UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO TECNOLÓGICO

DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Günter Heinrich Herweg Filho

Simulação de ataques ao protocolo de roteamento AODV

Orientadora

Kathia Regina Lemos Jucá

Florianópolis,

Dezembro, 2005.

Simulação de ataques ao protocolo de roteamento AODV

Projeto de Pesquisa para elaboração do Trabalho de Conclusão de Curso apresentado como exigência para a obtenção do título de Bacharel em Ciências da Computação à Universidade Federal de Santa Catarina - UFSC, no curso de Ciências da Computação.

Banca Examinadora

_____

Kathia Regina Lemos Jucá (Orientadora)
Universidade Federal de Santa Catarina

_____

Prof. Dr. João Bosco Mangueira Sobral (Co-Orientador)
Universidade Federal de Santa Catarina

_____

Dra. Mirela Sechi Moretti Annoni Notari (Membro)
Fundação Bardall de Educação e Cultura

Florianópolis,
Dezembro, 2005

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Gráficos

Acrônimos

AODV	Ad hoc on Demand Distance Vector
ARAN	Authenticated Routing for Ad hoc Network
CMU	Carnegie Mellon University
DSDV	Destination-Sequenced Distance Vector
DSR	Dynamic Source Routing
IP	Internet Protocol
NAM	Network Animator
NS	Network Simulator
OSI	Open Systems Interconnection
OTCL	Object Tool Command Language
PDA	Personal Digital Assistants
RERR	Route Error Message
RREP	Route Reply Message
RREQ	Route Request Message
SAODV	Secure AODV
SDI	Sistema de detecção de intrusão
TCL	Tool Command Language
WLAN	Wireless Local Area Networks
WPAN	Wireless Personal Area Networks
WRP	Wireless Routing Protocol

1. Introdução

Observando o grande crescimento nas áreas de comunicação celular, redes locais sem - fio e serviços via satélite juntamente com o comércio de dispositivos que utilizam tais serviços, estima-se que em poucos anos, dezenas de milhões de pessoas terão um *laptop*, *palmtop* ou algum tipo de PDA (*Personal Digital Assistants*). Este crescimento permitirá, em um futuro bem próximo, que informações e recursos possam ser acessados a qualquer instante e em qualquer lugar. Independente do tipo de dispositivo portátil, a maior parte desses equipamentos deverá ter capacidade de se comunicar com a parte fixa da rede e, possivelmente, com outros computadores móveis. A esse ambiente de computação dá-se o nome de computação móvel

Este tipo de ambiente onde os usuários podem realizar comunicações sem-fio para acessar recursos distribuídos faz parte da linha de pesquisa de Redes Móveis sem-fio. Basicamente, existem dois tipos de Redes Móveis sem-fio: as redes *ad hoc* e as redes infra-estruturadas. É abordado nesta pesquisa o tipo de rede *ad hoc*.

A integração de computadores com comunicações e outras formas de tecnologias de informação está criando novas formas de sistemas e serviços de informação distribuída. É o surgimento dos ambientes de computação ubíquos que deverão ser a nova forma de trabalho do próximo século. Este é o cenário altamente desafiador e excitante que motiva a computação móvel. Nesse cenário as redes móveis *ad hoc* terão uma importância cada vez maior.

Neste contexto tecnológico e móvel, em que a Ciência da Computação e as telecomunicações se relacionam as redes *ad hoc* ganham força. Entre as características destas redes que contribuem para tal, destaca-se: (i) fácil instalação; por não serem dependentes de infra-estrutura fixa. (ii) Apresentam maior conectividade, uma vez que a comunicação pode ser direta, ou seja, não é obrigada a passar pela infra-estrutura; (iii) além da mobilidade, seu fator de maior sucesso.

Fica clara a participação de tais redes no processo de evolução tecnológica que vivemos. Cada vez mais se da à necessidade de dispositivos que não

dependem de qualquer estrutura que detenha sua mobilidade. Também fica muito claro neste contexto o papel da segurança computacional como base do sucesso da tecnologia apresentada. Não é exagero dizer que o fator determinante para que a tecnologia alcance patamares sólidos dentro da sociedade e crie raízes fortes o suficiente para sair de um contexto idealizado e alcançar em definitivo níveis comerciais, é a segurança da informação que circula neste ambiente.

É justamente o fator de maior importância neste contexto o mais delicado e difícil de ser resolvido. Por motivos que são explanados neste trabalho, veremos como e porque hoje ainda é tão fácil manipular, desviar ou roubar informações de uma rede *ad hoc.* São abordados em detalhes os pontos críticos no protocolo de roteamento de informações que será simuladamente atacado no intuito de provar a existência de graves falhas de segurança no protocolo analisado.

1.1 Tema

É abordado para este Trabalho de Conclusão de Curso o tema de simulação de cenários de ataque a uma rede *ad hoc*, a segurança relacionada a elas e também a questão da intrusão em protocolos de roteamento.

1.2 Área de Pesquisa

Redes de Computadores sem fio e sem infra-estrutura, redes *ad hoc*, protocolos de comunicação sem fio.

1.3 Justificativa.

Os requisitos de segurança de redes *ad hoc* estão intrinsecamente ligados ao tipo de cenário de aplicação da tecnologia. Atualmente, operações táticas militares é a principal aplicação.

Unidades de combate ou resgate, equipadas com dispositivos de comunicação sem fio, em incursão num terreno hostil, constituem uma rede *ad hoc* a fim de trocar informações sobre a missão de forma segura. Cabe lembrar que estes mecanismos devem estar consoantes com as restrições encontradas nos sistemas de comunicação móvel, tais como escassez de recursos de rádio, pouca memória, baixa capacidade de processamento e duração restrita da bateria. Posto isto, deve-se imaginar que as abordagens tradicionais dos

problemas de segurança em redes de comunicação não são totalmente e facilmente portáveis para estes cenários de aplicação.

Permanecendo como desafio o desenvolvimento e implementação de mecanismos de segurança robustos, do ponto de vista das ameaças para a rede; flexíveis, do ponto de vista da dinâmica da rede, e compatível, do ponto de vista das restrições do sistema.

1.4 Objetivos

Além de levantar as principais bibliografias hoje existentes sobre o assunto e buscar uma significativa melhora na percepção pessoal sobre o assunto, destaca-se o objetivo geral e os específicos a seguir mostrados.

1.4.1 Objetivo geral

O objetivo da pesquisa visa estudar, testar, simular e possivelmente acrescentar informações sobre estudos feitos sobre a simulação de ataques em diversas situações (cenários) possíveis de uma rede *ad hoc* real. Buscando determinar possíveis problemas relacionados com a questão da segurança e contribuir de forma a deixar clara e rica as informações referentes ao assunto.

1.4.2 Objetivos específicos

- Estudo das tecnologias e do estado da arte existente sobre o assunto;
- Simulação de cenários baseado no algoritmo AODV (*Ad hoc on Demand Distance Vector*) de roteamento para redes *ad hoc*.
- Possível implantação no mercado dos resultados obtidos: área militar, telecomunicações, comunidade Internet, e exploração espacial;
- Buscar o aprimoramento ou uma solução para todos os níveis da segurança em redes *ad hoc* através da exposição dos resultados.
- Explicar as causas do aumento da demanda desta tecnologia e os benefícios que ela pode oferecer ao usuário.

1.5 Problema

Ao contrário das redes de comunicação tradicionais, as redes sem fio e sem infra-estrutura, demandam mecanismos provedores de segurança que se compatibilizem com as características deste novo paradigma de redes de comunicação de dispositivos móveis.

A maior parte da pesquisa em redes *ad hoc* destina-se ao desenvolvimento dos mecanismos básicos de operação. Muito ainda deve ser feito no que tange aspectos de segurança, principalmente considerando cenários de operação hostis como em aplicações militares e transações comerciais. Os requisitos e a complexidade dos mecanismos de segurança devem variar com o tipo de aplicação.

As redes *ad hoc* apresentam vulnerabilidades em diversos níveis nas suas atuais implementações, sendo o objetivo das pesquisas em segurança o de dotar estas implementações de mecanismos capazes de conferir à rede a segurança em seus diversos aspectos, respeitando as limitações do sistema, como a escassez de recursos de rádio, bateria, processamento e memória.

1.6 Metodologia

É abordada a estratégia de análise da simulação, pois são simulados os principais possíveis cenários para roteamento em redes *ad hoc* através do simulador *Network Simulator*. Baseado em dados obtidos com a simulação é possível fazer a análise detalhada dos resultados.

1.7 Organização do trabalho

Este trabalho está organizado da seguinte forma: No capítulo 2 é apresentado um levantamento dos principais conceitos abordados neste trabalho, onde é apresentada uma breve contextualização sobre a segurança em redes *ad hoc,* os protocolos de roteamento e muitos conceitos ligados a estes tópicos.

No capítulo 3 a ênfase está na fundamentação e detalhamento dos ataques ao protocolo AODV, é mostrado neste capítulo 3 de que forma um ataque se torna bem sucedido ao alterar a rotina do protocolo estudado.

Já no capítulo 4 é explicado como se sucede a simulação dos ataques, o cenário de simulação, o simulador e as tecnologias envolvidas.

E para complementar o capítulo anterior, o capítulo 5 mostra uma análise dos resultados obtidos com a simulação e também apresenta com dados estatísticos o que acontece no procedimento do ataque.

Concluindo o trabalho, o capítulo 6 mostra as principais conclusões tiradas do trabalho junto com uma apresentação dos trabalhos futuros.

2 Fundamentação Teórica

2.1 As redes Ad hoc

Atualmente existem basicamente dois tipos de redes sem fio. O primeiro tipo são as redes infra-estruturadas, que se conectam, se comunicam e fazem o roteamento das informações com unidades da rede através de bases fixas. Esse tipo de rede é muito comum hoje em dia e pode ser encontrado com facilidade até mesmo em grandes centros públicos, como *shoppings* e aeroportos, são conhecidas pela sigla em inglês *WLANs – wireless local area networks*. Possuem uma nomenclatura diferente dependendo da distância que a rede atua, por exemplo, a *WPAN – wireless personal area network*, onde a distância entre os dispositivos é pequena e não é preciso tanto desempenho de velocidade.

O segundo tipo de rede sem fio é a rede móvel sem fio e sem infra-estrutura, também conhecido como rede *ad-hoc*, que é o foco deste trabalho.

Redes *ad hoc* não possuem roteadores fixos nem qualquer tipo de base de transmissão fixa, cada nodo da rede é capaz de se movimentar, conectar e transmitir dados dinamicamente e de maneira arbitrária. Cada unidade da rede funciona como um roteador que descobre e mantém rotas para outras unidades da rede.

Devido ao raio de transmissão limitado, muitos saltos podem ser requeridos para que haja comunicação entre nodos distantes através da rede. Devido a isso, funcionalidades de roteamento são incorporados em cada nodo, e assim redes *ad hoc* adquirem características como topologia dinâmica, multi-salto e em constante movimentação [7].

As unidades de rede são usualmente chamadas de nós ou nodos e seu conceito é muito importante no contexto de redes *ad hoc* e também muito utilizado neste trabalho. Os nodos são elementos que implementam a lógica associada aos computadores na rede, sejam eles *hosts* ou roteadores. Os nodos de uma rede *ad hoc* implementam o protocolo especifico para isso, como o AODV que será explicado mais adiante. Também possuem recursos próprios e são elos fundamentais da rede.

O ponto crítico em uma rede *ad hoc* são os protocolos de roteamento. Os protocolos implementados devem se preocupar necessariamente com as limitações que este tipo de rede possui como baixa capacidade de energia e de processamento de seus nodos, por exemplo, além de que os nodos estão em constante movimento. É também no protocolo que ocorrem os ataques mais comuns e perigosos da rede, como será explicado mais adiante.

2.2 Questões de segurança em Redes Ad-hoc

Estabelecer uma rede segura e ao mesmo tempo robusta e eficiente é o principal desafio a ser alcançado em qualquer tipo de rede. O que torna essa questão ainda mais desafiadora na rede *ad hoc*, é o fato de essa rede possuir características peculiares como: uma arquitetura aberta e topologia dinâmica, como já mencionado.

O grau de comprometimento entre os nodos é alto, já que todos dependem uns dos outros para o pleno funcionamento da rede. Além de que, a perda de um único nodo acarreta no comprometimento de todo esquema de segurança.

Atualmente a maioria dos protocolos de roteamento utilizados foram propostos e analisados em cenários idealizados, onde não foram considerados os problemas de segurança relativos aos protocolos de roteamento. Como conseqüência, os protocolos são falhos no que diz respeito à segurança no roteamento, além de todas as outras características de vulnerabilidade que são intrínsecas de uma rede *ad hoc*.

Até mesmo os protocolos de redes sem fio como o 802.11, assumem um meio de interação confiável e cooperativo, como resultado, fica muito simples para nós maliciosos atuarem sobre tal protocolo e deturpar a rede.

O canal de acesso ao meio sem fio está acessível tanto para usuários legítimos dessa rede, como para usuários maliciosos. Sendo assim, nós maliciosos ou comprometidos podem participar do processo de descoberta de rotas e aproveitar-se disso. Por exemplo, 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[3][22]. Mais adiante, outras ações maliciosas são apresentadas.

Para que a rede torne-se confiável, ela deve possuir um modelo de segurança completo, o qual deve considerar todos os principais aspectos na área da segurança, que são prevenção, detecção e reação. Cada um de seus nodos deve estar preparado para enfrentar um adversário (nó malicioso), garantindo indiretamente maior grau de segurança para toda a rede [1].

Além disso, precisam prover serviços seguros como autenticação, confidencialidade, integridade, anonimato para usuários móveis, e tudo isso, é claro, sem perder aspectos de eficiência de roteamento.

Yang et al., da uma visão mais ampla de todo o esquema de segurança que uma rede deve prover (baseado no modelo OSI), independente do foco dos protocolos. Veja a **Erro! Fonte de referência não encontrada.**:

Tabela 1: Tabela de questões de segurança relevantes no modelo de camadas OSI.

Camada	Questão de segurança
Aplicação	Detectar e prevenir vírus, códigos maliciosos e alterações na aplicação.
Transporte	Autenticar e segurar a comunicação ponto a ponto através da criptografia dos dados.
Rede	Proteger os protocolos de roteamento e encaminhamento *ad hoc*.
Sessão	Proteger o protocolo base de rede sem fio e prover suporte seguro na camada de sessão
Física	Prevenir o bloqueio de sinal de ataques de “fora de operação”

As vulnerabilidades da camada de rede geralmente caem em duas categorias: ataques de roteamento e ataques de encaminhamento de pacotes de dados [25].

Ataques de roteamento se referem a toda ação na rotina de roteamento que não segue as especificações do protocolo de roteamento.

Embora um modelo de segurança completo necessite prever o ataque, detectá-lo e conseguir tratá-lo, os protocolos que buscam o foco em maior segurança, se atêm em apenas uma das questões anteriores. E por isso há hoje basicamente dois meios de proteger uma rede *ad hoc*: pró - ativamente e reativamente. A maneira pró-ativa tenta frustrar o ataque antes que ele aconteça, geralmente através de técnicas de criptografia, em contrapartida, a maneira reativa busca detectar o ataque e agir de acordo.

A bibliografia esta repleta de propostas de modelos seguros para o roteamento de informações. Geralmente são baseados em melhorias feitas em algum protocolo existente. Dahill *et al.* propõe o protocolo ARAN (*Authenticated Routing for Ad hoc Network*) [5], que se baseia no protocolo AODV e em certificados digitais, através de assinaturas digitais em mensagens do protocolo. Em uma abordagem similar Zapata, M. e Asokan, N. propõem o protocolo SAODV (*Secure AODV*) [8]. O protocolo também explora o campo das assinaturas digitais, porém requer apenas que as mensagens sejam assinadas pelo emitente. Para proteção dos campos das mensagens, alteração de campos são a principal forma de ataques no protocolo, são usadas cadeias de *hash* [10].

2.2.1 Prevenção de falhas de Segurança

Os protocolos de roteamento implementam técnicas para manter atualizadas as informações sobre as rotas que possuem em suas tabelas de roteamento [3].

Essas técnicas têm como objetivo perceber o mais rapidamente possível mudanças na topologia da rede e assim ganham maior poder de prevenção.

A prevenção também é a idéia quando são utilizadas as chaves simétricas, que basicamente funcionam baseadas na distribuição de chaves secretas para cada par de nós (origem e destino) que desejam comunicar-se.

A dificuldade na utilização desse mecanismo é a distribuição das chaves secretas, porém tem a vantagem de ser mais rápida computacionalmente, e não requerer muito processamento do nodo.

Chaves assimétricas são muito mais seguras que chaves simétricas, pois somente as chaves públicas são divulgadas, no entanto, requer um poder de processamento muito maior nos nodos, o que nem sempre está disponível.

2.2.2 Detecção de intrusão

A intrusão pode ser definida como “um conjunto de ações que visa comprometer a integridade, confiabilidade ou a disponibilidade de algum recurso da rede” [9]. Assim sendo, a detecção de intrusão pode ser definida como um mecanismo automático de detecção e geração de alerta para que sistemas de segurança possam agir de forma eficiente [12].

Sistemas de detecção de intrusão (SDIs) são sistemas que monitoram continuamente a rede em busca de atividade suspeita e, caso necessário, bloqueiam a conexão do nodo que age com atividade suspeita, ou seja, tais sistemas identificam e respondem a atividades não usuais na rede. Porém, eles não previnem o nodo malicioso de entrar na rede, o sistema apenas age após a intrusão e então tenta detectar o momento do ataque para então agir.

A ação de um SDI depende do tipo de ataque detectado. Os sistemas mais comuns geralmente respondem a um ataque reiniciando os canais de comunicação entre todos os nodos ou então identificando e cortando canais de comunicação do nodo detectado como malicioso, se for o caso.

Neste trabalho são apresentados vários cenários de intrusão em rede *ad hoc*, onde um sistema de intrusão eficiente se mostra fundamental.

2.3 Protocolos de roteamento

Os protocolos são responsáveis por procurar, estabelecer e manter rotas entre nós que querem se comunicar. Corson e Macker [4] sugerem algumas propriedades que protocolos de roteamento de redes *ad hoc* devem ter:

- *Operações distribuídas:* Propriedade intrínseca a rede devido a sua natureza descentralizada.
- *Segurança:* Como já visto em 2.2 esta é uma propriedade critica nos protocolos de roteamento de redes *ad hoc*.
- *Hibernação:* É muito desejável que nodos tenham capacidade de conservar sua energia por um período maior possível. O protocolo

ao detectar a falta de atividade do nodo, deve prover mecanismos que salvem o máximo de energia possível.

- *Suporte a rota unidirecional:* O protocolo deve ser capaz de distinguir entre tráfegos de dados uni e bi direcionais.

Os protocolos de roteamento das redes *ad hoc* são divididos em duas categorias, os protocolos **(i) pró-ativos** e os **(ii) reativos** ou sob demanda.

(i) Os protocolos pró-ativos mantêm uma tabela com informações sobre rotas para todos os nós da rede, mesmo as que nunca foram usadas ou pouco usadas. Os nós da rede trocam mensagens periódicas entre si para sempre manter atualizada a tabela de rotas. Esse tipo de protocolo tende a ser mais veloz que os do tipo reativos por ter sempre pronto as rotas para o destino; porém o consumo de energia e banda passante tende a ser muito alto e em alguns casos as tabelas podem ser insuportavelmente grandes para dispositivos com limitações de memória.

Os principais protocolos pró-ativos são o *Destination-Sequenced Distance Vector* (DSDV) e o *Wireless Routing Protocol* (WRP).

(ii) Os protocolos reativos estabelecem a rota apenas quando ela é solicitada por um nó de origem. O nó de origem faz um pedido de descoberta de rota para seus nós vizinhos (nós que estão no raio de alcance) e caso eles não saibam a rota para o nó destino fazem um pedido para os vizinhos deles, até encontrar o nó destino ou um nó que saiba a rota para o destino. Esse tipo de protocolo é a melhor solução quando a escassez de energia e de tráfego são fatores críticos, como também quando há um intenso movimento dos nós da rede, pois neste caso, um protocolo pró-ativo manteria em sua tabela uma rota que nem existe mais. Os principais protocolos reativos são o *Ad hoc On demand Distance Vector* (AODV) e o *Dynamic Source Routing* (DSR)

O foco deste trabalho é o protocolo de roteamento AODV.

2.3.1 Protocolo de roteamento AODV

O protocolo AODV foi projetado para o uso em redes *ad hoc* que podem possuir até milhares de nós móveis. É implementado de um a modo a evitar o desperdício de banda e minimizar o uso de memória e processamento nos nós

que atuam como roteadores, uma vez que se trata de um protocolo reativo e não necessita ter a rota previamente conhecida. É capaz de manter rotas unidirecionais e multidirecionais. Também provê um rápido mecanismo de detecção de rotas inválidas através do uso de mensagens de RRER (2.3.1.4).

2.3.1.1 Funcionamento

Durante a operação do protocolo reativo em uma rede *ad hoc*, os nós participantes geram mensagem de determinados tipos[1] e as trocam convenientemente entre si, gerando assim vários cenários de funcionamento, os quais são explicados sucintamente a seguir.

Quando um nodo deseja enviar uma mensagem para algum outro nodo (nodo destino), e não possui a rota para tal, é iniciado um processo de descoberta da rota, da origem até o destino. Tal processo também é iniciado se a rota armazenada estiver inválida ou em desuso.

O processo inicia com a transmissão de uma mensagem de *route request* (RREQ) para seus vizinhos, que por sua vez enviam o sinal via *broadcast* até que a RREQ chegue a um nodo que conheça a rota para o destino ou para o próprio nodo destino (processo de difusão da mensagem). O valor que está no campo “Número de seqüência do destino” na mensagem RREQ (ver formato de mensagem no capítulo 2.3.1.2) é o último número de seqüência conhecido para o destino requerido e foi copiado do respectivo campo na tabela de roteamento. Caso o “Número de seqüência” não é conhecido, o marcador de *unknown sequence number* deve estar ativo na mensagem. O protocolo utiliza tal número de seqüência para assegurar que não ocorram laços durante a busca pela rota. Assim cada nodo mantém uma entrada na sua tabela de roteamento com seu número de seqüência do destino, sempre associado ao endereço IP do destino. Este número é atualizado toda vez que o nodo recebe informações novas de mensagens (RREQ, RREP, RERR) relacionadas com o destino.

O nó destino ou um nó intermediário que possua uma rota para o destino, envia uma mensagem de RREP de volta para o nó de origem assim que este receber a mensagem de RREQ. À medida que a mensagem trafega

[1] Vide capítulos 2.3.1.2 a 2.3.1.4

de volta para a origem, os nós intermediários atualizam seus ponteiros em direção ao destino e assim que a mensagem chega à origem, está estabelecida a rota, e todos os nós estão aptos a transmitir pacotes de conteúdo pelo caminho estabelecido.

Caso a mensagem de RREP contiver um número de seqüência maior ou o com o mesmo número de seqüência e com o contador de saltos menor, o nó atualiza a tabela de roteamento para este destino e passa a usá-lo.

Tal rota é mantida enquanto ela permanecer ativa, isto é, enquanto houver tráfego passando pela rota periodicamente. Caso o tempo de vida da rota terminar, ela é removida da tabela de roteamento por algum nó intermediário. Caso o nó origem desejar enviar informações pela rota após o seu rompimento, uma mensagem de RERR é envida ao emissor, que terá de reiniciar o processo de descoberta de rota.

2.3.1.2 Formato de uma mensagem de *Route Request*.

Uma RREQ é enviada na forma de um pacote de 160 bits de informação. Veja se formato na Figura 1.

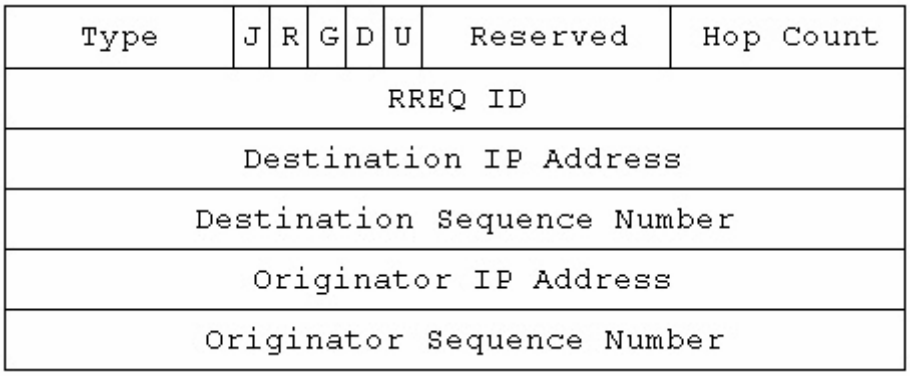

Figura 1: Formato de mensagem RREQ.

Contêm os seguintes campos:

- *Tipo J|R|G|D|U (32bits):*

  J|R: Indicam comunicação *multicast*;

  G: Indica se um RREQ deve ser enviado ao destino por um nó intermediário;

  D: Indica que somente o destino pode responder a esta requisição;

  U: Número de seqüência do destino é desconhecido.

- *RREQ ID:* Identifica juntamente como o endereço da fonte, um pedido de requisição de rota.
- *Contador de saltos:* Informa o número de saltos (nodos) do nodo origem até o nodo corrente.
- *Número de seqüência do destino (32bits):* Contêm o último número de seqüência recebido pela fonte, referente a alguma rota para o destino.
- *Número de seqüência da origem (32bits):* Contêm o número de seqüência atual.
- *Endereço IP destino (32bits):* Indica o endereço IP do nodo final da rota.
- *Endereço IP origem (32bits):* Indica o endereço IP do nodo origem.

2.3.1.3 Formato de uma mensagem de *Route Reply*.

Uma RREP é enviada na forma de um pacote de 160 bits de informações. Veja seu formato na Figura 2.

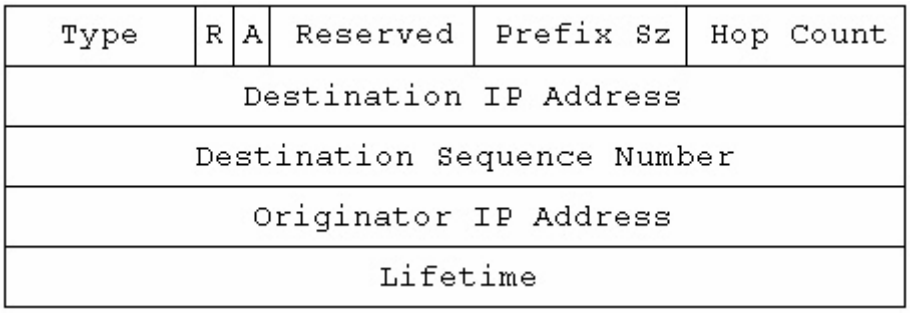

Figura 2: Formato de mensagem RREP.

Contêm os seguintes campos:

- *Tipo R| A (32bits):*

  R – Repair: Indica comunicação *multicast*;

  A – *Acknowledgment:* Indica a necessidade da transmissão de uma confirmação de recebimento de resposta (RREP-ACK) pelo nó fonte. A mensagem RREP-ACK possui 16 bits.

- *Prefix size: (5 bits)* Especifica que o próximo salto indicado, pode ser usado por algum nodo com o mesmo prefixo do destino desejado.
- *Contador de saltos:* Informa o número de saltos (nodos) do nodo origem até o nodo corrente.

- *RREQ ID:* Identifica juntamente como o endereço da fonte, um pedido de requisição de rota.
- *Número de seqüência do destino (32bits):* Contêm o último número de seqüência recebido pela fonte, referente a alguma rota para o destino.
- *Número de seqüência da origem (32bits):* Contêm o número de seqüência atual.
- *Life time:* Indica o tempo em milisegundos para cada nodo receber a RREP, considerando a rota válida.

2.3.1.4 Formato de uma mensagem de *Route Error*.

A mensagem RERR é enviada toda vez que ocorre a quebra do enlace e torna um ou mais vizinhos inalcançáveis para algum nodo destino. Veja seu formato na Figura 3.

Type	N	Reserved	Dest Count
Unreachable Destination IP Address			
Unreachable Destination Sequence Number			
Additional Unreachable Destination IP Address			
Additional Unreachable Destination Sequence Number			

Figura 3: Formato de mensagem RERR.

- *Tipo*

  N: Indica que um nodo reparou um enlace e que os nodos subseqüentes não devem apagar a rota.
- *DestCount:* Conta o número de destinos inalcançáveis e deve no mínimo ser 1.
- *Endereço IP inalcançável:* Indica o endereço IP do destino que se tornou inalcançável, até o momento da quebra.
- *Número de seqüência do destino inalcançável:* Número de seqüência na entrada da tabela de roteamento referente a este destino.

2.3.2 Falhas de segurança do Protocolo.

Esta seção apresenta e descreve quais as falhas de segurança especificamente para o protocolo AODV. Como ocorrem, e quais suas conseqüências no funcionamento da rede.

Como já dito, a cooperação entre nós é assumida, assim sendo, ataques maliciosos podem deturpar operações da rede, violando as especificações do protocolo.

Ocorrem mais usualmente tipos de ataques de roteamento e ataques de encaminhamento de pacotes de dados.

Em ataques que visam o encaminhamento de pacotes, o atacante pode alterar campos do próprio pacote recebido no intuito de invalidar ou subverter o encaminhamento desse pacote e dos demais.

Ataques de Modificação:

Nesse tipo de ataque, o nó malicioso altera informações de mensagens de roteamento recebidas, gerando informações de rotas falsas, ou tenta atrair para si o tráfego da rede, fazendo com que todas as rotas passem por ele, no AODV, o nó malicioso simplesmente diminui o valor do campo *Hop Count* para que isso aconteça.

Com uma simples falsificação do campo de *Número de seqüência do destino* é possível redirecionar o tráfego da rede e até mesmo impedi-lo de alcançar seu destino [3].

Ataques de Fabricação:

O nó malicioso pode inclusive “fabricar” sua própria mensagem de RREQ, RREP ou RERR, cada uma tendo uma conseqüência diferente para o desempenho da rede.

A fabricação de uma mensagem de RERR, por exemplo, para certo destino, tornaria esse nó (destino) inalcançável. Caso seja utilizado também um número de seqüência muito alto, esse ataque poderia fazer com que esse nó ficasse inalcançável durante um longo período na rede.

Ataques de Personificação:

Em um ataque de personificação, o nó malicioso utiliza o endereço de outros nós da rede, fingindo ser quem ele não é. Como não temos nenhum tipo de mecanismo de autenticação nos protocolos de roteamento, não há como os outros nós saberem se o nó malicioso é ou se o nó não é quem ele realmente diz ser.

Já em ataques visando o roteamento dos pacotes, nodos atacantes podem criar laços eternos ou até mesmo criar um congestionamento insuportável para a rede.

Embora muitas vezes ocorra a ação de somente um nó malicioso, devemos esperar também o ataque de vários nós maliciosos, que podem atuar em conjunto em uma rede, causando ataques “cooperativos”. Esse tipo de ataque é muito mais difícil de ser detectado, e até hoje nenhuma das soluções propostas para a segurança no roteamento das redes *ad hoc* trata completamente desse tipo de ataque.

3 A simulação

Este trabalho esta baseado no *paper* de Ning P. e Sun K., "*How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols*" [13], e visa analisar caso por caso os ataques que ocorrem em determinados cenários de uma rede *ad hoc*, conforme descrito em [13] e introduzido em 2.3.1. Após uma análise detalhada dos tipos de ataque, far-se-á o uso do simulador *Network Simulator* [21], para comprovar via simulação os efeitos dos ataques.

São padronizados alguns parâmetros referentes ao cenário da simulação. Os parâmetros estão definidos de acordo com a **Erro! Fonte de referência não encontrada.** e fazem referência aos cenários descritos em [13].

Tabela 2: Parâmetros da simulação.

Tipo de comunicação	CBR
Número de Nodos	5 a 20
Área de simulação	1000m X 600m
Tempo de simulação	100 segundos
Tempo de parada	2 segundos
Taxa de transmissão de pacotes	4 pacotes por segundo
Raio de transmissão	250 metros
Banda	2 Mbps
Número de atacantes	1
Número de conexões	20

A seguir é explicada a metodologia empregada na simulação dos cenários, e usa a terminologia usada em [13] para fins de padronização.

3.1 O Network Simulator

O *Network Simulator* (ns-2) é um simulador de eventos discretos usado para simular cenários de redes sem fio e também infra-estruturadas. Suporta vários tipos de protocolos de roteamento e modelos de tráfego, incluindo protocolos de redes *ad hoc* que são objetos de estudo neste trabalho. Desenvolvido por pela universidade de Berkley, Estados Unidos como parte do projeto VINT [21].

O simulador é orientado a componentes e escrito na linguagem de programação C++. Sua arquitetura esta baseada em um interpretador de *scripts* OTcl, escritos na linguagem TCL (*Tool Command Language*) [14], juntamente com um módulo C++.

TCL é uma linguagem de programação *open source* muito utilizada no mundo. Sua sintaxe possibilita a criação de programas inteiros na linguagem e no caso do ns-2, executa embutida em softwares escritos em outras linguagens.

A utilização de duas linguagens de programação contribui para a flexibilidade do simulador. C++ é usado para o processamento de eventos e forma o núcleo central do simulador, tarefas para as quais o uso de TCL ficaria inviável devido a velocidade. Porém, a linguagem TCL provê muitas vantagens para a produção de *scripts* de cenários de simulação e protocolos de roteamento e permite que parâmetros de simulação sejam modificados sem a necessidade de compilação do código, já que TCL é uma linguagem interpretada.

Os eventos gerados são gerenciados por um escalonador de eventos que faz parte de sua arquitetura. Um evento para o simulador é um objeto na arquitetura C++, com um identificador único, um tempo de escalonamento e um ponteiro para um objeto que trata o evento.

A saída do simulador gera arquivos *nam* que podem ser representados graficamente através de um programa auxiliar, o NAM (Network Animator)[21]. Também é gerado um arquivo *trace* que guarda todos os eventos gerados na simulação, como pacotes enviados, recebidos e também traz informações

detalhadas sobre todos os campos das mensagens geradas, como o tipo de protocolo, o número de IP do destino e da origem.

3.2 Metodologia de análise da simulação

A seguir são descritos os objetivos mais comuns nos ataques a uma rede *ad hoc* usando o protocolo AODV. São as metas que o atacante deseja atingir para que o ataque seja bem sucedido, também estão descritas as ações tomadas por um atacante a fim de atingir tais objetivos.

Neste trabalho são abordados apenas alguns dos problemas ocorridos em um ataque, apesar de existirem outros. Por exemplo, vazamento de informações sigilosas, alteração de dados, distorção de mensagens ou até mesmo colapso e pane na rede; porém tais possíveis problemas não serão abordadas neste trabalho.

Nesta abordagem primeiramente foram definidos alguns dos objetivos que um atacante de rede *ad hoc* deseja alcançar, para posteriormente serem analisados nos testes, são eles:

- **Interrupção de rota:** Visa à quebra de uma rota já estabelecida entre nodos da rede ou mesmo a inviabilidade que uma nova rota seja formada.
- **Invasão de rota:** Significa que o atacante se insere dentro de uma rota e passa a fazer parte do caminho de dados.
- **Isolamento de Nodo:** Faz com que o nodo atacado cesse a comunicação com o resto da rede, tornando-o isolado.
- **Consumo de recursos:** O nodo invasor faz com que seja consumida toda a banda de rede disponível formando um ciclo entre nodos, por exemplo, ou esgotando qualquer outro recurso necessário para o bom funcionamento da rede.

Também foram definidas quais ações que são tomadas pelo atacante para alcançar o seu objetivo:

- **Descarte de mensagem:** Onde um nodo invasor descarta a mensagem que recebe uma RREQ, por exemplo, ação muito usada no intuito de isolar um nodo.

- **Modificação e repasse:** O nodo invasor ao receber uma mensagem de qualquer tipo, a altera e depois a repassa normalmente, manipulando, assim, o fluxo normal da mensagem.
- **Resposta falsa:** O atacante forja uma mensagem em resposta a uma mensagem recebida e a envia.
- **Fabricação Ativa:** O atacante simplesmente fabrica e envia uma mensagem falsa.

Sendo que os tipos de mensagem de roteamento analisadas são:

RREQ (*Route Request*);

RREP (*Route Reply*); e

RERR (*Route Error*).

Sendo assim a seguinte padronização de abreviações foi seguida, conforme mostra a Tabela 3:

Tabela 3: Abreviações

Objetivos de ataque:	
Interrupção de rota	(RD)
Invasão de rota	(RI)
Isolamento de Nodo	(NI)
Consumo de recursos	(RC)
Ações de Ataque:	
Repasse de mensagem	(DR)
Modificação e repasse	(MF)
Resposta falsa	(FR)
Fabricação Ativa	(AF)
Mensagens de roteamento	
Route Request	(RREQ)
Route Reply	(RREP)
Route Error	(RERR)

Para fins de análise de simulação, os casos de ataque do protocolo são divididos em duas categorias, sendo elas *ataque simples* e *ataque composto*.

- *Ataques simples* ocorrem quando a manipulação acontece com uma única mensagem de roteamento.
- *Ataques compostos* são composições dos ataques simples, ou seja, são ataques simples repetidos ciclicamente, o que geralmente representa o funcionamento normal de um ataque ao protocolo na rede.

A análise acontece de forma que sempre combina o tipo de mensagem a ser analisada com uma ação e um objetivo de ataque. Ou somente a mensagem com a ação, ficando na forma: `tipoMensagem_acao_objetivo`, ou somente `tipoMensagem_acao`. Portando quando é analisado um ataque de modificação e repasse visando à interrupção da rota através de uma mensagem *Route Request*, a abreviação fica RREQ_MF_RD, sempre usando as abreviações da Tabela 3.

3.3 Análise de ações de ataque simples

O foco desta análise é a composição de ataques simples, que uma vez analisados e avaliados, são usados na análise de ataques compostos, que por sua vez são mais poderosos em termos de desestabilização da rede; sempre analisando sob a ótica do protocolo AODV, protocolo analisado neste trabalho.

A seguir são apresentados os ataques ao protocolo que são analisados via simulador, bem como as descrições detalhadas sobre a forma que o ataque consegue seu objetivo através de modificações nas mensagens de roteamento do protocolo. Para um melhor entendimento, as explicações são divididas por tipo de mensagem.

3.3.1 Ataques com mensagens de RREQ

- **Interrupção de rota fabricando uma mensagem de RREQ:**

Existindo uma rota estabelecida entre uma origem e um destino, um atacante pode quebrar tal rota enviando uma mensagem uma RREQ forjada. A RREQ é alterada da seguinte forma:

1. Altera-se o campo “TIPO”;
2. Modifica-se o IP destino para outro não existente; e
3. Modifica-se o IP origem para outro não existente.

Com isso a rota se estabelece do destino para a origem, com a origem sendo um nodo não existente. O nodo origem irá atualizar sua rota para o destino, que é um nodo não existente. Desta maneira a rota estará quebrada.

- **Invasão de rota fabricando uma mensagem de RREQ:**

O método de invasão é o mesmo descrito em RREQ_MF_RI. A invasão só ocorrerá se o atacante estiver no alcance do nodo origem. A intenção do atacante é iniciar uma mensagem forjada que inicia na origem e vai até o destino, assim, após o nó de origem receber a mensagem de RREP repassada do atacante, ele atualiza o seu próximo salto para o destino como sendo o nó atacante. A partir desse ponto o nó malicioso passa a fazer parte da rota.

- **Isolamento de nodo fabricando uma mensagem de RREQ:**

O método utilizado é o mesmo descrito em RREQ_MF_NI. O isolamento ocorrerá somente por um determinado intervalo de tempo, até que a rota seja restabelecida, e também não impede o nodo de enviar pacotes para seus vizinhos.

- **Consumo de recursos fabricando uma mensagem de RREQ:**

A única maneira de consumo de recursos da rede com esse tipo de ataque é enviando por *broadcast* mensagens para seus vizinhos de forma massiva.

- **Interrupção de rota modificando uma mensagem de RREQ recebida:**

  Se o nodo atacante é a única conexão entre a origem e o destino, ele pode fazer a conexão deixar de ser estabelecida, modificando alguns campos da RREQ que ele recebeu. A modificação ocorre da seguinte maneira:

  1. Altera-se o campo “TIPO”;
  2. Modifica-se o IP destino para outro não existente; e
  3. Modifica-se o IP origem para outro não existente.

Se ele não for à única rota, também há uma chance, fazendo o seguinte:

1. Troca-se o ID da mensagem do nodo origem para o ID da mensagem do nodo destino;

2. Troca-se o IP da origem pelo IP do destino na mensagem RREQ;
3. Incrementa-se o número de seqüência do destino e então o troca pelo número de seqüência da origem; e
4. Coloca-se um número de IP não existente no lugar do IP da origem.

O objetivo disso é inverter a ordem: propagar um RREQ do destino para origem em vez de o contrário. Os vizinhos do atacante aceitam a mensagem forjada desde que não tenham recebido uma RREQ do nodo destino antes (RREQ ID).

Devido à mensagem forjada conter um número de seqüência maior, seus vizinhos irão atualizar seu próximo salto para a origem que é um nodo que não existe, conforme indicado no campo de IP da origem no campo *IP header*.

Assim que o nodo destino receber a mensagem forjada, ele a descarta, pois parecerá que a mensagem se originou dele mesmo. Quando o nodo de origem recebe a mensagem forjada, ele atualiza sua tabela de roteamento reversa desde que o número de seqüência de origem, na mensagem forjada, seja maior que esta na sua tabela de roteamento.

Como a mensagem original RREQ esta sendo enviada via broadcast, o nodo origem irá receber a RREP correspondente, porém a rota estabelecida pela mensagem forjada prevalecerá, desde que não tenham recebido uma RREQ do nodo destino antes (RREQ ID).

O nodo origem começa a enviar pacotes através da rota estabelecida, mas todos os pacotes são descartados quando alcançarem o nodo não existente.

As entradas na tabela de roteamento escritas pela mensagem de RREQ podem ser atualizadas pala RREP e vice versa.

Os pacotes endereçados para o nodo inexistente são descartados e quando um nodo vizinho descobre a falha, ele manda uma mensagem RREQ de volta para origem.

- **Invasão de rota modificando uma mensagem de RREQ recebida:**

Considerando um cenário no qual o nodo atacante esta dentro do raio de transmissão do nodo que origina a mensagem de RREQ, a mensagem recebida deve ser modificada da seguinte maneira:

1. Sobrescreve-se o RREQ ID do nodo origem atualizado em pelo menos mais um;
2. Sobrescreve-se o número de seqüência da origem atualizado em pelo menos mais um; e
3. Sobrescreve-se o número de seqüência do nodo destino atualizado em pelo menos mais um.

Feito isso, o nodo atacante passa a mensagem por *broadcast* adiante para seus vizinhos. Tais vizinhos aceitam a mensagem forjada devido ao novo par de RREQ ID e endereço IP da origem. Como o número de seqüência da mensagem forjada é maior do que o número de seqüência que eles (nodos vizinhos) têm em suas tabelas de roteamento, eles atualizam o próximo salto para o nodo origem como sendo o nodo atacante. Quando a mensagem é recebida pelo nodo de origem verdadeiro, ele simplesmente a descarta, pois a mensagem aparece como sendo originada dele mesmo.

Assim que o nodo destino recebe a mensagem forjada, ele atualiza seu próximo salto para o nodo origem como sendo para o nodo de quem ele recebeu a mensagem forjada e atualiza o seu próprio número de seqüência para o máximo entre o seu número de seqüência atual e o número de seqüência do destino na mensagem de RREQ. Feito isso, ele copia o número de seqüência atualizado para o campo de “número de seqüência destino” na mensagem de RREP. A mensagem de RREP, então segue o caminho inverso até chegar ao nodo origem passando pelo atacante. Devido à mensagem de RREP conter um número de seqüência maior do que o que está na tabela de roteamento do nodo origem, que pode ter sido atualizada por outra mensagem de RREP, o nodo origem atualiza o seu número de seqüência para o que está na RREP recebida pelo atacante, e o coloca como sendo o próximo salto para o nodo destino. A partir desse ponto a rota esta invadida pelo atacante.

A Figura 4 sintetiza o caminho das mensagens até o estabelecimento da rota junto com o atacante. O círculo maior em volta do nodo origem mostra a

área de alcance do nó origem. O ataque descrito só é possível devido ao fato do atacante estar no raio de alcance do nó origem, caso contrário, o atacante estabelece um *loop* entre o nó imediatamente anterior a ele na rota da RREP.

Veja a Figura 4:

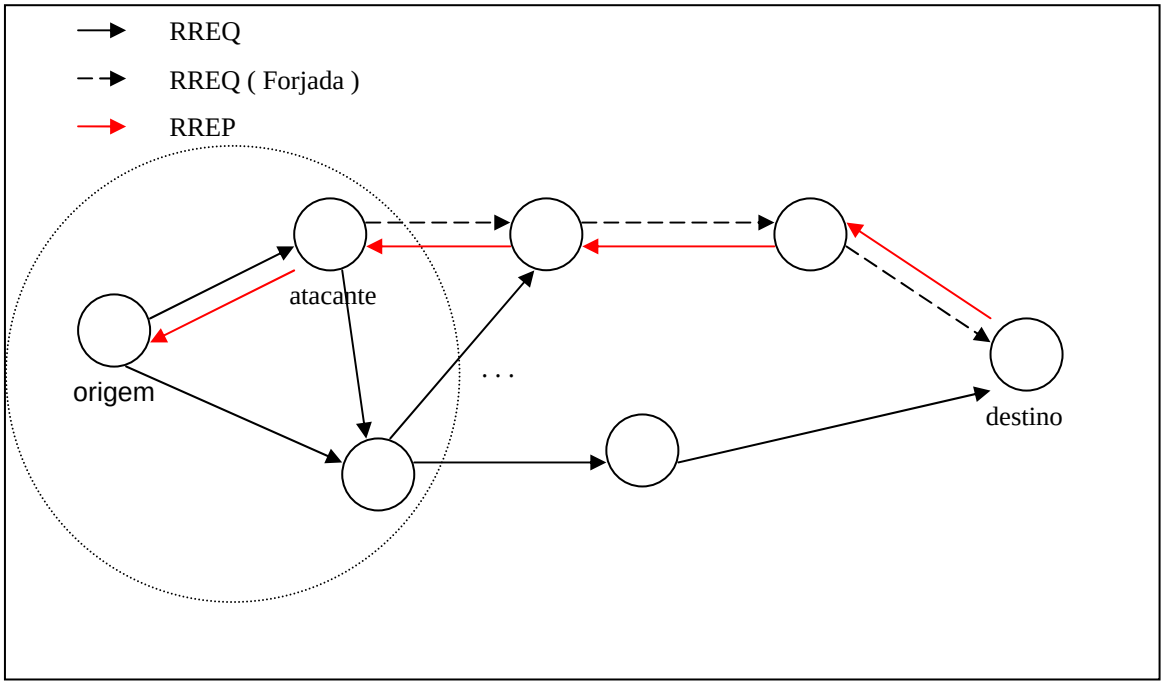

Figura 4: Cenário onde o atacante envia a mensagem para a vítima

Veja a Figura 5:

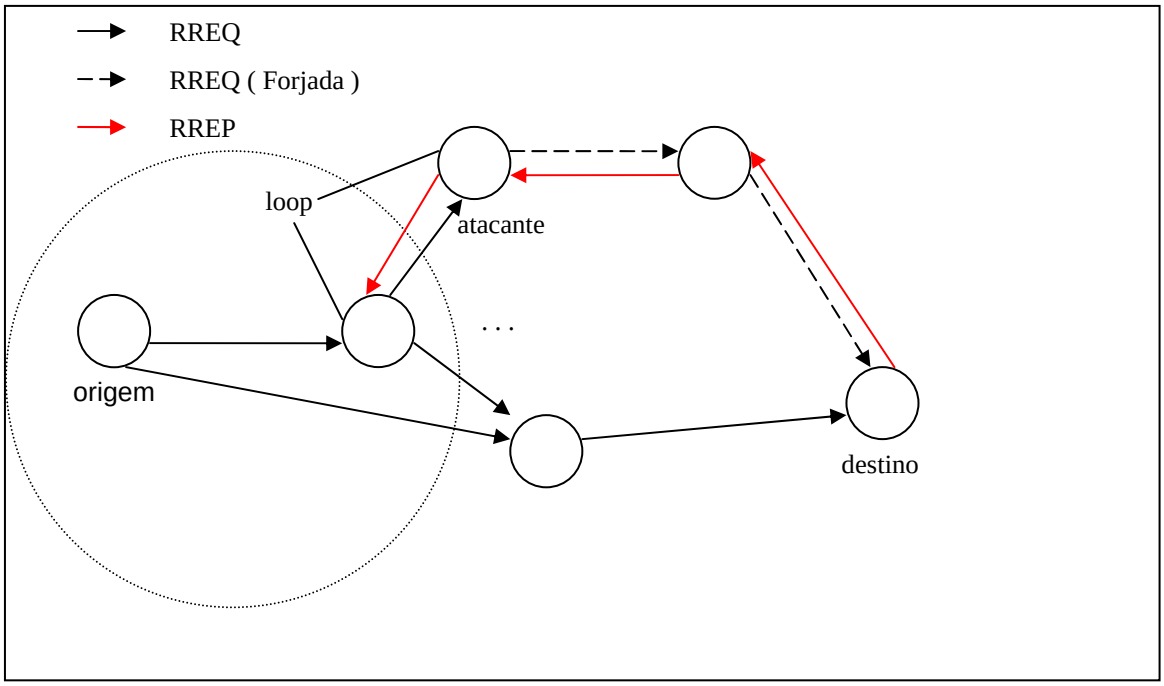

Figura 5: Cenário onde há um *loop* estabelecido entre 2 nodos

- **Isolamento de nodo modificando uma mensagem de RREQ recebida:**

De maneira geral, um nodo atacante não consegue isolar um nodo completamente apenas modificando uma única mensagem de RREQ, porém é possível evitar que um nodo receba pacotes por um determinado período de tempo fazendo as seguintes alterações na RREQ recebida:

1. Sobrescreve-se o RREQ ID para um número menor;
2. Coloca-se um número de IP destino não existente;
3. Incrementa-se o número de seqüência de origem em pelo menos um; e
4. Coloca-se um número de IP de origem não existente no campo *IP header* da mensagem.

Quando os vizinhos do atacante recebem a mensagem forjada, eles atualizam o próximo salto para o nodo origem para sendo um nodo não existente, conforme indicado no campo de número de IP de origem no *IP header* da mensagem forjada, e fazem isso porque o número de seqüência de origem é maior que o de suas tabelas, pois ele foi incrementado pelo atacante.

Devido ao número de IP destino ser um nodo não existente, nunca haverá uma mensagem de RREP para essa RREQ. E quando outros nodos quiserem mandar pacotes de dados para a origem, eles simplesmente usam a rota estabelecida pela RREQ forjada. Então os pacotes recebidos são descartados devido ao nodo não existente descrito na mensagem.

Essa situação persiste até o momento em que uma nova rota é estabelecida.

- **Consumo de recursos modificando uma mensagem de RREQ recebida:**

Devido ao ataque se caracterizar como sendo simples, fica difícil ocorrer um grande consumo de recursos forjando apenas uma RREQ, todavia é possível introduzir mensagens desnecessárias via *broadcast* na rede. O atacante, modificando o ID da mensagem RREQ recebida, a faz parecer recente e a repassa para os seus vizinhos. O impacto causado por esse ataque é mais bem sentido em ataques compostos.

3.3.2 Ataques com mensagens de RREP

- **Interrupção de rota fabricando uma mensagem de RREP:**

Existindo uma rota estabelecida entre a origem e o destino, um nodo que ataque esta rota pode interrompê-la forjando uma mensagem de RREP como segue:

1. Coloca-se o número 2 no campo de tipo e 1 no contador de saltos;
2. Coloca-se o endereço de IP da origem como sendo o nodo origem e o endereço de IP destino como o nodo destino da rota;
3. Incrementa-se o número de seqüência de destino em pelo menos um; e
4. Coloca-se o endereço IP da origem no cabeçalho do IP para um nodo não existente.

Quando o nodo de origem receber a mensagem forjada, ele irá atualizar sua rota para o destino que é um nodo não existente. Assim a rota estará desfeita.

- **Invasão de rota fabricando uma mensagem de RREP:**

Se um nodo malicioso conhecer a rota para o nodo destino e também para o nodo de origem, ele pode invadir a rota enviando uma mensagem de RREP para o nodo origem. Veja a Figura 6:

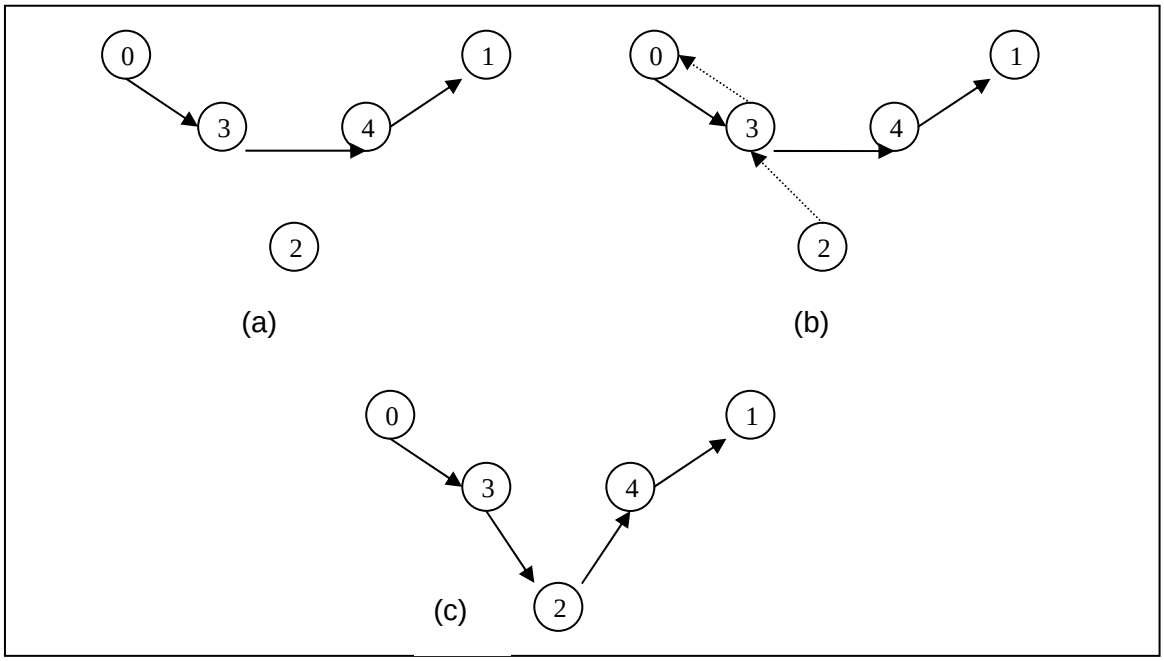

Figura 6: (a) Situação inicial onde o atacante envia o ataque. (b) Nodo 3 sob influência da mensagem forjada. (c) A situação final com o ataque efetivado.

A Figura 6(a) mostra uma rota estabelecida entre os nodos 0 e 1. O atacante (2) envia uma mensagem de RREP falsa para o nodo 3, que a repassa para o nodo 0.

Para que o ataque tenha efeito, a mensagem deve ser fabricada da seguinte forma:

1. O endereço de IP da origem deve ser o nodo 0;
2. O endereço de IP do destino deve ser o nodo 1;
3. O número de seqüência do destino deve ser incrementado em pelo menos 1;
4. O número de IP da origem no cabeçalho IP deve ser o nodo 2; e
5. O número de IP do destino no cabeçalho IP deve ser o nodo 3.

Quando os nodos 3 e 0 recebem a mensagem forjada, eles irão substituir o número de seqüência do nodo destino (1) para o número de seqüência do destino na mensagem forjada. O nodo 3 terá como seu próximo salto para o destino o nodo 2. Devido ao nodo 2 possuir a rota para o destino (1), ele agora pode encaminhar pacotes de dados de 0 para 1.

- **Isolamento de nodo fabricando uma mensagem de RREP:**

Não é possível para um atacante isolar um nodo enviando apenas uma mensagem forjada de RREP.

- **Consumo de recursos fabricando uma mensagem de RREP:**

Neste tipo de ataque, o atacante forma um *loop* na rede para consumir recursos dos nodos em *loop.* Veja a Figura 7.

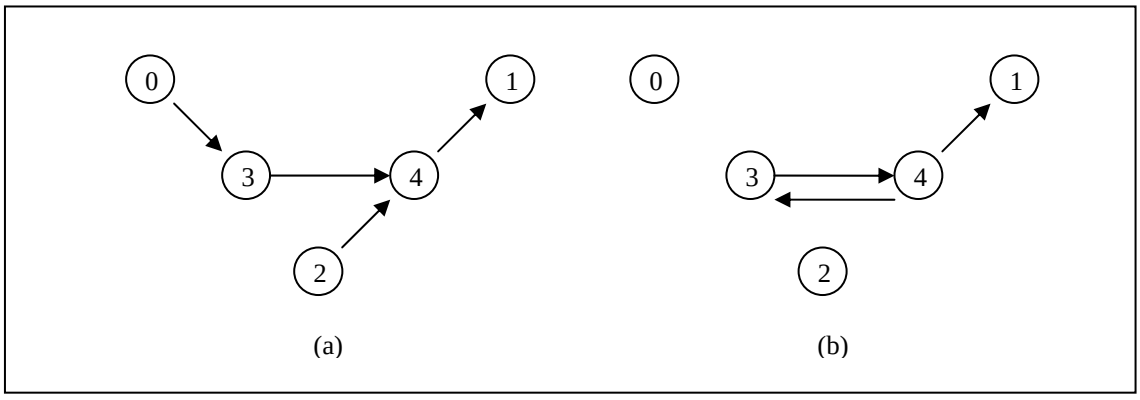

Figura 7: O ataque efetivando um *loop* na rede.

A mensagem forjada deve ser fabricada da seguinte forma:

1. O endereço de IP destino deve ser o nodo 1;
2. O número de seqüência do destino deve ser colocado como sendo número de seqüência do nodo 1 incrementado em um;
3. O endereço de IP da origem deve ser o nodo 0;
4. O endereço de IP da origem no cabeçalho de IP deve ser o endereço do nodo 3; e
5. O endereço de IP do destino no cabeçalho de IP deve ser o endereço do nodo 4.

Quando o nó 4 receber a mensagem forjada ele irá atualizar seu próximo salto até o destino como sendo o nó 3. O nó 4 enviará a mensagem forjada para o nó 3 que, por sua vez, a encaminhará ao nó 0. Se a partir deste ponto o nó 0 continuar a enviar dados para o nó 1, os dados serão enviados de 0 para 3, 4 e 3 novamente, caracterizando assim um *loop* entre os nós 3 e 4. Esses pacotes de dados serão descartados enquanto os campos TTL nos pacotes IP não forem 0.

- **Interrupção de rota usando descarte de mensagens RREP:**

Durante o processo de descobrimento de rota, o nodo destino envia uma mensagem de RREP de volta a origem, se tal mensagem passar pelo nodo malicioso, ele descarta essa mensagem e o nodo de origem nunca receberá uma RREP. Por outro lado, se o nodo origem tiver outros nodos vizinhos que não são maliciosos, a mensagem de RREP poderá chegar por outra rota e o efeito do nodo malicioso não terá grandes efeitos.

- **Invasão de rota usando descarte de mensagens RREP:**

O atacante não tem como invadir uma rota estabelecida, apenas descartando mensagens.

- **Isolamento de nodo usando descarte de mensagens RREP:**

Devido aos nodos se comunicarem com vários outros nodos, uma mensagem de RREP pode ser enviada por diferentes nodos vizinhos da origem, não necessariamente passando pelo atacante. Desta forma o atacante

pode fazer o descarte de uma RREP, porém não tem o controle sobre os outros nodos, de forma que o nodo origem não se isola somente com tal ação. Obviamente, se o nodo atacante for o único vizinho do nodo origem, este pode isolar o nodo parcialmente descartando todas as RREP recebidas.

- **Interrupção de rota forjando respostas com mensagens RREP:**

Após o recebimento de uma mensagem RREQ, um nó malicioso pode forjar uma mensagem de RREP desde que ele tenha uma rota suficientemente nova para o destino. Para que outras mensagens de RREP verdadeiras não se sobreponham à mensagem forjada, o atacante deve forjar sua mensagem da seguinte maneira:

1. O campo de endereço IP de destino deve conter o endereço do nodo destino;
2. O campo de endereço IP de origem deve conter o endereço do nodo origem;
3. No cabeçalho do IP, o endereço IP do nodo origem deve conter um endereço não existente;
4. No cabeçalho do IP, o endereço IP do nodo destino deve conter o endereço do nodo o qual o atacante recebera a mensagem RREQ; e
5. O número de seqüência do destino deve ser incrementado em pelo menos um e o contador de saltos atualizado para 0.

A mensagem forjada então segue o caminho para o nodo origem pela tabela de roteamento inversa, determinada pela mensagem de RREQ. Depois de ter recebido a mensagem de RREP forjada, o nodo vizinho do atacante irá atualizar o próximo salto para o destino como sendo um nodo não existente. Antes de receber a mensagem forjada, o nodo origem pode ter recebido mensagens legítimas de RREP, porém ele irá atualizar seu próximo salto para o destino conforme determinado pela mensagem falsa, desde que tal mensagem possua um número de seqüência maior ou um número de saltos menor do que está na tabela de roteamento do nodo de origem.

O resultado disto é que os pacotes enviados pelo nó origem serão perdidos, uma vez que são enviados para um nodo inexistente.

- **Invasão de rota forjando respostas com mensagens RREP:**

Se um o nodo malicioso já tiver uma rota para o nodo destino, ele poderá invadir a rota enviando uma mensagem de RREP forjada para a origem através da tabela de roteamento inversa. O propósito do atacante é garantir que outras mensagens de RREP, possivelmente com caminhos mais curtos para o destino, sejam descartadas pela origem. Para tanto, o atacante poderá colocar um número de seqüência de destino pequeno ou então decrementar o contador de saltos para 1. Após receber todas as mensagens de RREP, o nodo origem irá atualizar o seu próximo salto para o destino, como sendo o nodo do qual ele recebeu a mensagem forjada. Feito isso o nodo atacante passará a fazer parte da rota de dados.

- **Isolamento de nodo forjando respostas com mensagens RREP:**

Um atacante não é capaz de isolar um nodo forjando apenas uma mensagem de RREP.

- **Consumo de recursos forjando respostas com mensagens RREP:**

Este ataque consome poucos recursos da rede, pois diferente de uma mensagem de RREQ, é enviada via *unicast.*

- **Interrupção de rota modificando uma mensagem de RREP recebida:**

Durante o processo de estabelecimento de rota, no momento em que uma RREP passa pelo nó atacante, é possível prevenir o estabelecimento da rota fazendo uma das seguintes alterações:

1. Substitui-se o endereço IP do destino por outro endereço;
2. Substitui-se o endereço IP da origem por outro endereço;
3. Decrementa-se o campo TTL no cabeçalho do IP para 1;
4. Decrementa-se o campo de tempo de vida para 0; e
5. Substitui-se o endereço IP da origem no cabeçalho do IP para um endereço não existente.

Devido às modificações, o nodo de origem irá receber uma mensagem de RREP inválida ou não irá receber nenhuma mensagem. Como resultado, a rota

fica impedida de ser estabelecida. Porém, é importante notar que o nodo origem poderá receber mensagens de RREP de outros nodos.

- **Invasão de rota modificando uma mensagem de RREP recebida:**

O atacante escreve um número de seqüência de destino pequeno na mensagem RREP. Chegando a mensagem no nodo origem, este atualiza sua tabela de roteamento com a mensagem falsa que este recebeu e escolhe a rota que tem o maior número de seqüência de destino, que é a rota que envolve o nodo atacante.

- **Isolação de nodo modificando uma mensagem de RREP recebida:**

Não é possível isolar um nodo com apenas uma mensagem de RREP. Se o atacante for o único vizinho do nodo atacado, ele pode isolar o nodo parcialmente não deixando que ele receba as mensagens de RREP. Porém, esta situação se desfaz no momento que outro nodo se põe em alcance da origem.

3.3.3 Ataques com mensagens de RERR

- **Interrupção de rota fabricando uma mensagem de RERR:**

Se o nodo atacante estiver ao alcance de algum nó intermediário em alguma rota, é possível para o atacante enviar uma mensagem de erro ao nó intermediário de maneira que ele propague a mensagem de erro adiante.

Basta para isso fazer o seguinte:

1. Substituir o endereço do destino por outro inexistente;
2. Colocar o endereço do nodo intermediário como sendo o endereço de origem no cabeçalho de IP; e
3. Colocar o número de seqüência do destino inalcançável com um número maior que número de seqüência nodo destino.

Então o atacante envia a mensagem para os seus vizinhos. Se um dos nodos tiver a rota para o destino, ele desabilitará tal rota e ainda enviará a mensagem de erro forjada para os seus vizinhos, que farão o mesmo.

- **Invasão de rota fabricando uma mensagem de RERR:**

Não é possível invadir a rota com este tipo de ataque.

- **Isolamento de nodo fabricando uma mensagem de RERR:**

Não é possível isolar um nodo com este tipo de ataque.

- **Consumo de recursos fabricando uma mensagem de RERR:**

Este ataque fará com que vários nodos tenham que enviar mensagens de RREQ para estabelecer novas rotas, devido ao fato de que o atacante enviou uma mensagem de RERR, interrompendo, assim, varias rotas.

Ataques de RRER_DR se caracterizam quando um nodo atacante simplesmente descarta a mensagem de erro recebida sem notificar seus vizinhos.

- **Interrupção de rota usando descarte de mensagens RERR:**

Supondo que o atacante seja o único vizinho na lista de precursores do nodo que está enviando a RERR. Os nodos vizinhos do atacante não recebem a mensagem de erro, portanto eles continuam usando a rota inválida para enviar dados. Porém a rota estará quebrada apenas por um período curto de tempo.

- **Invasão de rota usando descarte de mensagens RERR:**

Não é possível invadir uma rota descartando uma mensagem de RERR.

- **Isolamento de nodo usando descarte de mensagens RERR:**

Não é possível isolar um nodo descartando uma mensagem de RERR.

- **Consumo de recursos usando descarte de mensagens RERR:**

Se os nodos vizinhos do atacante não recebem a mensagem de erro, eles continuam usando a rota inválida para enviar dados, porém não há muito consumo de recursos neste caso.

- **Interrupção de rota modificando uma mensagem de RERR recebida:**

Alterando uma mensagem de RERR recebida, é possível interromper todas as rotas que passam pelo atacante, bastando para isso substituir o endereço IP de destino que está inalcançável, por outro endereço de IP. O atacante deve

incrementar o número de seqüência do destino em pelo menos um, e então enviar a mensagem por *broadcast* aos seus vizinhos. Se um dos nodos vizinhos tiver uma rota válida para o nodo destino da mensagem forjada, o nó desabilita tal rota e atualiza o número de seqüência do destino para o número indicado pela falsa mensagem. Os vizinhos, então, encaminharão a mensagem forjada para os seus. Como resultado, todas as rotas passantes pelo nó atacante serão desabilitadas.

- **Invasão de rota modificando uma mensagem de RERR recebida:**

Não é possível invadir uma rota com este tipo de ataque.

- **Isolamento de nodo modificando uma mensagem de RERR recebida:**

Se o nó malicioso for o único vizinho do nó atacado, ele pode desabilitar todas as rotas do nó atacado, porém o nodo origem pode se refazer enviando novamente uma mensagem de RREQ.

- **Consumo de recursos modificando uma mensagem de RERR recebida:**

Uma mensagem de RERR falsa pode desabilitar muitas rotas em uma rede *ad hoc*. Com isso todos os nodos afetados terão que enviar novamente uma mensagem de RREQ para o estabelecimento de uma nova rota. Em grande escala isto representa uma tentativa bem sucedida de consumo de recursos.

3.4 Análise de ações com ataques compostos

Como visto nas ações de ataques simples, o efeito do ataque muitas vezes dura apenas por um curto período de tempo. Para que o ataque tenha seu efeito prolongado, se da necessária a repetição do mesmo ataque várias vezes. Assim é caracterizado um ataque composto. Em muitos casos, a eficiência do ataque é melhorada devido à mudança na quantidade de ataques.

A Tabela 4 contém um resumo do que é possível alcançar nas ações de ataques compostos.

Tabela 4: Ataques compostos com o mesmo tipo de mensagem.

Ataque composto	Interrupção de rota	Invasão de rota	Isolamento de nodo	Consumo de recursos
RREQ_DR	Sim (às vezes)	Não	Não	Não
RREQ_MF	Sim	Sim	Parcialmente	Sim
RREQ_AF	Sim	Sim	Parcialmente	Sim
RREP_DR	Sim (às vezes)	Não	Não	Não
RREP_MF	Sim	Sim	Não	Sim
RREP_FR	Sim	Sim	Parcialmente	Não
RREP_AF	Sim	Sim	Parcialmente	Sim
RERR_DR	Sim (às vezes)	Não	Não	Não
RERR_MF	Sim	Não	Não	Sim
RERR_AF	Sim	Não	Não	Sim

3.4.1 Ataques com mensagens de RREQ

- **Interrupção de rota usando descarte de mensagens RREQ:**

Neste caso, o ataque só torna se possível se o nodo atacante for a única conexão entre o nó origem e o nó destino. O efeito deste ataque perdura por um determinado período de tempo, mais precisamente até que a origem mande nova mensagem de RREQ para estabelecimento de rota. No caso do atacante ser o único entre as extremidades, este ataque terá sucesso, pois todas as mensagens geradas serão descartadas pelo atacante e nenhuma mensagem de RREP será gerada.

- **Interrupção de rota modificando mensagens de RREQ recebidas:**

No caso de haver mais de um caminho para a mensagem de RREQ chegar ao seu destino, o nodo atacante pode usar um ataque de RREQ_MF_RD para interromper a rede.

Neste caso, o nó destino pode receber várias mensagens de RREQ por diferentes meios, sem passar pelo atacante, porém uma vez que o atacante receber uma mensagem de RREQ, ele a modificará da forma com mostrado nos ataques simples e a enviará para o destino que suprirá todas as outras mensagens recebidas devido ao maior número de seqüência contido na

mensagem. Para que o ataque tenha efeito, o nodo de ataque deve estar no raio de ação do nó de origem.

- **Invasão de rota modificando mensagens de RREQ recebidas:**

O nodo de ataque deve estar no raio de transmissão do nodo vítima para que o ataque possa acontecer. Quando uma rota estiver quebrada, o nodo origem envia uma mensagem de RREQ para estabelecer a rota novamente. O atacante então ataca a rede modificando a mensagem recebida e consegue invadir a rota.

- **Isolamento de nodo modificando mensagens de RREQ recebidas:**

Este tipo de ataque impede que o nó vítima receba pacotes de dados de outros nodos por um longo período de tempo. Em um ataque simples desta natureza, o atacante troca o endereço de IP no cabeçalho IP por um endereço não existente, com isso o nodo subseqüente do local onde ocorreu a quebra de rota acionará o processo de reparo de rota para o nodo origem. Assim, o nodo que iniciou o processo de reparo irá guardar os pacotes de dados recebidos por um período de tempo (30 segundos no CMU), para que possam ser encaminhados para o nó origem posteriormente.

Nas simulações o nodo atacante faz com que outro nó envie dados para a origem através dele mesmo que descarta tais mensagens, isolando o nodo de origem de receber pacotes de dados.

- **Consumo de recursos modificando mensagens de RREQ recebidas:**

Quando o nodo atacante recebe uma mensagem de RREQ, ele incrementa o número de RREQ ID para fazer a mensagem parecer nova, e então a envia para seus vizinhos. O nodo irá descartar a mensagem se o campo TTL no cabeçalho de IP chegar a 0, para que os vizinhos aceitem a mensagem e a passem adiante, o atacante precisa incrementar o valor TTL para o valor máximo. Cada vez que o atacante receber a mensagem de RREQ dos seus vizinhos, ele repetira a mesma ação. Com isso o consumo de banda da rede aumentará drasticamente.

- **Interrupção de rota fabricando mensagens de RREQ:**

Para que o efeito deste ataque se torne persistente, é necessário que vários ataques simples desta natureza ocorram. Nas simulações, o atacante envia mensagens de RREQ em uma freqüência de 20 pacotes por segundo para interromper uma rota.

- **Invasão de rota fabricando mensagens de RREQ:**

Supondo o cenário da Figura 8(a), onde existem outros nodos entre a origem e o destino. Considerando o nodo 2 como sendo o atacante e os outros nodos normais. Existe uma rota de 0 para 1 através de 3, 4 e 5. O atacante inicia o ataque enviando uma mensagem de RREQ com as seguintes configurações:

1. O endereço de IP da origem é o nodo 1;
2. O endereço de IP do destino é o nodo 0;
3. O número de seqüência de origem é maior que o número de seqüência atual do nodo 1;
4. O número de seqüência de destino é maior que o número de seqüência atual do nodo 0; e
5. O endereço de IP da origem no cabeçalho IP é o nodo 2.

Quando os nodos 3 e 4 recebem a mensagem forjada, ambos atualizam seus próximos saltos para o destino como sendo o nodo 2, como mostra a Figura 8(b). Assim o nodo atacante consegue a rota para o destino. Agora, para estabilizar a rota de 2 para 1 e evitar um *loop* entre 2 e 4, o atacante gera uma segunda mensagem de RREQ como segue:

1. O endereço de IP da origem é o nodo 2;
2. O endereço de IP do destino é o nodo 1;
3. O número de seqüência de origem é o número de seqüência atual do nodo 2;
4. O número de seqüência de destino é maior que o número de seqüência atual do nodo 1; e
5. O endereço de IP da origem no cabeçalho IP é o nodo 2.

Assim, quando o nodo 4 receber a mensagem, ele irá reenviá-la para o nodo 1. O nodo 1 gera uma mensagem de RREP que irá se encaminhar para o nodo 2 e assim o atacante forma uma rota para o nodo 1 (Figura 8(c)).

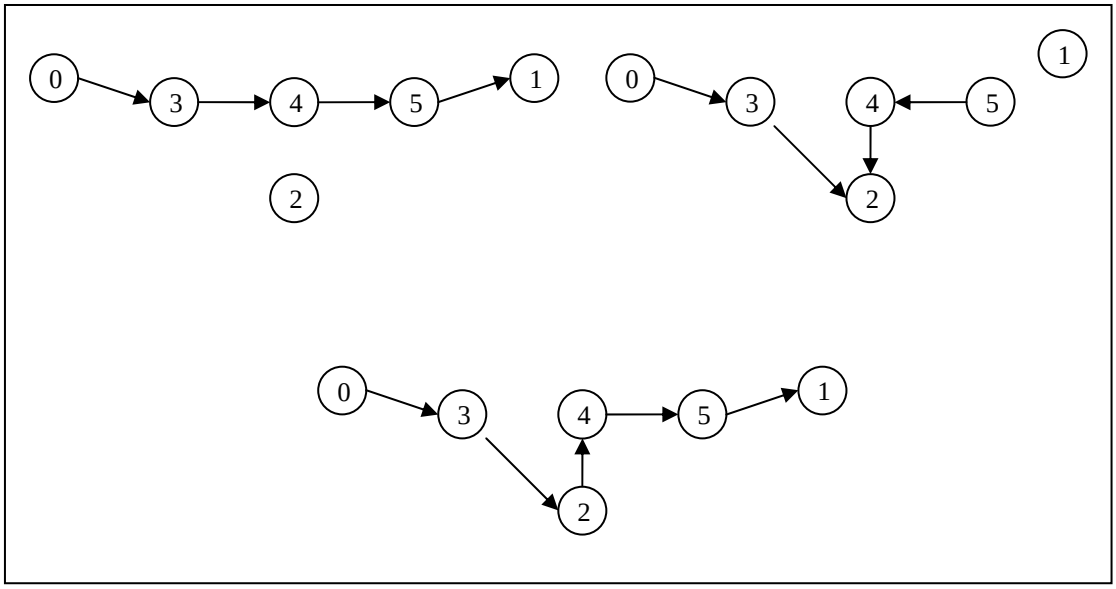

Figura 8: Cenário simulando um ataque de invasão de rota.

- **Isolamento de nodo fabricando mensagens de RREQ:**

Em um ataque simples deste tipo, o ataque é capaz de isolar um nodo por um curto período de tempo. Porém é capaz de isolar um nodo por um longo período se repetir à mensagem forjada de RREQ várias vezes. Na mensagem forjada, o atacante pode colocar o endereço IP da origem como um endereço não existente. Para que as mensagens não cheguem ao nodo vítima, o atacante usa seu próprio endereço de IP como IP de origem no cabeçalho IP. Assim que ele receber os pacotes de dados enviados, o atacante simplesmente os descarta e evita que o nodo vítima receba pacotes. Nas simulações realizadas o atacante envia 10 mensagens forjadas de RREQ por segundo.

- **Consumo de recursos fabricando mensagens de RREQ:**

O atacante consome banda da rede ao fabricar e enviar várias mensagens de RREQ. Nas simulações realizadas, o atacante envia 20 mensagens forjadas por segundo.

3.4.2 Ataques com mensagens de RREP

- **Interrupção de rota modificando mensagens de RREQ recebidas:**

Quando um nodo envia uma mensagem de RREQ para estabelecer uma nova rota, ele pode receber como resposta várias mensagens de RREP. No protocolo AODV, nodos intermediários podem responder a uma RREQ se tiverem uma rota atualizada para o destino. Para interromper a rota, o atacante altera o número de seqüência das mensagens de RREP recebidas e coloca o endereço de IP da origem com endereço não existente.

- **Interrupção de rota modificando mensagens de RREQ recebidas:**

Para anular o efeito de outras mensagens RREP recebidas pelo nó origem, em resposta a uma RREQ, o atacante coloca um número de seqüência de destino pequeno na mensagem, assim, o nó origem escolherá a rota que passa pelo nó atacante para enviar pacotes de dados. Aplicando este ataque várias vezes, um nodo consegue invadir várias rotas diferentes.

- **Invasão de rota forjando respostas com mensagens RREP:**

Devido à mobilidade dos nós em uma rede *ad hoc*, uma rota entre dois nodos pode ser interrompida após algum tempo, com isso, o nodo origem enviará nova mensagem de RREQ. Aplicando o ataque simples desta natureza várias vezes, o atacante conseguirá invadir a rota.

- **Interrupção de rota fabricando mensagens de RREP:**

Uma rota quebrada por um ataque simples desta natureza, pode ser restabelecido rapidamente. Porém o ataque repedido toda vez que a rota se estabelece, pode garantir a ruptura da rota por um longo período de tempo. Para garantir que o nodo vítima receba as mensagens forjadas, o atacante deve estar sempre ao alcance da vítima.

- **Invasão de rota fabricando mensagens de RREP:**

O atacante pode invadir muitas rotas aplicando vários ataques simples deste tipo.

- **Isolamento de nodo fabricando mensagens de RREP:**

Desde que o atacante esteja no raio de alcance da vitima, ele será capaz de garantir que outros nodos da rede não recebam dados da vitima, apenas enviando mensagens de RREP forjadas para a vítima. Para isso, o atacante faz

com que outros nodos vizinhos da vítima, enviem mensagens RREP forjadas, com as seguintes características:

1. O endereço de IP do destino é o endereço de outro nodo da rede;
2. O endereço de IP da origem é o endereço de outro nodo da rede;
3. Incrementa o número de seqüência do destino em pelo menos um; e
4. O endereço de IP da origem no cabeçalho IP da mensagem é o endereço IP do atacante.

O atacante simplesmente descarta as mensagens que passa a receber da vítima. Na simulação, o atacante envia 4 mensagens de RREP por segundo.

É muito difícil para o atacante isolar um nodo forjando mensagens de RREP, pois elas são enviadas via *unicast* para a vítima, que pode não ter a rota para o destino descrito na mensagem forjada.

- **Consumição de recursos fabricando mensagens de RREP:**

Quando aplicado um ataque simples deste tipo, ou seja, enviando apenas uma mensagem forjada, o atacante consegue formar um *loop* entre dois nodos da rede. Quando o ataque passa a ser composto, o atacante tem a capacidade de formar um *loop* envolvendo outros nodos da rede. Na Figura 9, o atacante (2) envia a primeira mensagem forjada para o nodo 5 com as seguintes características:

1. O número de IP da origem é o nodo 0;
2. O número de IP do destino é o nodo 1;
3. O número de seqüência do destino é um número maior que o número de seqüência no nodo 1;
4. O número de IP da origem no cabeçalho de IP é o nodo 3; e
5. O número de IP da origem no cabeçalho de IP é o nodo 5.

Após o nodo 5 receber a mensagem, ele atualiza seu próximo salto para o nodo 1, como sendo o nodo 3. Então o atacante envia uma segunda mensagem forjada, desta vez para o nodo 6, com as seguintes características:

1 O número de IP da origem é o nodo 0;

2 O número de IP do destino é o nodo 1;

3 O número de seqüência do destino é um número maior que o número de seqüência no nodo 1;

4 O número de IP da origem no cabeçalho de IP é o nodo 5; e

5 O número de IP da origem no cabeçalho de IP é o nodo 6.

O nodo 6 então atualiza seu próximo salto para o destino, como sendo o nodo 5. O resultado disto é um *loop* envolvendo os nodos 3, 4, 5 e 6 , como mostra a Figura 9(d).

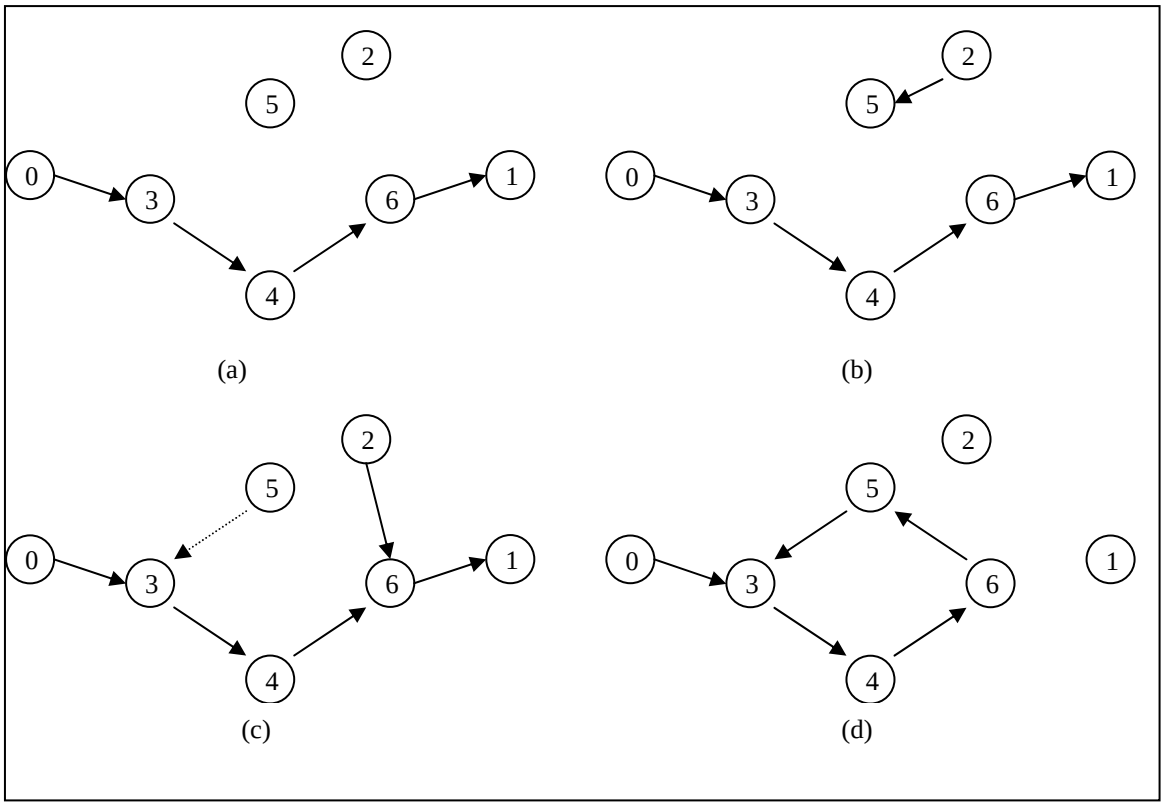

Figura 9: Cenário simulando um ataque composto para formação de *loop* entre 4 nodos.

A Tabela 5 mostra como fica a energia dos nodos envolvidos no *loop* formado pelo ataque em comparação com um cenário onde ocorre roteamento de pacotes feito de forma normal.

Tabela 5: Comparativo de consumo de energia em um cenário normal e um cenário de ataque.

Nodo	Energia inicial (Watt)	Energia Final Normal (Watt)	Energia Final No *Loop* (Watt)

Nodo3	100.00	98.9133	91.8482
Nodo4	100.00	98.9119	91.9932
Nodo5	100.00	99.9580	92.0660
Nodo6	100.00	98.9121	92.0630

3.4.3 Ataques com mensagens de RERR

- **Interrupção de rota fabricando mensagens de RERR:**

O atacante pode desabilitar todas as rotas do nodo vítima, enviando várias mensagens forjadas de RERR para a vítima, desde que esta esteja no raio de ação do atacante. O atacante faz com que cada vizinho envie mensagens de RERR para o nó vítima, assim, se o nodo tiver outras rotas e que não passam pelo atacante, todas serão desabilitadas.

4 Resultados

Nesta seção são apresentados as análises sobre os dados obtidos com a simulação dos ataques descritos anteriormente, através do uso do simulador *Network Simulator.*

Como já foi dito, as simulações geram arquivos que registram cada movimento da rede e cada propriedade dos pacotes e mensagens movimentadas. Tais arquivos são chamados de *trace files*, e neste trabalho é usado o formato de arquivo *cmu-trace*.

Os arquivos foram analisados através de um algoritmo próprio, desenvolvido de acordo com as necessidades deste trabalho. Através do algoritmo foi-se capaz de extrair informações relevantes para cada tipo de ataque, e então, tinha-se a base para a construção dos gráficos.

A seguir é descrito um exemplo de registro feito nos arquivos *trace* do trabalho de acordo com o formato *cmu-trace*:

f[1] 1.093796178[2] _5_[3] RTR --- 13 cbr[4] 220[5] [13a 5 9 800] ------- [1:0 6:0 28 6][6] [2][7]

Onde:

1. Refere-se ao tipo do evento, podendo variar entre:

   M: *movement*;

   s: *sent*;

   r: *received*

   f: *forwarded*

   D: *dropped*
2. Tempo em segundos da ocorrência do evento.
3. Nodo gerador do evento.
4. Tipo de pacote, neste caso *constant bit rate.*
5. O tamanho do pacote.
6. Cabeçalho de IP.

7. Número de seqüência.

4.1 Análises

A seguir encontram-se as representações em forma de gráficos dos ataques simulados em mensagens RREQ e mensagens RREP.

4.1.1 Mensagens *Route Request*:

- **Isolamento de nodo fabricando uma mensagem de RREQ:**

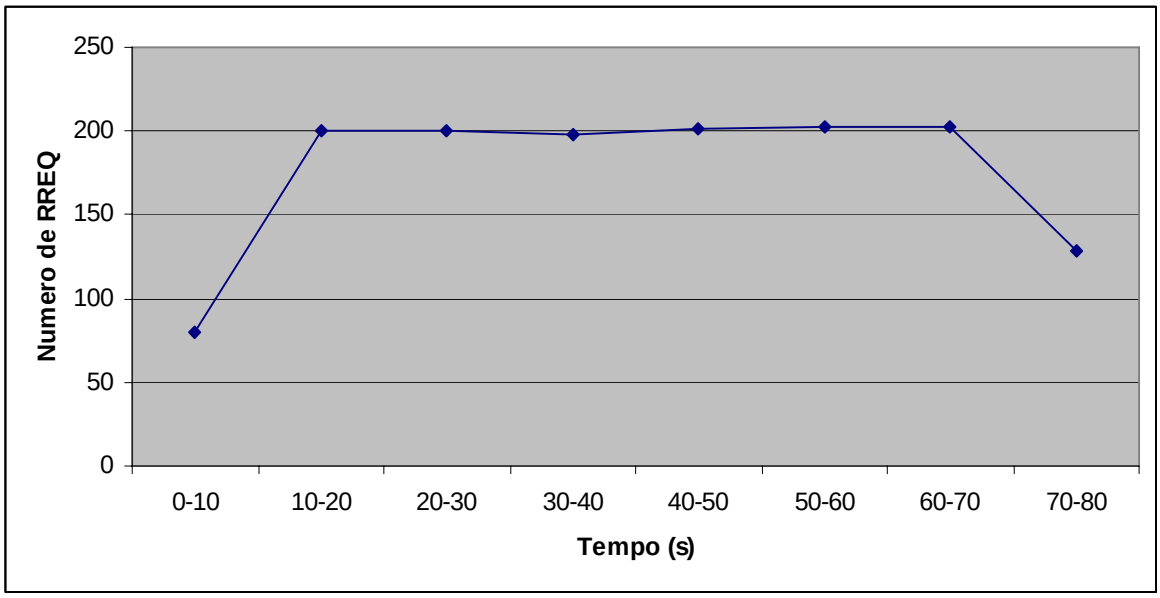

Gráfico 1: Quantidade de RREQ enviadas pelo atacante.

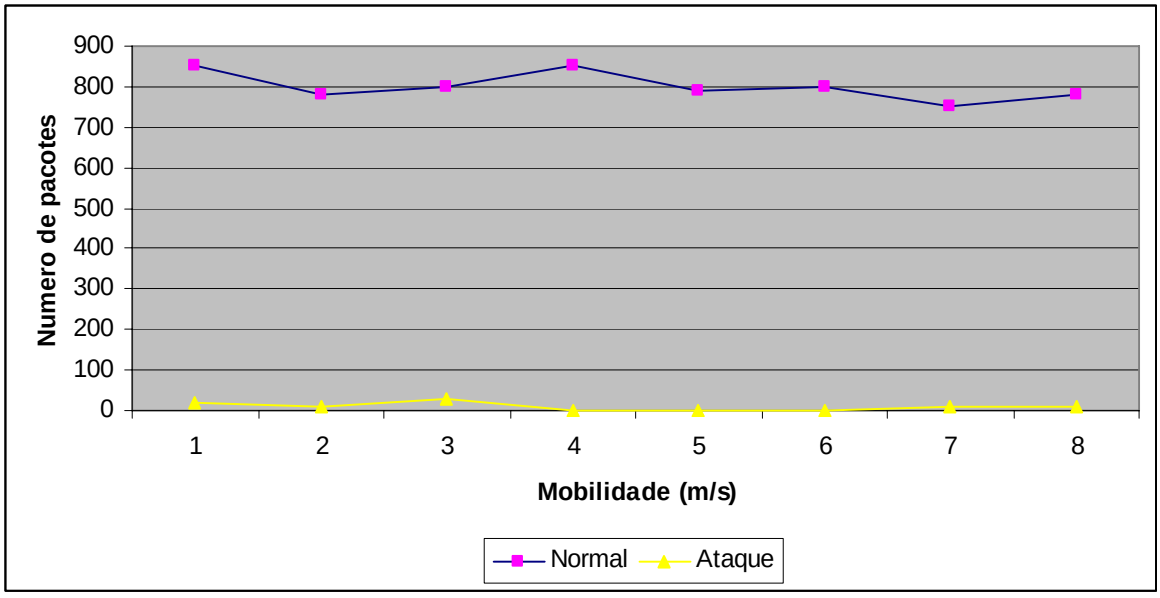

Gráfico 2: Quantidade de pacotes recebidos pela vitima[13].

Ao se olhar para o Gráfico 1, tem-se a nítida visão da estratégia adotada pelo nodo malicioso. Há uma constante demanda no envio de mensagens de RREQ, o que é uma evidente pista de ataque envolvendo mensagens RREQ. Observando então o Gráfico 2, pode-se notar como um ataque de isolamento deste tipo pode ser eficiente, pois deixa em praticamente em zero a atividade do nodo vítima.

Embora o nodo tenha se isolado da rede, esta ação depende muito da constância do ataque, pois um nodo, embora isolado, não esta inativo, e por este motivo pode muito bem formar outras rotas com outras requisições, que acontecem depois de um determinado tempo. Por isso o nodo atacante deve sempre repetir o ataque, para que seu efeito permaneça. Ataques compostos são os mais indicados para este objetivo.

- **Interrupção de rota com mensagens RREQ:**

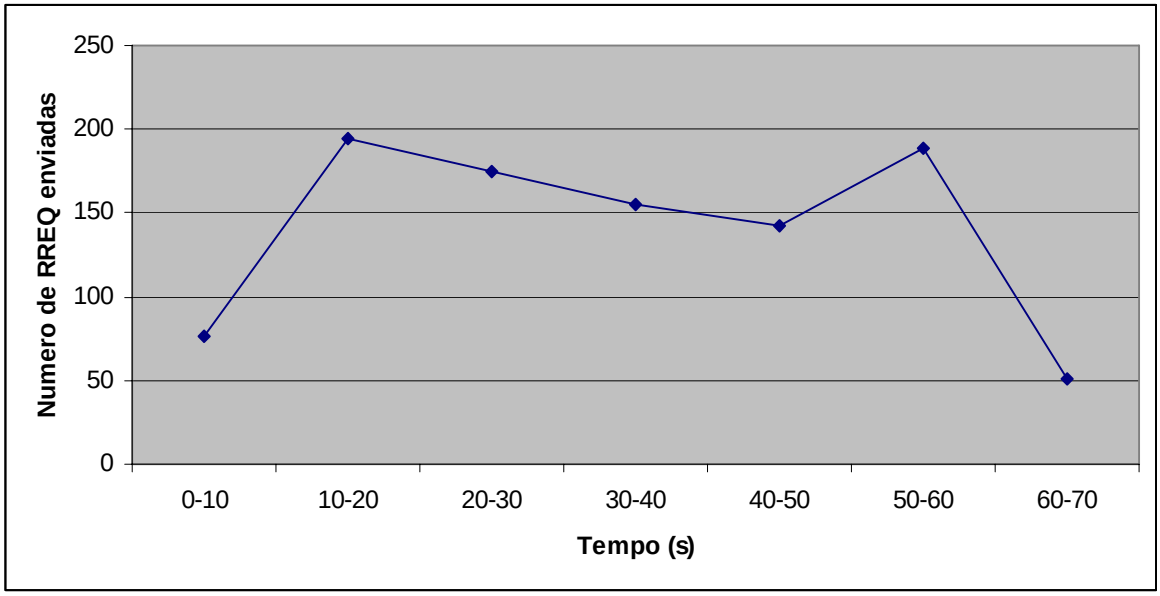

Gráfico 3: Quantidade de mensagens RREQ enviadas pelo atacante.

O Gráfico 3 mostra o atacante efetivando seu ataque através do envio constante de mensagens forjadas ao longo do tempo, o resultado desta ação podemos ver no Gráfico 4.

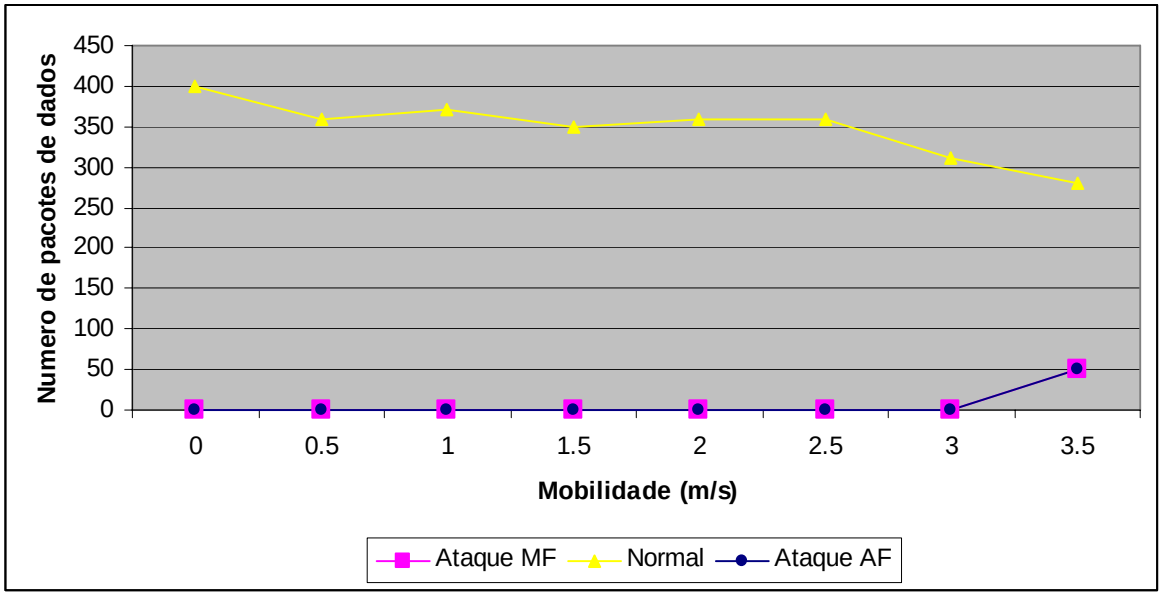

Gráfico 4: Quantidade de pacotes de dados recebidos pela vitima – Ataque com RREQ [13].

Ataques para interrupção de rota através de mensagens RREQ se mostram bastante eficientes na simulação. De acordo com os resultados obtidos em [13] e confirmados neste trabalho, quando um ataque deste tipo é aplicado a atividade da rota quebrada fica zerada e o resultado é o mesmo aplicando ataques de AF ou ataques de MF.

- **Consumo de recursos:**

A análise do Gráfico 5 é completada quando se verifica a Tabela 5, que mostra claramente o efeito deste ataque em cima de cada nodo em separado. No gráfico podemos ver o impacto do ataque sobre toda rede.

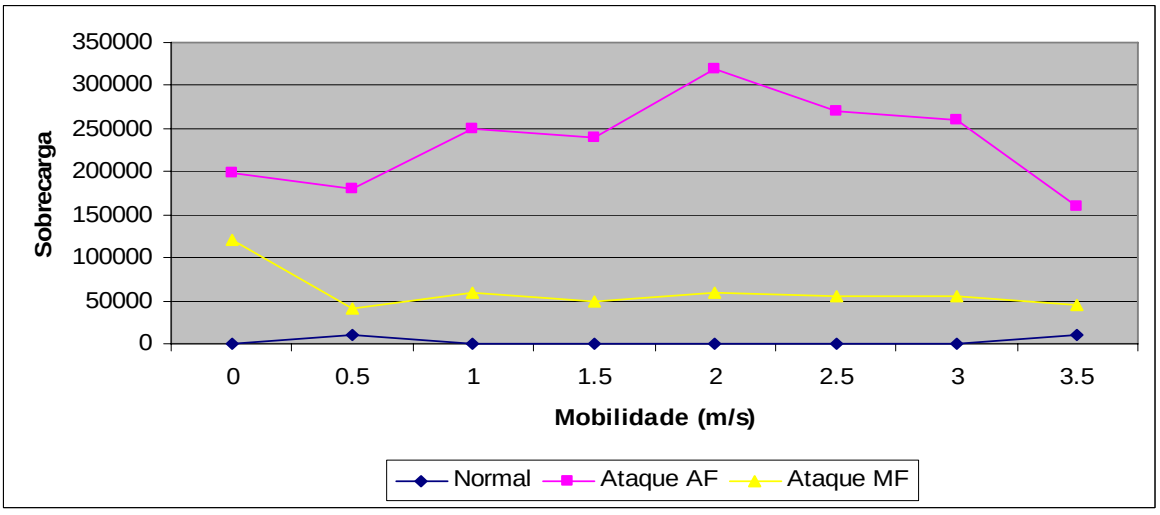

Gráfico 5: sobrecarga na capacidade de roteamento.

Pode-se notar, também no Gráfico 5, que um ataque AF tem maior eficiência que um ataque MF. Isso se deve ao fato de que em ataques AF as mensagens são fabricadas pelo atacante de uma maneira constante, diferente dos ataques MF onde o atacante precisa receber uma mensagem enviada por outro nodo, para então modificá-la e repassá-la, ou seja, para o ataque se efetivar, o atacante depende de outros nós da rede.

É importante citar que para um eficiente ataque de consumo de recursos, o atacante ao utilizar o tipo de mensagem RREQ, utiliza-se de uma característica de envio desta mensagem, que é o envio *broadcast,* estratégia de ataque que não poderia ser usada em um ataque com mensagens de RREP, por exemplo, que é enviada *unicast*.

4.1.2 Mensagens de *Route Reply*

- **Isolamento de nodo forjando uma mensagem de RREP:**

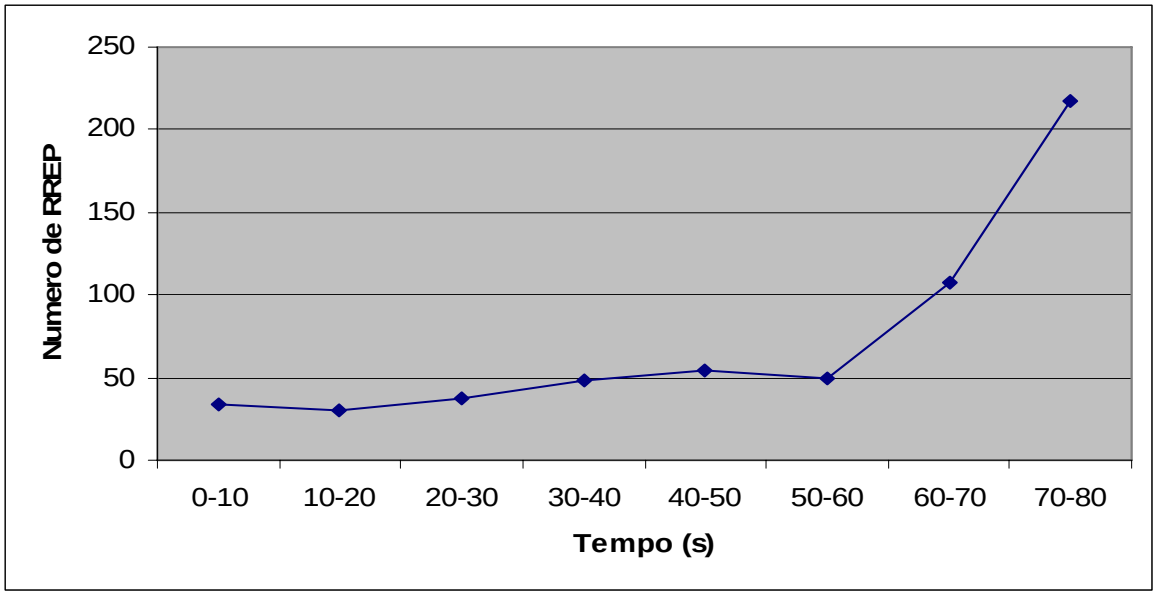

Gráfico 6: Quantidade de mensagens RREP recebidas pelo nodo vitima.

De acordo com o Gráfico 6, o número de mensagens RREP recebidas pelo nodo vítima aumenta muito em pouco tempo. Isso mostra que o atacante obteve sucesso ao induzir seus vizinhos a enviarem mensagens forjadas de RREP para a vítima conforme 3.3.1. Neste gráfico estão representados dois cenários, em um primeiro momento em condições normais de funcionamento e, logo após, com a ação do atacante.

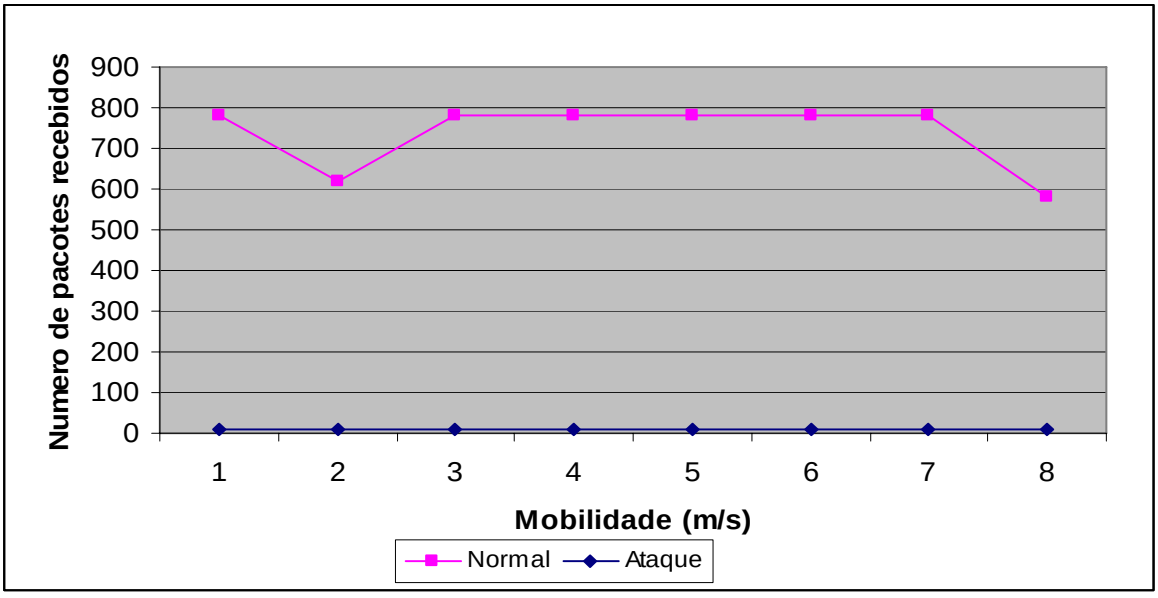

Gráfico 7: Quantidade de pacotes de dados recebidos pela vitima[13]

O ataque de isolação de nodo se mostra muito eficiente com mensagens RREP, o mesmo fato observado com mensagens de RREQ. Relembrando que há uma diferença entre o modo de ação dos ataques com RREP e RREQ, sendo que o primeiro tipo é repassado pela rede de maneira *unicast,* o que por um momento poderia sugerir uma menor eficiência do ataque, o que não se mostra real.

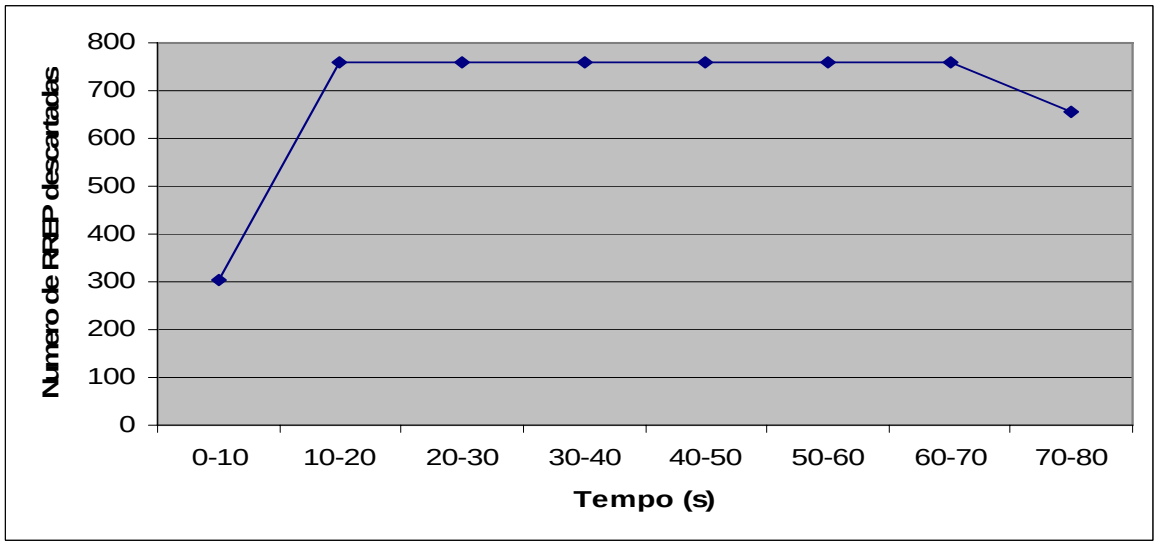

Gráfico 8: Quantidade de mensagens RREP descartadas pelo atacante.

Quando se analisa os gráficos 7 e 8 em conjunto, pode-se observar a relação existente entre a quantidade de pacotes recebidos pela vítima, com a quantidade de pacotes descartados pelo atacante. No Gráfico 7, observando a linha que representa a condição de ataque, nota-se que a vítima praticamente

não recebe pacotes de dados, enquanto que no Gráfico 8 há uma alta taxa de descarte de pacotes pelo atacante. Quando a linha que representa condições normais é analisada, nota-se que é praticamente o mesmo número de pacotes que o atacante descarta em condições de ataque. O Gráfico 7 é retirado de [13] e confirma os dados obtidos nas análises.

- **Interrupção de rota com mensagens RREP:**

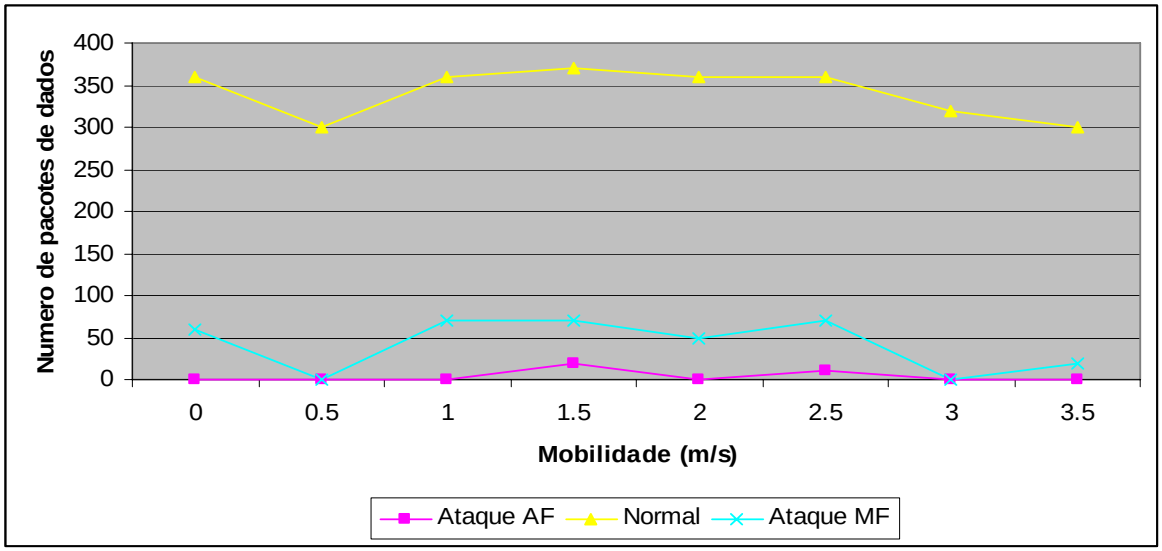

Gráfico 9: Quantidade de pacotes de dados recebidos pela vítima – Ataque com RREP [13].

A mesma eficiência de interrupção de rota observada no Gráfico 4 pode ser observada no ataque com mensagens de RREP, porém, com uma pequena perda de desempenho no ataque. Isso se deve ao fato de que mensagens RREP são enviadas via *unicast* pela rede enquanto mensagens RREQ são enviadas via *broadcast*.

- **Invasão de rota fabricando uma mensagem de RREP:**

Fica nítida a invasão da rota quando se analisa o Gráfico 10. O gráfico mostra que o nodo atacante pode entrar em uma rota de dados já estabelecida, e com aceso a 100% dos dados que transitam pela rota. Isso esta claro ao se analisar no Gráfico 10, a linha que mostra o ataque com a linha que mostra o total de pacotes transmitidos pela rota, as linhas andam coincidentes pelo gráfico.

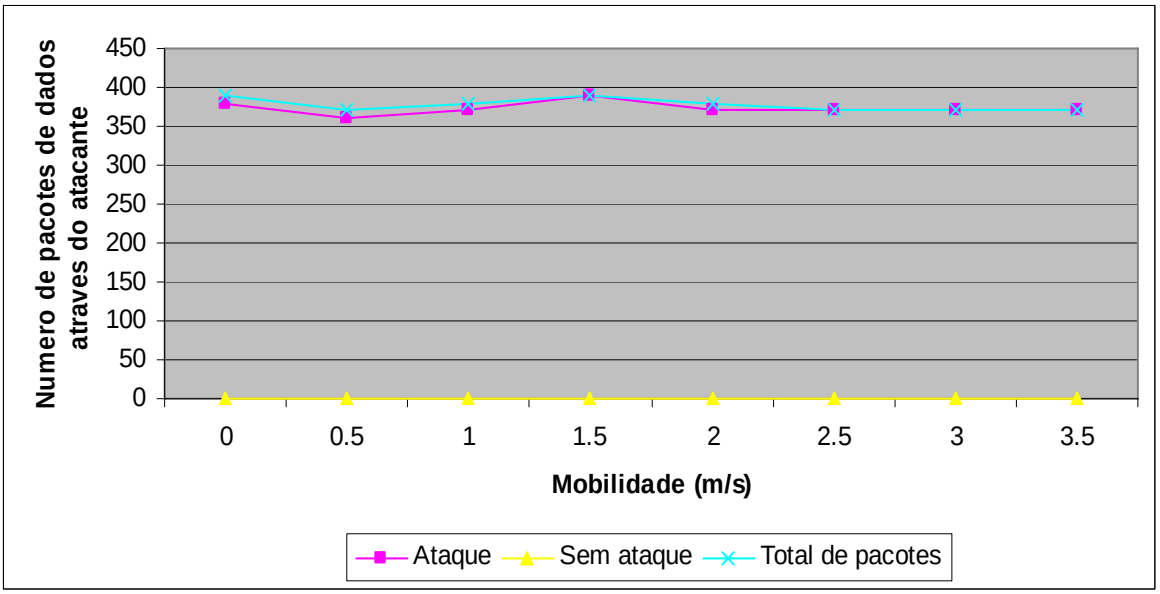

Gráfico 10: Comparativo da quantidade de pacote de dados que passam através do atacante antes e depois do ataque [13].

Ao entrar na rota, o nodo atacante não encontra nenhum empecilho por parte dos outros nodos que já compunham a rota e todo o tráfego de dados começa a passar pelo atacante.

5 Conclusão

Fica claro ao se ver com estatísticas e simulações, que a segurança de uma rede *ad hoc* é um ponto delicado que merece muito estudo e observação.

Apesar de toda tecnologia hoje existente dando suporte a segurança computacional, como os excelentes avanços que se tem feito na área de criptografia, técnicas de detecção de intrusão e sistemas de proteção avançados, ainda assim nada é suficiente para garantir a segurança e integridade dos dados de uma rede sem fio. Viu se que fatores peculiares a tais redes derrubam um a um os processos de segurança hoje existentes em qualquer ambiente computacional. Como no caso de algoritmos poderosos de criptografia que simplesmente não são aplicáveis em redes *ad hoc* devido ao fato de os nodos que compõe a rede não terem capacidade de energia ou processamento o suficiente para suportá-los.

O estudo feito, além de analisar teoricamente os pontos de vulnerabilidade do protocolo AODV, tem como complemento as simulações feitas que se aproximam muito dos resultados reais de funcionamento da rede.

Foi possível observar que esforços estão sendo feitos e idéias não faltam para que o problema da segurança seja resolvido.

Muitos subsídios de informação e de ferramentas estão disponíveis para quem deseja se aprofundar no assunto e possivelmente contribuir para a solução de problemas. O *Network Simulator* se mostrou uma ferramenta muito completa no estudo e suporte de vários ambientes e possibilitou a reprodução perfeita de cenários onde se da à comunicação entre nodos da rede e principalmente se mostrou uma ferramenta flexível no sentido de inclusão de novas ferramentas e métodos de simulação, uma vez que para este trabalho, foi necessário o uso de extensões de código para o simulador.

Para aprofundar o tema, em trabalhos futuros poderiam ser abordados uma gama maior de ataques, o que completaria o resultado deste trabalho. Assim, posteriormente poderiam se analisar outros protocolos de roteamento existentes, como o DSDV, e assim fazer um trabalho comparativo entre a segurança dos protocolos analisados.

Em um estágio posterior, se deixaria de lado o campo de simulações e passar-se-ia a fazer testes de campo real, com dispositivos atuais e suas limitações, podendo, desta maneira, detectar detalhes que uma simulação, por mais que se aproxime da realidade, não poderia detectar.

6 Referências

[1].Albuquerque, L. R., “Segurança Redes Ad Hoc”, Universidade Federal do Rio de Janeiro, Brasil, 2003.

[2].Amodei, A. e Duarte, O. M. B., “Segurança no roteamento de em Redes Moveis Ad Hoc”, Universidade Federal do Rio de Janeiro, Brasil, 2003.

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

[4].Corson, S., Macker, J., “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, Request For Comments (RFC) 2501, 1999.

[5]. Dahil, B., Sanzgiri, B. N. Levine, Shields, C. e Royer, E., “A secure routing protocol for ad hoc network”. In the Proceedings of the 2002 IEEE International Conference on Network Protocols (INCP 2002), Nov. 2002.

[6].Dantas, M. A. R. Tecnologias de Redes de Comunicação e Computadores. Rio de Janeiro: Axcel Books do Brasil Editora, 2002, 328 p.

[7].D. D. Perkins, H. D. Hughes, C. B. Owen, “Factors Affecting the Performance of Ad Hoc Networks”, in Proceedings of the IEEE International Symposium on Performance Evaluation of Computer and Telecommunication System, San Diego, July 2002.

[8].Guerrero, M. e Asokan, N., “Securing Ad Hoc Routing Protocols”, in the Proceedings of 2002 ACM Workshop on Wireless Security (WiSe 2002), Setembro, 2002.

[9].Heady, R., Luger, A. Maccade, Servilla, M., “The arquiteture of a Network Level Intrusion Detection System”, Technical report, Computer science Department, University of New Mexico, 1990.

[10]. Hu, Y., Perring, A., e Johnson, - Efficient Security Mechanisms for Routing Protocols. IETF NDSS 2003.

[11]. KATZ, R. H. Adaptation and Mobility in Wireless Information Systems. IEEE Personal Communications Magazine, v.1, n. 1, 1994

[12]. Mishra, A. et al., “Intrusion Detection in Wireless Ad Hoc Netwoks”, IEEE wireless communications, 2004, pages 48-60.

[13]. Ning P. e Sun K., “How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols”, Tech. Rep. TR-2003-07, CS Department, NC State University, 2003.

[14]. Ousterhout, John K., “Tcl/Tk Engineering Manual”, 1994, Pagina do projeto, http://tcl.sourceforge.net

[15]. Parcher, J. M., Albers, P., Jouga, B., Me, R., Puttini, R., “Secure in Ad Hoc Networks: a General Intrusion Detection Architeture Enhancing Trust Based Approaches”, The 1st International workshop on Wireless Information Systems (WIS 2002), in the 4rth International Conference on Enterprise Information Systems, 2002.

[16]. Perkins C. Network Working Group,Request for Comments: 3561.Nokia Research Center University of California, Santa Barbara,July 2003 Ad hoc On-Demand Distance Vector (AODV) Routing

[17]. Rocha, L. G., Duarte, C. M. B. Aspectos e Mecanismos de Segurança em Redes Ad Hoc, Workshop em Qualidade de Serviço e Mobilidade - WQoSM 2002, Angra dos Reis, RJ.

[18]. Royer, Elizabeth; Toh, Chai-Keong; “A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks” IEEE Personal Communications 1999, pp. 46–54.

[19]. Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., and Belding-Royer, E. M. (2002). A secure routing protocol for ad hoc networks.

[20]. Stamouli, Ioanna, “Real-Time Intrusion Detection for Ad Hoc Networks”, 2003

[21]. The VINT (Virtual InterNetwork Testbed) Pagina do projeto, http://www.isi.edu/nsnam/vint/index.html

[22]. Vanhala A., “Security in ad hoc networks”, in Research Seminar on Security in Distributed Systems, 2000.

[23]. Zhang e W. Lee. Intrusion Detection in Wireless Ad Hoc Networks. MobiCom`2000, Agosto, 2000.

[24]. Wang,W. and Bhargava, B. (2002). On vulnerability and protection of ad hoc on-demand distance vector protocol. Technical report, Technical report, TR-2002-18, CERIAS Security Research Center, Purdue University.

[25]. Wang, W., Lu, Y., and Bhargava, B. (2002). On security study of two distance-vector routing protocols for mobile ad hoc networks. Technical report, Technical report, Dept. of Computer Sciences, Purdue University.

[26]. Yang, H. et al., “Security in Mobile Ad Hoc Netwoks: Challenges and solutions”, IEEE wireless communications, 2004, pages 38-47.

Anexos – A: Artigo

SIMULAÇÃO DE ATAQUES AO PROTOCOLO DE ROTEAMENTO AODV

Günter Heinrich Herweg Filho
Curso de Bacharelado em Ciências da Computação
Departamento de Informática e Estatística
Universidade Federal de Santa Catarina (UFSC), Brasil, 88040-900
gunter@inf.ufsc.br

RESUMO

As redes sem fio figuram um papel de destaque quando se fala de tecnologias para o futuro, porém pouco aproveitadas, e o maior fator para este pouco aproveitamento é sem dúvida a fraca segurança de uma rede ad hoc.

Este trabalho visa contribuir com o estudo da melhoria dos protocolos de roteamento para as redes sem fio, mais especificamente do protocolo AODV. São simulados vários cenários de ataque à rede e analisadas as conseqüências de tais ataques através de gráficos comparativos.

Palavras – chave: *ad hoc, redes sem fio, AODV, protocolos de roteamento.*

ABSTRACT

The wireless networks appear a prominence paper when it is said of technologies for the future, however little used to advantage, and the biggest factor for this little exploitation is without a doubt the weak security of a ad hoc networks.

This work aims at to contribute with the study of the improvement of the ad hoc routing protocols, more specifically the AODV protocol. Some attack scenarios are simulated and analyzed the consequences of such attacks through comparative graphs.

Keywords: *ad hoc, wireless networks, AODV, routing protocols, security.*

Introdução

Observando o grande crescimento nas áreas de comunicação celular, redes locais sem-fio e serviços via satélite juntamente com o comércio de dispositivos que utilizam tais serviços, estima-se que em poucos anos, dezenas de milhões de pessoas terão um *laptop*, *palmtop* ou algum tipo de PDA (*Personal Digital Assistants*). Este crescimento permitirá, em um futuro bem próximo, que informações e recursos possam ser acessados a qualquer instante e em qualquer lugar.

Este tipo de ambiente onde os usuários podem realizar comunicações sem-fio para acessar recursos distribuídos faz parte da linha de pesquisa de Redes Móveis sem-fio. Basicamente, existem dois tipos de Redes Móveis sem-fio: as redes *ad hoc* e as redes infra-estruturadas. É abordado nesta pesquisa o tipo de rede *ad hoc*.

Neste contexto tecnológico e móvel, em que a Ciência da Computação e as telecomunicações se relacionam as redes *ad hoc* ganham força. Entre as características destas redes que contribuem para tal, destaca-se: (i) Fácil instalação; por não serem dependentes de infra-estrutura fixa. (ii) Apresentam maior conectividade, uma vez que a comunicação pode ser direta, ou seja, não é obrigada a passar pela infra-estrutura; (iii) Além da mobilidade, seu fator de maior sucesso.

É justamente o fator de maior importância neste contexto , é também o mais delicado e difícil de ser resolvido. Por estes motivos são apresentados neste trabalho, onde veremos o como e o por que é tão fácil manipular, desviar ou roubar informações de uma rede *ad hoc.* São abordados em detalhes os pontos críticos do protocolo de roteamento de informações que será atacado no intuito de provar a existência de graves falhas de segurança no protocolo analisado.

Questões de segurança em Redes Ad-hoc

Estabelecer uma rede segura e ao mesmo tempo robusta e eficiente é o principal desafio a ser alcançado em qualquer tipo de rede. O que torna essa questão

ainda mais desafiadora na rede *ad hoc*, é o fato de essa rede possuir características peculiares como: uma arquitetura aberta e topologia dinâmica, como já mencionado.

Para que a rede torne-se confiável, ela deve possuir um modelo de segurança completo, o qual deve considerar todos os principais aspectos na área da segurança, que são *prevenção*, *detecção e reação*. Cada um de seus nodos deve estar preparado para enfrentar um adversário (nó malicioso), garantindo indiretamente maior grau de segurança para toda a rede [1].

Além disso, precisam prover serviços seguros como *autenticação*, *confidencialidade*, *integridade*, *anonimato* para usuários móveis, e tudo isso, é claro, sem perder aspectos de eficiência de roteamento.

Embora um modelo de segurança completo necessite prever o ataque, detectá-lo e conseguir tratá-lo, os protocolos que buscam o foco em maior segurança, se atêm em apenas uma das questões anteriores. E por isso há hoje basicamente dois meios de proteger uma rede *ad hoc*: pró-ativa e reativa. A maneira pró-ativa tenta frustrar o ataque antes que ele aconteça, geralmente através de técnicas de criptografia, em contrapartida, a maneira reativa busca detectar o ataque e reagir de acordo.

Protocolo de roteamento AODV

O protocolo AODV faz parte da família de protocolos reativos e foi projetado para o uso em redes *ad hoc* que podem possuir até milhares de nós móveis. É implementado de forma a evitar o desperdício de banda e minimizar o uso de memória e processamento nos nodos que atuam como roteadores, uma vez que se trata de um protocolo reativo e não necessita ter a rota previamente conhecida. É capaz de manter rotas unidirecionais e multidirecionais. Também provê um rápido mecanismo de detecção de rotas inválidas através do uso de mensagens de mensagens de erro.

Quando um nodo deseja enviar uma mensagem para algum outro nodo (nodo destino), e não possui a rota para tal, é iniciado um processo de descoberta da rota, da

origem até o destino. Tal processo também é iniciado se a rota armazenada for inválida ou em desuso.

O processo inicia com a transmissão de uma mensagem de *route request* (RREQ) para seus vizinhos, que por sua vez enviam o sinal via *broadcast* até que a RREQ chegue a um nodo que conheça a rota para o destino ou para o próprio nodo destino (processo de difusão da mensagem).

O nodo destino ou um nodo intermediário que possua uma rota para o destino, envia uma mensagem de *route reply* (RREP) de volta para o nodo de origem assim que este receber a mensagem de RREQ. À medida que a mensagem trafega de volta para a origem, os nodos intermediários atualizam seus ponteiros em direção ao destino e assim que a mensagem chega à origem, está estabelecida a rota, e todos os nodos estão aptos a transmitir pacotes de conteúdo pelo caminho estabelecido.

Tal rota é mantida enquanto ela permanecer ativa, isto é, enquanto houver tráfego passando pela rota periodicamente. Caso o tempo de vida da rota terminar, ela é removida da tabela de roteamento por algum nodo intermediário. Caso o nodo origem desejar enviar informações pela rota após o seu rompimento, uma mensagem de RERR é envida ao emissor, que terá de reiniciar o processo de descoberta de rota.

A simulação

A simulação está baseada no artigo: Ning P. e Sun K., "*How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols*" [13], e visa analisar caso a caso os ataques que ocorrem em determinados cenários de uma rede *ad hoc*, conforme descrito em [13]. Após uma análise detalhada dos tipos de ataque, far-se-á o uso do simulador *Network Simulator 2* [21], para comprovar via simulação os efeitos dos ataques.

Metodologia de análise da simulação

Nesta abordagem primeiramente foram definidos alguns dos objetivos que um atacante de rede *ad hoc* deseja alcançar, para posteriormente

serem analisados nos testes, são eles:

- **Interrupção de rota:** Visa à quebra de uma rota já estabelecida entre nodos da rede ou mesmo a inviabilidade que uma nova rota seja formada.
- **Invasão de rota:** Significa que o atacante insere-se dentro de uma rota e passa a fazer parte do caminho de dados.
- **Isolamento de Nodo:** Faz com que o nodo atacado cesse a comunicação com o resto da rede, tornando-o isolado.
- **Consumo de recursos:** O nodo invasor faz com que seja consumida toda a banda de rede disponível formando um ciclo entre nodos, por exemplo, ou esgotando qualquer outro recurso necessário para o bom funcionamento da rede.

Também foram definidas quais ações que são tomadas pelo atacante para alcançar o seu objetivo:

- **Descarte de mensagem:** Onde um nodo invasor descarta a mensagem que recebe uma RREQ, por exemplo, ação muito utilizada se o objetivo for o de isolar um nodo.
- **Modificação e repasse:** O nodo invasor ao receber uma mensagem de qualquer tipo, a altera e depois a repassa normalmente, manipulando, assim, o fluxo normal da mensagem.
- **Resposta falsa:** O atacante forja uma mensagem em resposta a uma mensagem recebida e a envia.
- **Fabricação Ativa:** O atacante simplesmente fabrica e envia uma mensagem falsa.

Resultados

A seguir encontram-se as representações em forma de gráficos de alguns dos ataques simulados em mensagens RREQ e mensagens RREP.

Mensagens *Route Request*: Isolamento de nodo fabricando uma mensagem de RREQ:

Ao se olhar para o Gráfico 1, tem-se a nítida visão da estratégia adotada pelo nodo malicioso. Há uma constante demanda no envio de mensagens de RREQ, o que é uma evidente pista de ataque envolvendo mensagens RREQ. Observando então o Gráfico 2,

pode-se notar como um ataque de isolamento deste tipo pode ser eficiente, pois deixa em praticamente em zero a atividade do nodo vítima.

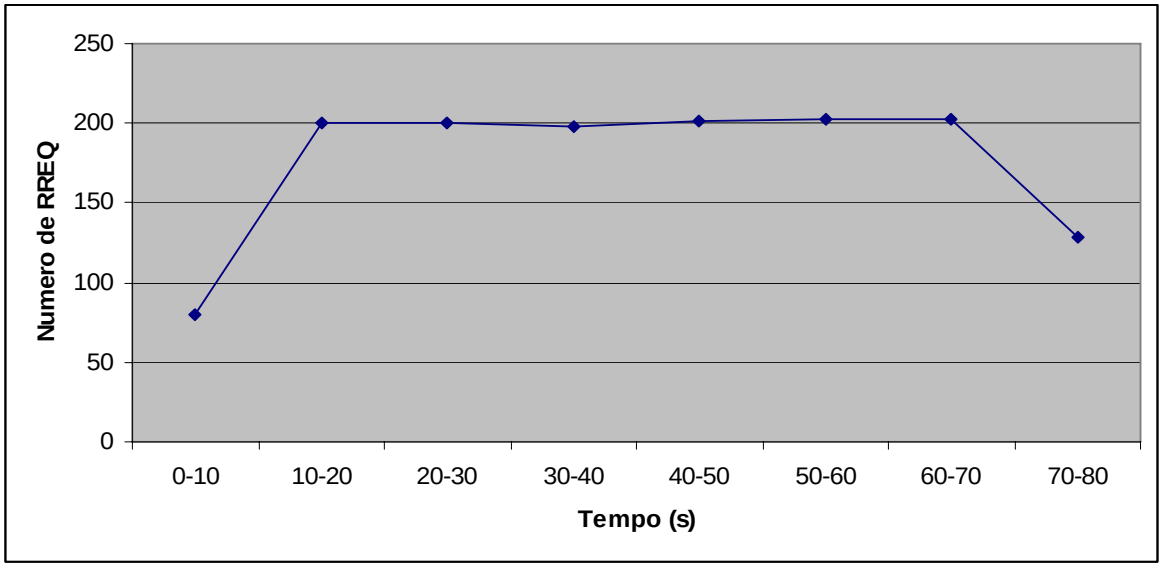

Gráfico 11: Quantidade de RREQ enviadas pelo atacante.

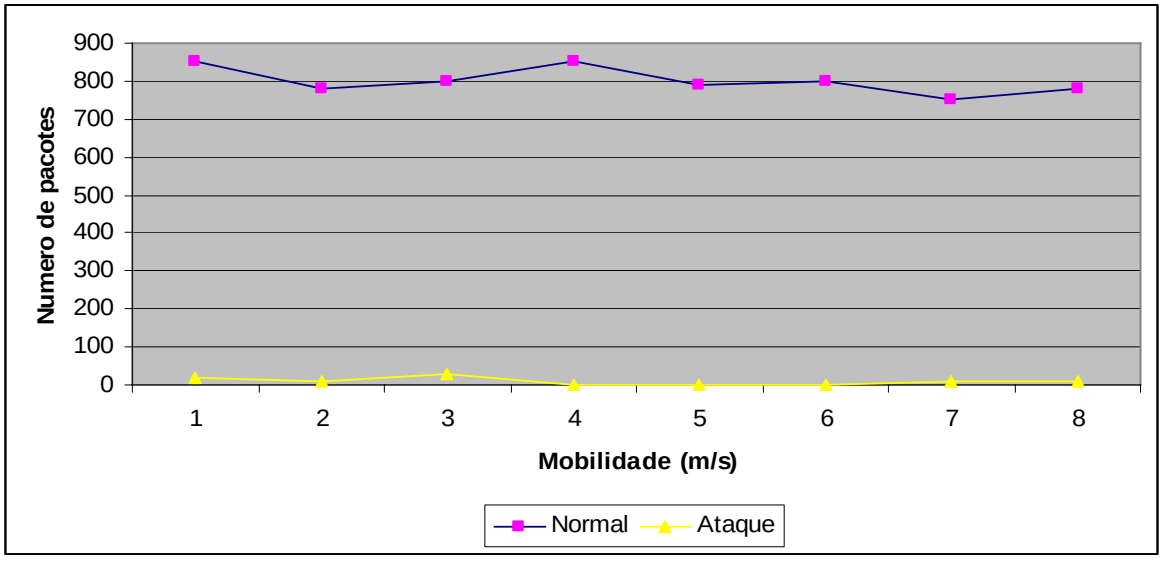

Gráfico 12: Quantidade de pacotes recebidos pela vítima.

Conclusão

Torna-se claro ao observar os gráficos e as simulações, que a segurança de uma rede *ad hoc* é um ponto delicado que merece muito estudo e observação.

O estudo feito, além de analisar teoricamente os pontos de vulnerabilidade do protocolo AODV,

tem como complemento as simulações feitas que se aproximam muito dos resultados reais de funcionamento da rede.

Muitos subsídios de informação e de ferramentas estão disponíveis para quem deseja se aprofundar no assunto e possivelmente contribuir para a solução de problemas. O *Network Simulator* se mostrou uma ferramenta muito completa no estudo e suporte de vários ambientes e possibilitou a reprodução perfeita de cenários onde se da à comunicação entre nodos da rede e principalmente se mostrou uma ferramenta flexível no sentido de inclusão de novas ferramentas e métodos de simulação.

Referências

[1]. Albuquerque, L. R., “Segurança Redes Ad Hoc”, Universidade Federal do Rio de Janeiro, Brasil, 2003.

[2]. Amodei, A. e Duarte, O. M. B., “Segurança no roteamento de em Redes Moveis Ad Hoc”, Universidade Federal do Rio de Janeiro, Brasil, 2003.

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

[4]. Ning P. e Sun K., “How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols”, Tech. Rep. TR-2003-07, CS Department, NC State University, 2003.

[5]. The VINT (Virtual InterNetwork Testbed) Pagina do projeto, http://www.isi.edu/nsnam/vint/index.html

[6]. Wang, W., Lu, Y., and Bhargava, B. (2002). On security study of two distance-vector routing protocols for mobile ad hoc networks. Technical report, Technical report, Dept. of Computer Sciences, Purdue University.

[7]. Yang, H. et al., “Security in Mobile Ad Hoc Netwoks: Challenges and solutions”, IEEE wireless communications, 2004, pages 38-47.