pela informação de *trapdoor* do pacote de requisição) a estrutura *onion* representa uma rota anônima de volta ao nó de origem. A mensagem de resposta possui o seguinte formato:

{ RREP, *N, prdest, onion* }

O primeiro campo identifica um pacote de resposta de rota. O campo *N* é um número randômico único que representa o pseudônimo da rota. O terceiro campo é uma prova de abertura do *trapdoor* pelo destino. O *onion* desse pacote é uma cópia exata do onion que chega ao nó de destino.

Durante a resposta de rota o nó tenta decriptar o *onion* utilizando sua chave privada. Quando não encontra sua identificação na mensagem decriptada (primeiro campo), o nó não faz parte da rota e a mensagem é descartada. Ao perceber que a rota deve passar pelo nó, é gerado um *nonce* Ni que substitui o nonce *N* da mensagem. Uma correspondência interna da relação N pra Ni é mantida na tabela interna de encaminhamento.

Em seguida, a camada externa do *onion* é retirada e a mensagem é encaminhada. O esquema de chaves assimétricas do modelo ANODR-PO prejudica o desempenho da rede em termos de latência e *overhead*. Imaginando que as mensagens de RREQ e RREP são enviadas via *broadcast*, toda a rede ficará comprometida em executar operações computacionais custosas para montar e verificar os *onions* das rotas. Assim, é proposto um esquema com chaves simétricas, chamado de ANODR-BO (*Boomerang Onion*) – em referência ao uso da mesma chave simétrica usada na requisição e depois na resposta.

É possível verificar o esquema de roteamento usando a idéia das chaves simétricas. Quando o nó B intermediário recebe uma requisição para encaminhamento, ele adiciona uma camada ao *Boomerang Onion* e encripta o resultado com uma chave simétrica 26 randômica KB. Quando a resposta retorna ao nó, a mesma chave é utilizada para remover uma camada do esquema. Assim é garantido que a latência não será grande, pelo menos se depender das operações criptográficas executadas durante a requisição e resposta. O uso de chaves simétricas tem sem mostrado muito eficiente em equipamentos móveis de reduzido poder computacional.

Uma modificação é proposta ao esquema do ANODR-BO para chegar ao modelo final. Como a identidade dos nós intermediários pode ser encontrada nas mensagens, o anonimato não é alcançado entre os vizinhos da rota. É adicionado, então, um *trapdoor* nas camadas. Quando um nó intermediário B recebe a mensagem de requisição de rota, ele gera um *nonce* NB e adiciona na camada. Da mesma forma do esquema anterior, a mensagem é encriptada usando uma chave simétrica antes de ser enviada via *broadcast* pela rede. A informação de *trapdoor* é a chave simétrica do nó e o *nonce* gerado pelo nó. Durante a resposta de rota o nó será capaz de decriptar a mensagem e confirmar o *nonce* com seu registro interno.

4.2.2.2 Manutenção de Rota

A manutenção de rota no protocolo ANODR segue um esquema de atualização das tabelas de roteamento. Após certo número de tentativas de retransmissões de dados, o nó

verifica o pseudônimo N' que está associado com o pseudônimo N do provável nó defeituoso (desligado ou com defeito). Assim, uma mensagem de erro é enviada no seguinte formato: {REER, N'}. Os nós que recebem via broadcast essa mensagem e verificam que estão usando essa rota, realizam o mesmo procedimento em cascata para notificar os vizinhos.

4.2.2.3 Encaminhamento de Dados

Após receber a resposta de rota, o nó de origem encripta os dados utilizando o pseudônimo de rota da sua tabela de encaminhamento. O pacote é então enviado via *broadcast* para a rede e, para cada nó intermediário, verifica-se a tabela de encaminhamento para encontrar uma correspondência com o pseudônimo. Caso pertença à rota, o nó altera o pacote e inclui o seu pseudônimo. Esse procedimento é repetido até o nó chegar ao destino.

4.2.3 Considerações Sobre a Implementação

Algumas questões são levantadas pelo autor em relação a analise de pacotes feita por um atacante (*eavesdropper,* por exemplo), que pode associar requisições com respostas de rota. Em termos computacionais, dificilmente alguém que não possui a chave de abertura do *onion* consegue relacionar a estrutura de um *onion* (os pseudônimos das rotas, por exemplo) encriptado com o correspondente sem encriptação. Entretanto, algumas associações são possíveis em outros campos: (1) pacotes de resposta de rota (RREP) com a mesmo prova de abertura do *trapdoor* (*prdest*) podem facilmente serem associados com a mesma rota. (2) Pacotes de requisição de rota (RREQ) com o mesmo sequencial (*seqnum*) e *trapdoor* podem pertencer à mesma rota. Ainda assim, caso a rede esteja comprometida, a estrutura do onion entre RREP e RREQ pode ser igualada, permitindo associar os dois pacotes à mesma rota. Para contornar alguns desses problemas, é proposto o uso de chaves assimétricas temporárias durante a fase de requisição nos nós intermediários. Assim, o nó intermediário gera um par de chaves pública/privada para toda requisição de rota encaminhada pelo nó:

{ RREQ, *seqnum, pkone, trdest, TBO* }

Quando o nó de destino inicializa a resposta de rota, uma chave simétrica *Kseed* é gerada para proteger a prova de abertura do *trapdoor* e o *onion* TBO. Incluíndo a metodologia de *trapdoor* mencionada anteriormente, os pacotes de requisição e resposta de rota (já protegendo a chave simétrica K*seed* com a chave pública) são:

{ RREQ, *seqnum, pkone,* KT(*dest*, KC), KC(*dest*), *TBO* }

{ RREP, {K*seed*}*pkone,* Kseed{K'C, TBO} }

Posteriormente nos nós intermediários, durante a resposta, a prova de abertura do *trapdoor* pelo destino é realizada verificando-se a igualdade: KC(*dest*) = K'C(*dest*). Durante os pacotes de RREP e RREQ, e no encaminhamento de dados, são utilizados ACK's (*acknowledgments*) anônimos para confirmar certas operações (como abertura do *trapdoor*) e cancelar assim o *re-broadcast* de pacotes. O anonimato é alcançado utilizando como referência o pseudônimo do nó que se deseja informar o ACK.

4.3 Simulação dos Ataques

A plataforma utilizada para rodar o simulador foi um notebook equipado com processodor *AMD Core 2 Duo* de 32 bits e sistema operacional *Microsoft Windows XP Sp2*. É possível compilar o simulador em outras plataformas, sendo necessário baixar os códigos fontes específicos.

Para simular o protocolo uma rede ad-hoc móvel foi criada dentro de um campo de 1000 metros x 1000 metros, onde 7 nós foram dispostos uniformemente. Todos os nós são considerados simétricos, ou seja, se um determinado nó A consegue se comunicar diretamente com B, então B consegue se comunicar diretamente com A. O resumo das configurações do cenário pode ser visto na tabela 4.

Tabela 6: Detalhes de configuração do cenário de simulação

Parâmetro	Valor
Tempo de simulação	1 minuto
Dimensões do cenário	1000 metros X 1000 metros
Número de nós	7
Alcance dos nós	250 metros
Velocidade do canal	2 Mbits/seg

A estratégia para geração do tráfego de dados da simulação foi montada de acordo com as verificações desejadas. Para simular os dados foi utilizado o gerador padrão de bytes (CBR – *Constant Bit Rate*). As ligações entre os nós foram ajustadas dinamicamente de

acordo com a necessidade de validação de determinado parâmetro.

Os resultados de cada simulação são analisados de acordo com os tipo de ataque. Os ataques podem ser classificados em ativos ou passivos, externos ou internos. Em um ataque ativo, o adversário interfere na rede e tenta mudar o comportamento normal dos protocolos. Em um ataque passivo, o adversário somente observa a rede, a fim de obter informações importantes. Exemplos: monitoramento das mensagens e análise de
tráfego.

Segundo Tamashiro (2007), através dos ataques de análise de tráfego um atacante pode inferir informações úteis sobre os nós da rede, localização, topologia, freqüência de comunicação e padrões de movimento. Foram simulados os seguintes ataques:

4.3.1.1 Ataque de análise de tempo

Se os pacotes são processados e encaminhados na mesma ordem em que são recebidos, um atacante pode inferir quais pertencem à mesma rota. Para simular o ataque de análise de tempo, foi realizada uma simulação. Assim, foi observado que o protocolo adiciona um atraso (*delay*) aleatório antes de fazer o *broadcast* na rede. O atraso no envio dos pacotes pode ser visualizado:

```
for (i = 0; i < node->numberInterfaces; i++)
{
    IpInterfaceInfoType* intfInfo = ip->interfaceInfo[i];
    if (intfInfo->routingProtocolType == ROUTING_PROTOCOL_ANODR)
    {
        clocktype delay = (clocktype) RANDOM_erand(node->globalSeed) * ANODR_BRO
```

Figura 3: Atraso adicionado no envio de pacotes

Tabela 7: Atraso verificado entre o envio e recebimento de mensagens

```
SIMULAÇÃO 01: (seed = 3535)
======= PACOTE RREQ [Simulação: 1.000000000 segundos] [Nó 1] [Send/Receive S]
======= PACOTE RREQ [Simulação: 1.001755132 segundos] [Nó 2] [Send/Receive R]
delay: 1.75 ms
======= PACOTE RREQ [Simulação: 1.001795132 segundos] [Nó 2] [Send/Receive S]
======= PACOTE RREQ [Simulação: 1.012804374 segundos] [Nó 3] [Send/Receive R]
delay: 11.01 ms
======= PACOTE RREQ [Simulação: 1.012844374 segundos] [Nó 3] [Send/Receive S]
======= PACOTE RREQ [Simulação: 1.021248526 segundos] [Nó 4] [Send/Receive R]
delay: 8.04 ms
======= PACOTE RREQ [Simulação: 1.021288526 segundos] [Nó 4] [Send/Receive S]
======= PACOTE RREQ [Simulação: 1.030986021 segundos] [Nó 5] [Send/Receive R]
   delay: 9.69 ms
```

Foram executadas duas simulações com *seeds* globais distintos. Ao remover o código que adiciona o *delay*, o atraso entre envio e recebimento permaneceu constante em 1.33 ms. Com os resultados da simulação foi comprovado o anonimato de identidade e o anonimato em relação aos nós fora da rota, pois o ataque análise de tempo não pode ser executado.

4.3.1.2 Ataque de conteúdo do pacote

Quando parte ou todo seu conteúdo (campos do cabeçalho ou carga útil) permanece inalterado durante sua transmissão, um atacante pode identificar e seguir um pacote. O mecanismo de criptografia salto a salto o protege contra este ataque. Para simular este ataque, uma simulação de transmissão de dados foi configurada entre o nó [1] e o nó [4]. Pela disposição geográfica dos mesmos, os pacotes de requisição e respostas precisam passar pelos nós intermediários [2] e [3] para alcançarem o destino.

Um nó intermediário ao receber uma requisição de rota não tem como verificar a origem do pacote. A captura dos pacotes RREQ e RREP no nó intermediário pode ser observada na tabela 5.

Tabela 8: Captura dos pacotes RREQ e RREP

```
======= PACOTE RREQ [Simulação: 1.000000000 segundos] [Nó 1] [Send/Receive S]

 PkOne:
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000

 Kt(dest,Kc):
040000C06172652074686520646573741462FC6C8D2F9520EE8A02232A9673290E2CA11FC59A8C62B07
B9156DAC6846800000000000000028000000B61C0000000020180471200549DD2D434FF120020E990
7CE001917CFFFFFFFFDB01917C26D175000000020100000001C00000048500E0100000000

 Kc(dest): 596F752061726520746865206465737374

 TBO: 5562C6711AB9EC164DA52964779A574E

 ======= PACOTE RREQ =======



 ======= PACOTE RREQ [Simulação: 4.451334460 segundos] [Nó 2] [Send/Receive R]

 PkOne:
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000

 Kt(dest,Kc):
```

```
040000C06172652074686520646573741462FC6C8D2F9520EE8A02232A9673290E2CA11FC59A8C62B07
B9156DAC6846800000000000000000028000000B61C0000000002018047120054 9DD2D434FF120020E990
7CE001917CFFFFFFFFDB01917C26D175000000020100000000 1C00000048500E0100000000

 Kc(dest): 596F752061726520746865206465737 4

 TBO: 5562C6711AB9EC164DA52964779A574E

 ======= PACOTE RREQ =======


 [RREQ - Processamento interno] [Nó 2] [Time 4.451374460 seg.]

 ONION de entrada: 5562C6711AB9EC164DA52964779A574E

 Chave do ONION: AE2F145EA4300C66902C9B7E8E74E514

 ONION de saída: FB4DD22FBE89E070DD89B21AF9EEB25A


 ======= PACOTE RREQ [Simulação: 4.451374460 segundos] [Nó 2] [Send/Receive S]

 PkOne:
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000

 Kt(dest,Kc):
040000C06172652074686520646573741462FC6C8D2F9520EE8A02232A9673290E2CA11FC59A8C62B07
B9156DAC6846800000000000000000028000000B61C0000000002018047120054 9DD2D434FF120020E990
7CE001917CFFFFFFFFDB01917C26D175000000020100000000 1C00000048500E0100000000

 Kc(dest): 596F752061726520746865206465737 4

 TBO: FB4DD22FBE89E070DD89B21AF9EEB25A

 ======= PACOTE RREQ =======


 ======= PACOTE RREP [Simulação: 11.354123638 segundos] [Nó 4] [Send/Receive S]

 {Kseed}PKone:
040000C06172652074686520646573741462FC6C8D2F9520EE8A02232A9673290E2CA11FC59A8C62B07
B9156DAC6846800000000000000000028000000B61C0000000002018047120054 9DD2D434FF120020E990
7CE001917C

 Kseed{PRdest, TBO}:
1462FC6C8D2F9520EE8A02232A9673294C0C88151597BD3FC6EF6074EF3CE805

 ======= PACOTE RREP [FIM]    =======


 [RREP - Processamento interno] [Nó 3] [Time 11.395042235 seg.]

 Kseed: 00000000AD91BE31173D7728E3F9B620

 ONION: 4C0C88151597BD3FC6EF6074EF3CE805
```

```
K'c: 1462FC6C8D2F9520EE8A02232A967329
```

Na primeira captura, o *onion* TBO está cifrado com a chave simétrica do nó [1] e não possui nenhuma informação do nó de destino. Como o *onion* do pacote RREP é o mesmo da requisição, o anonimato é garantido da mesma forma durante a resposta. Analisando informações do processamento interno (considerado assim um nó malicioso), nenhuma informação permite associar o pacote à sua origem.

4.3.1.3 Ataque de volume do pacote

Quando pacotes possuem o mesmo tamanho ou se o tamanho muda de forma padronizada, o atacante pode seguir o pacote. A fim de prevenir esse ataque, cada salto preenche o onion da requisição e da resposta, até completar 400 bits. Assim, possuem tamanho único e fixo, apesar de o tamanho real do onion mudar, de modo padrão, a cada salto. Na requisição, cada nó acrescenta uma informação com tamanho fixo (um nonce - Ni) ao onion recebido e o resultado é cifrado com uma chave simétrica (Ki). No caso do nó origem, o onion é a sua identidade, cifrada com uma chave simétrica. Na resposta, decifra-se o onion e remove-se o nonce.

Para simular um ataque de volume, o nó de origem [1] deseja se comunicar com o nó de destino [4]. Os nós [2] e [3] são os nós intermediários. Ao analisar o tamanho do onion na estrutura interna do protocolo, observou-se o seguinte:

Tabela 9: Tamanho da camada *onion* durante o processamento

```
[RREQ - Processamento interno] [Nó 3] [Time 7.902749041 seg.]
 ONION de entrada: FB4DD22FBE89E070DD89B21AF9EEB25A
 Chave do ONION: B7415A3AAB1E5D4F1B66D26E16D25A5F
 ONION de saída: 4C0C88151597BD3FC6EF6074EF3CE805

[RREQ - Processamento interno] [Nó 2] [Time 4.451374460 seg.]
 ONION de entrada: 5562C6711AB9EC164DA52964779A574E
 Chave do ONION: AE2F145EA4300C66902C9B7E8E74E514
 ONION de saída: FB4DD22FBE89E070DD89B21AF9EEB25A
```

```
[RREP - Processamento interno] [Nó 3] [Time 11.479423399 seg.]
 Kseed: 00000000F420294BAD53AE7355527316
 ONION: 5562C6711AB9EC164DA52964779A574E
 K'c: 00000000000000000000000000000000

[RREP - Processamento interno] [Nó 2] [Time 11.437322817 seg.]
 Kseed: 00000000610CDD6E48223D355841AC63
 ONION: FB4DD22FBE89E070DD89B21AF9EEB25A
 K'c: 00000000000000000000000000000000
```

Com o resultado da simulação foi verificado que o tamanho da estrutura das camadas do *onion* não é alterado conforme os saltos aumentam, pois cada nó, para uma determinada rota, possui uma relação 1 para 1 com o nó vizinho. Um adversário que realiza um ataque de volume do pacote não consegue determinar, mesmo se tratando de um atacante interno, o *venue* de origem através de uma comparação de tamanho do primeiro *onion* recebido com os demais onions da rota. O anonimato de rota em relação aos nós fora da rota é garantido, pois o ataque de volume não pode ser executado.

4.3.1.4 Ataque de reconhecimento de fluxo

Diz respeito à capacidade que um atacante tem de identificar pacotes referentes à mesma rota. Se os pacotes possuem informações em comum, um atacante pode identificar quais pertencem à mesma rota.

O anonimato de rota é verificado através da análise de vulnerabilidade dos ataques de reconhecimento de fluxo. Pacotes pertencentes à mesma rota não podem ser correlacionados, porque não há informações em comum. Inclusive, os pseudônimos de cada enlace mudam dinamicamente a cada pacote encaminhado. Porém, um nó pertencente à rota pode correlacioná-los. Na fase de requisição, cada nó gera um par de chaves assimétricas temporárias, cuja chave pública (TPKi) é inserida no pacote RREQ. Essa chave é utilizada no pacote RREP para cifrar a semente criptográfica (ETPKi(Ki+1)), que gera a sequência de pseudônimos utilizados na fase de transferência de dados.

Pacotes de resposta de rota (RREP) com a mesmo prova de abertura do *trapdoor*

(pr_{dest}) podem facilmente serem associados com a mesma rota. Pacotes de requisição de rota (RREQ) com o mesmo seqüencial (*seqnum*) e *trapdoor* podem pertencer à mesma rota. Ainda assim, caso a rede esteja comprometida, a estrutura do onion entre RREP e RREQ pode ser igualada, permitindo associar os dois pacotes à mesma rota.

Para contornar alguns desses problemas, é proposto o uso de chaves assimétricas temporárias durante a fase de requisição nos nós intermediários. Assim, o nó intermediário gera um par de chaves pública/privada para toda requisição de rota encaminhada pelo nó.

Ao verificar a estrutura interna do código responsável por fazer a verificação da prova de abertura de *trapdoor*, nenhuma informação do destino fica disponível para leitura no nó intermediário. Os seguintes passos são executados para verificação da prova de abertura do *trapdoor*:

- ✓ A tag *dest* (que aqui não representa o ID do nó ou o endereço IP) é cifrada utilizando a chave simétrica K'_C;
- ✓ O resultado da operação anterior é verificado com a entrada K_C(*dest*) da tabela de rota do nó;
- ✓ Se não for igual o pacote é descartado, pois um possível ataque de injeção de RREP foi executado;

Na simulação do protocolo a tag *dest* é uma constante definida no cabeçalho da aplicação: #define ANODR_DEST_TAG ((byte *)"You are the dest"). O que realmente indica quem deve receber a mensagem é a chave previamente compartilhada entre a origem e o destino. No momento em que o destino recebe a mensagem, a chave compartilhada permite abrir o conteúdo da tag *dest* cifrada e verificar com a constante definida no protocolo. Portanto, o protocolo consegue manter o anonimato do destino nos nós intermediários.

4.4 Resultado dos Ataques

O protocolo ANODR é parcialmente seguro contra os ataques de análise de tempo, de conteúdo, de volume e de reconhecimento de fluxo, os mecanismos de segurança tornam o ataque mais difícil. A Tabela 6 compara o protocolo quanto à proteção dos ataques:

Tabela 10: Segurança contra Ataques de Análise de Tráfego

	Análise de tempo	Conteúdo do pacote	Volume do pacote	Reconhecimento de fluxo
ANODR	P	P	P	P

NOTA : X – vulnerável ao ataque, P – parcialmente seguro contra ataque

Considera-se que o protocolo é seguro contra o ataque, quando os pacotes não são vulneráveis sob o ponto de vista de qualquer nó; é vulnerável, quando todos os pacotes são propensos ao ataque sob o ponto de vista de qualquer nó; é parcialmente seguro, quando nem todos são vulneráveis ou se são sob o ponto de vista de apenas um tipo de nó ou sob determinadas condições.

• Ataque de análise de tempo: A fim de prevenir esse ataque, utiliza técnicas delay. Porém, somente os pacotes de resposta e de dados são protegidos.

• Ataque de conteúdo do pacote: Os dados não são vulneráveis, porque, a cada salto, a carga útil do segundo é cifrada salto a salto.

• Ataque de volume do pacote: A fim de prevenir esse ataque, cada salto preenche o onion da requisição e da resposta, até completar 400 bits. Assim, possuem tamanho único e fixo, apesar de o tamanho real do onion mudar, de modo padrão, a cada salto. Esse método protege somente contra ataques externos.

• Ataque de reconhecimento de fluxo: Pacotes pertencentes à mesma rota não podem ser correlacionados, porque não há informações em comum. Utiliza-se a técnica de envio de pacotes falsos.

5. CONCLUSÕES

O presente estudo procurou apresentar um panorama na área de redes sem fio ad-hoc móveis, e ainda verificar e simular os ataques de análise de tráfego realizados por TAMASHIRO (2007). Alguns conceitos foram apresentados no sentido de situar redes ad-hoc móveis em um contexto mais genérico. Foi detalhado o funcionamento e estrutura interna do protocolo ANODR, um protocolo do tipo *source-routing* sob demanda, que procura prover anonimato usando uma combinação de pseudônimos, chaves públicas e privadas, redes MIX-net e operações com chaves simétricas e assimétricas.

Em relação ao futuro dos protocolos que tentam prover anonimato nas redes sem fio ad-hoc móveis, é um pouco difícil prever o comportamento ideal de tais redes. A própria concepção dessas redes viabiliza um número grande de aplicações. O anonimato é apenas um dos itens de segurança. O conjunto de soluções de segurança para atender os requisitos vai depender do contexto da aplicação (energia, mobilidade, poder computacional, etc.). Assim, nenhuma solução poderá ser considerada ideal, já que a abrangência de aplicações é potencialmente infinita.

Em ambientes críticos, uma solução eficiente, que considere fatores internos (capacidade dos nós, consumo de energia, etc.) e externos (mobilidade, ataques passivos, etc.), se torna fundamental para operacionalização da rede e segurança das operações. Da mesma forma, o crescente uso de redes ad-hoc móveis em soluções comerciais e redes públicas também busca prover anonimato. Assim, uma solução ótima nunca será viável, principalmente devido à característica altamente heterogênia das aplicações. É necessário fazer um balanceamento de necessidades, procurando priorizar as características de cada rede e a viablidade comercial na adoção de um protocolo. Levando-se também em consideração o atual nível de pesquisa na área, dificilmente um protocolo será padronizado nos próximos anos e dificilmente, se assim for, apenas um será comercializado em equipamentos.

5.1 Trabalhos Futuros

Os vários protocolos disponíveis devem ser estudos no sentido de unificar os requisitos de anonimato, para então ser formalizado um protocolo de roteamento anônimo padrão e também analisar questões de segurança do protocolo contra ataques ativos, e análise de tráfego usando ataques ativos. Segue como sugestão a implementação do protocolo em

aplicações reais de redes sem fio ad-hoc móveis. Assim, será possível montar uma rede entre dispositivos e simular ataques utilizando adversários físicos.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ALECRIM, Paulo Dias de. **Simulação Computacional para Redes de Computadores**. Rio de Janeiro: Editora Ciência Moderna, 2009.

BANERJEE, Amal; JULIEN, Christine; SHMATIKOV, Vitality. **Certificate Free Anonymous Routing for Mobile Ad Hoc Networks**. 2006. The University of Texas at Austin.

BONEH, D.; FRANKLIN, M. **Identity Based Encryption From Weil Pairing**. 2003. SIAM Journal of Computing: 586-615.

CHLAMTAC, I.; CONTI, M.; LIU, J. J.-N. **Mobile Ad Hoc Networking: Imperatives and Challenges**. Ad Hoc Networks, v. 1, p. 13–64, July 2003.

CORSON, S.; MACKER, J. **Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations**. IETF, January 1999. RFC 2501 (Informational). (Request for Comments, 2501). Disponível em: <http://www.ietf.org/rfc/rfc2501.txt>. Acesso em: Nov. 2008

EL-KHATIB, K. et al. **Secure Dynamic Distributed Algorithm for Ad Hoc Wireless Networks**. In: International Conference on Parallel Processing Workshops. [S.l.: s.n.], 2003. p. 359–366.

GERLA, Mario; SANADIDI, M.Y.; HONG, Xiaoyan; KONG, Jiejun. **Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing**. 2006. University of Alabama, University of California.

GOLDSCHLAG, D.; REED, M., SYVERSON, P. **Onion Routing for anonymous and private internet connections**. Communications of the ACM, 42(2):39C4, 1999.

JIMENEZ T.; ALTMAN E. **NS Simulator for Beginners**. Univ. de Los Andes, Venezuela e Sophie-Antopolis, França. 2003-2004. Disponível em: < http://www-sop.inria.fr/maestro/personnel/Eitan.Altman/COURS-NS/n3.pdf>. Acesso em:

mar. 2008.

KONG, J.; HONG, X. ANODR: **ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks**. In: 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing. [S.l.: s.n.], 2003. p.291–302.

KUOSMANEM, Petteri. **Classification of Ad Hoc Routing Protocols**. 2007. Artigo publicado. Naval Academy – Helsinki – Finland.

MANET WG. **Mobile Ad-hoc Networks (manet) Charter**. Disponível em: <http://www.ietf.org/html.charters/manet-charter.html>. Acesso em: out. 2008.

MURTHY, C. S. R.; MANOJ, B. S. Ad **Hoc Wireless Networks. Architectures and Protocols**. [S.l.]: Prentice Hall Professional Technical Reference, 2004.

OTCL. **Object TCL Extension.** Disponível em: < http://bmrc.berkeley.edu/research/cmt/cmtdoc/otcl/> . Acesso em: Mar. 2009

PFITZMANN, A.; HANSEN, M. **Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology**. Feb 2008. Version 0.31. Disponível em: <http://dud.inf.tu-dresden.de/Anon Terminology.shtml>

QUALNET. **Qualnet 4.5.1 Installation Guide**. Jul 2008. Disponível em: < http://www.scalable-networks.com/publications/documentation/>. Acesso em: Mar. 2009.

SY, D.; CHEN, R.; BAO, L. ODAR: **On-Demand Anonymous Routing in Ad Hoc Networks**. In: Third IEEE International Conference on Mobile Ad-hoc and Sensor Systems. [S.l.: s.n.], 2006. p. 267–276

SNT. **Scalable Networks.** 2009. Disponível em: < http://www.scalable-networks.com/>. Acesso em: Mar. 2009

TAMASHIRO, Clytia Higa. **Uma Análise de Protocolos de Roteamento Anônimo para Redes Sem Fio Ad Hoc Móveis**. 2007. Tese. (Mestrado Ciências da Computação) UFSC,

Florianópolis.

TOR PROJECT, **The Tor Project**. 2006. Disponível em < https://www.torproject.org/ >. Acesso em: Mar. 2009

WIKIPEDIA – TCL. **Tool Comand Language.** Disponível em: <http://en.wikipedia.org/wiki/TCL> . Acesso em: Mar. 2009

WIKIPEDIA – MESH NETWORKS. **Mesh Networks.** Disponível em: <http://en.wikipedia.org/wiki/Mesh_network> . Acesso em: Nov. 2008

ZHANG, Y.; LIU, W.; LOU, W. **Anonymous Communications in Mobile Ad Hoc Networks.** In: Annual Joint Conference of the IEEE Computer and Communications Societies. [S.l.: s.n.], 2005. v. 3, p. 1940–1951.