UMA ANÁLISE DOS IMPACTOS DE AÇÕES MALICIOSAS
DE NÓS NO ROTEAMENTO EM REDES AD HOC

Luiz Gustavo Silva Rocha

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA ELÉTRICA.

Aprovada por:

Prof. Otto Carlos Muniz Bandeira Duarte, Dr. Ing.

Prof. Luís Henrique Maciel Kosmalski Costa, Dr.

Prof. Aloysio de Castro Pinto Pedroza, Dr.

Prof. Alfredo Goldman vel Lejbman, Dr.

RIO DE JANEIRO, RJ - BRASIL

JULHO DE 2004

ROCHA, LUIZ GUSTAVO SILVA

Uma Análise dos Impactos de Ações Maliciosas de Nós no Roteamento em Redes Ad Hoc [Rio de Janeiro] 2004

XII, 51 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia Elétrica, 2004)

Tese - Universidade Federal do Rio de Janeiro, COPPE

1. Redes Ad Hoc

2. Segurança

3. Roteamento

I. COPPE/UFRJ II. Título (série)

À Carmen Lúcia Rocha.

Agradecimentos

Agradeço primeiramente a Deus por chegar até aqui, aos meus pais pelo apoio e aos amigos pela companhia nessa jornada.

Muito obrigado aos colegas, professores, orientadores e membros da banca pela oportunidade.

Obrigado a UFRJ, COPPE, CAPES e seus funcionários pela colaboração.

Agradeço em especial a Fernanda por estar ao meu lado.

Resumo da Tese apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

UMA ANÁLISE DOS IMPACTOS DE AÇÕES MALICIOSAS DE NÓS NO ROTEAMENTO EM REDES AD HOC

Luiz Gustavo Silva Rocha

Julho/2004

Orientadores: Otto Carlos Muniz Bandeira Duarte
Luís Henrique Maciel Kosmalski Costa
Programa: Engenharia Elétrica

Este trabalho analisa ataques baseados no comportamento malicioso de alguns nós no roteamento das redes ad hoc e investiga as características desejáveis de um mecanismo de proteção para minimização do impacto dessas ações maliciosas. A análise se baseou no protocolo de roteamento AODV. As ações maliciosas têm como alvo os pacotes de dados e de controle, que estão no nível do agente de roteamento AODV, através do comportamento egoísta de nós comprometidos. Num ambiente distribuído onde cada nó age como roteador e as rotas são constituídas sob demanda, tais ações degradam sensivelmente o desempenho da rede como um todo. As métricas taxa de entrega, atraso de pacotes e sobrecarga de roteamento foram analisadas por meio de simulações variando-se características de tráfego, movimentação dos nós, tipo de ataque e densidade de atacantes.

Abstract of Thesis presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

PERFORMANCE ANALYSIS OF MALICIOUS NODES ACTION
IN AD HOC NETWORKS ROUTING

Luiz Gustavo Silva Rocha

July/2004

Advisors: Otto Carlos Muniz Bandeira Duarte
Luís Henrique Maciel Kosmalski Costa

Department: Electrical Engineering

This work analyzes attacks based on the malicious behavior of some nodes in the ad hoc networks routing and investigates the desirable features of a protection mechanism for mitigating the impact of these malicious actions. This analysis was based on the AODV routing protocol. The malicious actions have as target the packets that are in the AODV routing agent level, conferring selfishness behavior to the compromised nodes. In a distributed environment where each node acts as a router and the routes are constructed on demand, such actions significantly degrade the entire network performance. The metrics delivery rate, packet delay and routing overhead were analyzed by simulations according to different characteristics of traffic, movement of nodes, type of attack and density of attackers.

Lista de Acrônimos

AODV	- *Ad Hoc On-Demand Distance Vector;*
ARAN	- *Authenticated Routing for Ad Hoc Networks;*
CBR	- *Constant Bit Rate;*
DCF	- *Distributed Coordination Function;*
DoS	- *Denial of Service;*
DSDV	- *Destination-Sequenced Distance-Vector;*
DSR	- *Dynamic Source Routing;*
IETF	- *Internet Engineering Task Force;*
MAC	- *Message Authentication Code;*
MANET	- *Mobile Ad Hoc Network;*
MPR	- *MultiPoint Relays*
PCF	- *Point Coordination Function*
RFC	- *Request For Comments;*
RREP	- *Route Reply;*
RREQ	- *Route Request;*
RERR	- *Route Error;*
SAODV	- *Secure Ad Hoc On-Demand Distance Vector;*
SEAD	- *Secure Efficient Distance Vector Routing for Ad Hoc;*
TESLA	- *Timed Efficient Stream Loss-Tolerant Authentication;*
TTL	- *Time To Live;*
UDP	- *User Datagram Protocol.*

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

AS redes sem fio são uma realidade tecnológica que passaram a permear nossas vidas nos últimos anos e que a cada dia ainda conquistam novos nichos de aplicação. Isto se deve às características dessas redes, que introduziram comodidade, flexibilidade e praticidade na comunicação entre pessoas e dispositivos. Tais características são principalmente a inexistência de cabos e a utilização do ar como meio de propagação dos sinais e ainda, no caso das redes sem fio ad hoc, a não existência de uma infra -estrutura previamente estabelecida. Esses atributos dotaram de mobilidade os nós das redes e as tornam ideais para aplicações nas quais as redes tradicionais de nós fixos e cabeadas são inadequadas.

São inúmeros os cenários de aplicações das redes sem fio que vão desde a comunicação a distâncias curtas entre pessoas e principalmente entre dispositivos, até operações militares ou de resgate, que envolvem maiores distâncias e mobilidade dos nós da rede. Cada aplicação possui um conjunto de características que leva à utilização de soluções particularmente otimizadas para cada finalidade. Esse motivo justifica os diferentes tipos de tecnologia com diferentes interfaces e protocolos de comunicação. O Bluetooth, por exemplo, é uma tecnologia voltada para interligar até 7 dispositivos numa rede local pessoal de curto alcance (10 m) e baixa taxa de transferência (1 Mbps). Já o IEEE 802.11g pode interligar mais dispositivos com melhores taxas de transferência (54 Mbps) a distâncias superiores (100 m).

Embora a comunicação através desse tipo de rede tenha várias vantagens, elas ainda apresentam algumas desvantagens ou limitações em certos aspectos de sua operação. São nesses aspectos que se concentram os trabalhos dos pesquisadores e das indústrias que visam conceber tecnologias capazes de aliar as características desejáveis das redes sem fio e das redes fixas tradicionais.

Um aspecto desvantajoso ou uma limitação de aplicação das redes sem fio está relacionado à segurança nas transações. A utilização do ar como meio de transmissão compartilhado e a mobilidade dos nós são atributos que trazem grandes desafios para o desenvolvimento de mecanismos de segurança eficazes para esse tipo de rede.

O desafio de desenvolver mecanismos de segurança para redes móveis sem fio que ofereçam os mesmos níveis de proteção dos mecanismos das redes fixas tradicionais se torna ainda maior quando considerada a necessidade de tais mecanismos não impactarem significativamente no desempenho da rede e na vida dos usuários.

1.1 Redes sem fio

Pode-se distinguir basicamente dois tipos de redes sem fio. O primeiro tipo de rede sem fio baseia-se na comunicação de cada dispositivo móvel com os demais via um equipamento centralizador, denominado ponto de acesso ou estação base . Nessa configuração de rede, cada um dos dispositivos móveis comunica-se somente com um ponto de acesso que faz o roteamento das informações. Toda a comunicação entre os dispositivos necessariamente passa por um ponto de acesso e todos os dispositivos devem estar ao alcance de um ponto de acesso. Esses pontos de acesso podem ou não estar conectados a outros pontos de acesso e a outras redes, seja por meio de cabos ou pela interface aérea. Esse tipo de rede sem fio é denominada de infra-estruturada (ver Figura 1.1(a)).

Nessa configuração de redes, infra-estruturada, é possível alcançar melhores níveis de segurança dado o controle maior que se pode ter do ponto de acesso. Sendo o ponto de acesso uma estrutura central e que pode até ser fixa, torna-se mais simples estabelecer controles sobre as informações e ações dos nós da rede sem fio.

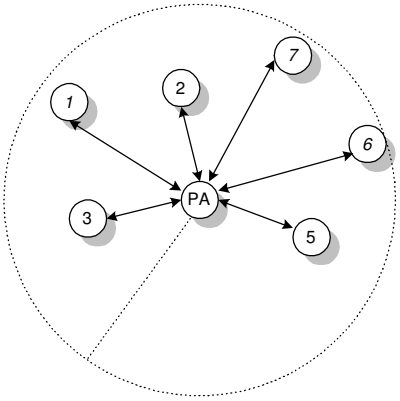
O segundo tipo de rede sem fio é constituído por um conjunto de dispositivos móveis capazes de se comunicar diretamente um com o outro, sem a necessidade de pontos de acesso, bastando apenas que os dispositivos estejam ao alcance mútuo. Quando um dispositivo destino das informações não se encontrar diretamente ao alcance de outro fonte, esse pode usar seus dispositivos vizinhos para alcançá-lo, ou seja cada dispositivo é capaz de rotear informações na rede fazendo uma comunicação por múltiplos saltos através dos nós da rede até que seja alcançado o nó destinatário (ver Figura 1.1(b)).

Nesses tipos de redes, chamadas de redes móveis ad hoc, torna-se mais difícil estabelecer algum tipo de controle das informações e ações dos nós, devido à inexistência de uma estrutura fixa ou central onde se possa instalar tais mecanismos.

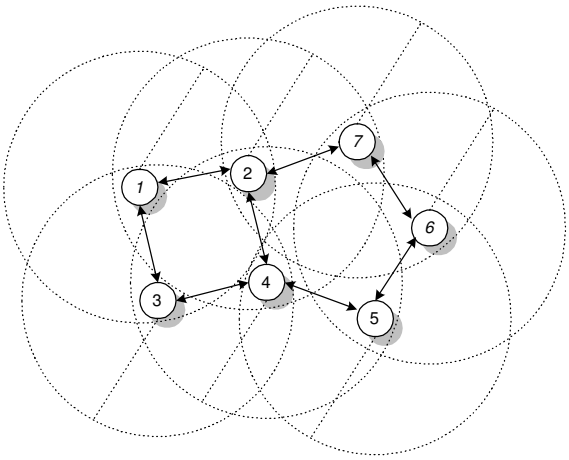
As tecnologias de redes de comunicação sem fio apresentam no entanto algumas limitações como: reduzida banda passante, altas taxas de erro e, no caso dos dispositivos portáteis, limitados poder computacional e de duração da bateria . Os alvos das constantes evoluções dessas tecnologias são a melhor utilização da interface aérea, da capacidade computacional e da energia disponíveis. As evoluções na parte de software têm acontecido por meio da implementação de novos protocolos que maximizem a utilização do meio de transmissão e minimize a quantidade total de dados transmitidos e de processamento realizado. As evoluções na parte de hardware têm chegado por meio dos novos *chipsets* para equiparem os rádios e as centrais de processamento desses dispositivos de maior capacidade para atender as demandas cada vez maiores de esforço computacional.

Embora as redes sem fio apresentem características vantajosas do ponto de vista da praticidade de utilização, elas também apresentam problemas relativos à segurança, intrínsecos ao processo de operação da rede. Possíveis cenários de aplicação onde a segurança das informações transmitidas pela rede é crítica, não poderiam ser contemplados devido à carência de mecanismos que proporcionem os níveis de segurança exigidos pela aplicação. Essa é a necessidade que leva ao desafio do desenvolvimento de mecanismos capazes de conferir às redes sem fio as características de segurança das redes tradicionais.

Com as constantes evoluções na parte de hardware e os avanços graduais na parte de software para as redes sem fio, ambos aliados a produção em escala, que diminuirá os preços dos componentes, é razoável afirmar que os acessos à internet hoje feitos por cabo,



(a) esquema da rede sem fio infra-estruturada.



(b) esquema da rede sem fio ad hoc.

Figura 1.1: Rede de nós móveis em ambos os modos de operação.

principalmente na última milha, serão plenamente substituídos por acessos sem fio. Para tanto é necessário que os usuários confiem na tecnologia de comunicação sem fio e isso só será alcançado no momento em que ela ofereça desempenho e, principalmente, segurança em níveis similares aos dos sistemas cabeados.

1.2 Segurança em redes sem fio

Como as redes sem fio utilizam o ar como meio de transmissão, as informações trocadas entre os nós da rede ficam sujeitas a serem interceptadas mais facilmente do que nas redes cabeadas. Dado que os sinais são propagados pelo ar, pode-se também impedir de alguma forma que estes sinais alcancem o seu destino. Sendo assim o mecanismo que controla o acesso da interface de comunicação ao meio de transmissão e o mecanismo de encaminhamento de informações pela rede sem fio tornam-se os alvos preferidos de ataques.

A segurança é um requisito fundamental para viabilizar o emprego das redes sem fio em ambientes hostis e sob condições adversas de operação. Podemos agrupar e resumir os requisitos para os mecanismos de segurança da seguinte forma [1]:

- integridade – garantir que a informação recebida no destino é idêntica àquela que foi enviada pela fonte;
- privacidade – garantir que somente o destinatário é capaz de compreender o conteúdo da mensagem;
- autenticação – garantir que uma entidade é realmente quem ela alega ser.

Para alcançar esses requisitos algumas medidas são adotadas e entre as mais comuns estão a utilização de códigos de integridade de mensagens e de algoritmos criptográficos, juntamente com os mecanismos e políticas de gerenciamento de chaves em grupo e certificação digital.

Os códigos de integridade de mensagem (MAC - *Message Authentication Codes*) são utilizados semelhantemente aos códigos detectores de erro, servindo para verificar alterações não autorizadas nas mensagens transmitidas, garantindo a integridade das informações.

Os algoritmos criptográficos são responsáveis pela codificação da informação tornando-a incompreensível para quem desconheça a maneira como ela foi codificada. Há dois

tipos de criptografia, uma denominada criptografia simétrica ou de chave secreta e outra denominada criptografia assimétrica ou de chave pública. A primeira faz uso de uma única chave para criptografar e decriptografar os dados, essa chave é mantida em sigilo e somente as entidades que desejam se comunicar com segurança devem conhecê-la. O segundo tipo de criptografia utiliza um par de chaves criptográficas associado a cada entidade da rede, sendo uma das chaves a privada, que deve ser mantida em sigilo, e a outra chave a pública, que pode ser livremente distribuída na rede. Nesse caso as informações criptografadas com uma das chaves (a privada) somente podem ser decodificadas pelo seu par correspondente de chave (a pública).

O ponto crítico dos esquemas de criptografia é o gerenciamento das chaves. O sucesso desses mecanismos depende fortemente dos mecanismos de gerenciamento de chaves que podem ter sua implementação complicada e o funcionamento prejudicado pelas características da rede. Embora existam estudos a respeito [1] a maioria das implementações de mecanismos de criptografia prevê que o estabelecimento prévio das chaves e até seu gerenciamento seja efetuado por fora da banda.

A utilização de entidades certificadoras também pode ser complicada devido as características de operação da rede. Uma saída é a realização de uma certificação digital compartilhada, onde vários dos nós da rede são responsáveis por certificar a identidade de outros nós [2].

1.3 Segurança em redes sem fio ad hoc

No que diz respeito a aplicações sensíveis no aspecto de segurança, as MANETs (*Mobile Ad hoc Networks*) devem ser auxiliadas por mecanismos que contemplem os requisitos de segurança e que impeçam a ação de nós com comportamento malicioso que objetivam atacar a rede das diferentes formas possíveis, aproveitando suas vulnerabilidades. Deve-se ainda observar para o desenvolvimento e avaliação desses mecanismos as limitações operacionais ligadas à mobilidade e ao enlace sem fio, como a restrição da bateria, alcance limitado do rádio, capacidade de processamento do dispositivo e banda passante estreita do meio físico utilizado.

Nas redes ad hoc a inexistência de dispositivos que centralizam a comunicação tornam a implementação de mecanismos de segurança mais complexa e desafiadora. Os mecanismos desenvolvidos para redes convencionais não são compatíveis com o ambiente ad hoc, devido às premissas geralmente necessárias a sua operação, como por exemplo um repositório de chaves públicas da rede ou um servidor de autenticação ou certificação digital.

A natureza da operação das redes móveis sem fio ad hoc dificulta a migração dos esquemas de segurança adotados nas redes fixas tradicionais. Isso se deve principalmente a características como: não disponibilidade de uma entidade central na rede, inconstância dos enlaces de comunicação entre os nós, variabilidade constante do número de nós e dos membros da rede, mobilidade dos dispositivos, que leva a constantes mudanças na topologia da rede, e necessidade de portabilidade dos dispositivos. A necessidade de conferir aos dispositivos a facilidade de movimentação (portabilidade) interfere diretamente nas características de capacidade da bateria e de processamento.

Os trabalhos sobre segurança em redes ad hoc, em sua maior parte, concentram-se na área de roteamento, que é o ponto crítico de funcionamento das redes móveis sem fio ad hoc. As vulnerabilidades dos mecanismos básicos de operação constituem uma forma de interferir na operação normal da rede através da inserção, modificação ou eliminação de informações, como por exemplo, do roteamento. Em especial nas redes ad hoc o mecanismo de roteamento é vulnerável a falhas e a ataques, pois todos os nós da rede atuam como roteadores e encaminhadores de pacotes, diferentemente das redes fixas tradicionais. É importante portanto avaliar o funcionamento desses protocolos de roteamento ad hoc sob condições adversas de operação.

Como todos os nós da rede atuam como roteadores, o que permite a comunicação entre os nós através de múltiplos saltos, e esses nós ainda são móveis e se comunicam através de um meio aberto, o cenário para aplicação de um mecanismo de suporte a segurança no roteamento em redes sem fio ad hoc se torna bastante complexo.

O objetivo deste trabalho é quantificar os efeitos de ataques ao protocolo de roteamento de uma rede ad hoc na forma de comportamento não-colaborativo dos nós da rede no nível do agente de roteamento, tomando-se como exemplo o protocolo AODV (*Ad Hoc On-Demand Distance Vector*) [3]. Esses ataques visam minar o roteamento, prejudicando

a operação da rede. A partir da avaliação do impacto dos ataques pode-se elaborar uma estratégia para minimizar a degradação de desempenho da rede tornando-a assim mais robusta e evitando o consumo excessivo de recursos da rede.

O resultados deste estudo são analises dos ataques baseados no comportamento malicioso de nós no roteamento das redes ad hoc e indicações das características desejáveis de um mecanismo de proteção para minimização do impacto dessas ações maliciosas. As ações maliciosas têm como alvo os pacotes de dados e de controle, que estão no nível da camada de roteamento, através do comportamento egoísta de nós comprometidos no ataque. Num ambiente distribuído onde cada nó age como roteador e as rotas são constituídas sob demanda, tais ações degradam sensivelmente o desempenho da rede como um todo. As métricas taxa de entrega de pacotes de dados, atraso dos pacotes e sobrecarga de roteamento foram analisadas variando-se características de tráfego na rede, movimentação dos nós, tipo de ataque e densidade de atacantes.

Este trabalho está organizado da seguinte forma. O Capítulo 2 apresenta as redes ad hoc com enfoque no protocolo de roteamento reativo AODV e descreve alguns aspectos de segurança em termos das vulnerabilidades e dos ataques às redes ad hoc, bem como as propostas de roteamento seguro encontradas na literatura. No Capítulo 3 são apresentados os detalhes de implementação do ambiente de simulação para a proposta de avaliação e os ataques implementados. Os resultados e as análises obtidas a partir das simulações dos casos estudados encontram-se no Capítulo 4. O Capítulo 5 encerra o trabalho apresentando as conclusões finais e direções para trabalhos futuros.

Capítulo 2

Redes ad hoc

AS redes ad hoc não possuem qualquer tipo de infra-estrutura e necessitam portanto de um esquema de encaminhamento de informações que seja adequado à conectividade através de múltiplos saltos, à freqüente mudança na topologia da rede e às restrições operacionais dos dispositivos e do meio físico utilizado para transmissão dos sinais. Além disso, numa rede ad hoc todos os nós participam das ações de roteamento e do encaminhamento de pacotes [4, 5]. Logo, o núcleo da operação de uma rede ad hoc é o mecanismo de roteamento e por isso é tão importante analisá-lo sob o enfoque dos aspectos de segurança.

Estes mecanismos de roteamento devem ser capazes de realizar o serviço de encaminhamento de pacotes com a menor sobrecarga (*overhead*) e consumo de banda possíveis e possuir uma latência que não prejudique as aplicações sensíveis ao atraso de pacotes, e ainda atender aos requisitos de segurança exigidos por determinadas aplicações [6, 7].

2.1 Roteamento em redes ad hoc

O objetivo do mecanismo de roteamento ad hoc é estabelecer uma rota através da rede que conecte dois nós distintos. Essa rota irá propiciar a transmissão de pacotes entre a fonte e o destino. A escolha da rota será feita com base em uma métrica, que pode ser por exemplo, o caminho com menor número de saltos ou com maior banda disponível.

No que diz respeito à maneira de implementar o esquema de encaminhamento de pacotes de informações há dois tipos de protocolo de roteamento ad hoc, os reativos (*on-demand*) e os pró-ativos (*table-driven*) [8].

O modelo pró-ativo (*table-driven*) é o utilizado nas redes fixas tradicionais e que posteriormente foi adaptado para o ambiente sem fio ad hoc. Os protocolos de roteamento pró-ativos operam mantendo, em cada nó, informações atualizadas da rota para se chegar a todos os outros nós da rede. As informações de roteamento são trocadas periodicamente, mesmo sem a necessidade de uso de determinada rota. Estas informações são armazenadas em tabelas de roteamento presentes em todos os nós que constituem a rede. A maneira como são formadas, atualizadas e o número e tipo de entradas nestas tabelas de roteamento variam de acordo com as diferentes implementações de protocolos de roteamento pró-ativos.

Um exemplo de protocolo pró-ativo é o DSDV (*Destination-Sequenced Distance-Vector*) [9], um protocolo de roteamento pró-ativo baseado no algoritmo de Bellman-Ford (algoritmo de vetor de distâncias). Os nós no DSDV operam requisitando de forma periódica a seus vizinhos suas tabelas de roteamento. A atualização das informações de roteamento também é feita quando é detectada uma mudança na topologia da rede, obedecendo apenas a um intervalo mínimo entre as atualizações, para evitar sobrecarga de informações de roteamento na rede. Há ainda a possibilidade dessa troca de tabelas de roteamento ser efetuada de forma incremental ou completa, informando somente o que foi alterado ou toda a tabela novamente. Essa opção também visa evitar sobrecarga de informações de roteamento na rede. Essas tabelas de roteamento contém apenas um rota para todos os outros nós da rede. Nessas tabelas constam o próximo salto e o número de saltos para cada destino alcançável da rede. O DSDV serve de base de funcionamento para uma série de outros protocolos [8, 10], inclusive o AODV.

Outro exemplo de protocolo de roteamento pró-ativo é o OLSR (*Optimized Link State Routing*) [11]. O OLSR é uma otimização de protocolo de roteamento para o ambiente sem fio ad hoc baseado no algoritmo clássico de estado de enlace (*link state*). A otimização se dá pela utilização de nós especiais (MPRs - *multipoint relays*) selecionados para transmissão de mensagens em *broadcast* e geração de estados dos enlaces, com isso o

número de pacotes de controle é sensivelmente minimizado, essas características o tornam mais aplicável à redes com muitos nós e de alta densidade. Nesta situação, de redes grandes e densas com tráfego esporádico e aleatório entre os nós, níveis maiores de otimização são atingidos em relação a outros protocolos de roteamento. Cada nó no roteamento OLSR elege, entre seus vizinhos diretos e com enlace bidirecional, um conjunto de nós MPRs que serão os responsáveis pelos pacotes de controle na rede e por declarar os estados dos enlaces de seus eleitores. Essas informações são difundidas periodicamente na rede nos pacotes de controle. Os nós comuns utilizam os MPRs para alcançar os outros nós da rede. E os nós MPRs utilizam uns aos outros para estabelecer as rotas para todos os destinos alcançáveis da rede fazendo roteamento dos pacotes salto a salto.

Os protocolos reativos (*on-demand*), por outro lado, criam rotas somente quando necessário. As rotas são solicitadas pelos nós de origem somente quando há necessidade de transmissão de pacotes de dados, por isto são também classificados como *source-initiated*. O processo de descoberta de rotas na rede é iniciado sob demanda, ou seja, quando há dados num nó fonte a serem transmitidos para um nó destino. Em seguida a essa descoberta, um procedimento de manutenção da rota é feito permanentemente, até que a rota não seja mais necessária, ou que o destino se torne inalcançável por alguma falha no caminho que leve à ruptura dessa rota. Os processos de descoberta e manutenção das rotas diferenciam os vários protocolos de roteamento reativos. O modelo reativo é uma novidade das redes ad hoc que foi motivada pelas suas características de mobilidade e escassez de recursos (bateria, memória e banda passante).

Um exemplo de protocolo reativo é o DSR (*Dynamic Source Routing*) [12]. O DSR emprega o roteamento pela fonte. O nó fonte inclui no cabeçalho do pacote a ser enviado o caminho a ser percorrido para alcançar o destinatário. Nesse cabeçalho encontra-se a seqüência completa e ordenada do caminho a ser seguido pelo pacote. Todas as rotas conhecidas são armazenadas em um *cache*. Esse *cache* é alimentado por um processo de descoberta de rotas e de manutenção de rotas, semelhante ao que será visto mais adiante para o AODV. O nós no DSR podem manter em seus *caches* múltiplas rotas para o mesmo destino e também verificar a existência de rotas com seus vizinhos antes de disparar processos completos de descoberta de rotas. Essas medidas têm como objetivo minimizar a sobrecarga de roteamento em redes com constantes mudanças na topologia. O protocolo

DSR também permite aos nós aprender rotas com pacotes não endereçados diretamente à ele, mas que podem ser "ouvidos"pela interface de comunicação devido a escuta em modo promíscuo. O DSR ainda permite o salvamento de pacotes que deveriam ser encaminhados por uma determinada rota, mas que se encontra indisponível no momento, então esses pacotes passam a ser encaminhados por uma rota alternativa designada pelo nó intermediário antecessor ao enlace indisponível. Além disso há o reparo gratuito de rotas que permite ao nó fonte distribuir em seus pedidos de rota informações de erro nas rotas que chegam até ele, permitindo assim a atualização dos *caches* de outros nós.

Outro exemplo de protocolo reativo é o AODV (*Ad Hoc On-Demand Distance Vector*) [3, 13]. O AODV foi escolhido para este trabalho por ser um dos mais difundidos e estudados na literatura e por se tratar de um protocolo de roteamento ad hoc reativo não seguro e, portanto, possuir vulnerabilidades diferentes de protocolos de roteamento clássicos. O AODV foi padronizado através de uma RFC pelo grupo de trabalho MANET (*Mobile Ad Hoc Network*) do IETF (*Internet Engineering Task Force*) [3]. A seção seguinte tratará especificamente do protocolo de roteamento AODV.

O desenvolvimento dessa nova linha de protocolos para as redes sem fio ad hoc, a dos protocolos reativos, é uma necessidade motivada pelo problema de desempenho apresentado pela linha de protocolos pró-ativos. A maneira de operar sob demanda e iniciada pela fonte dos protocolos reativos tende a melhorar o rendimento do mecanismo de roteamento com relação ao uso dos recursos da rede. Mas ainda não se pode afirmar a superioridade de um em relação ao outro para quaisquer cenários de aplicação da tecnologia. A melhor solução irá depender das características de tráfego e mobilidade da rede e deverá considerar a análise de desempenho *versus* custo.

Os protocolos de roteamento a fim de atingir melhores relações desempenho *versus* custo para cada uma das aplicações, passaram a integrar novos parâmetros para otimizar o roteamento como a localização geográfica, a energia disponível no nó e até o conteúdo da mensagem. Mas a melhor das soluções parece caminhar no sentido da auto-configuração e adaptação do mecanismo de roteamento a cada situação na rede, a flexibilidade continua sendo a característica mais desejável também para os protocolos de roteamento.

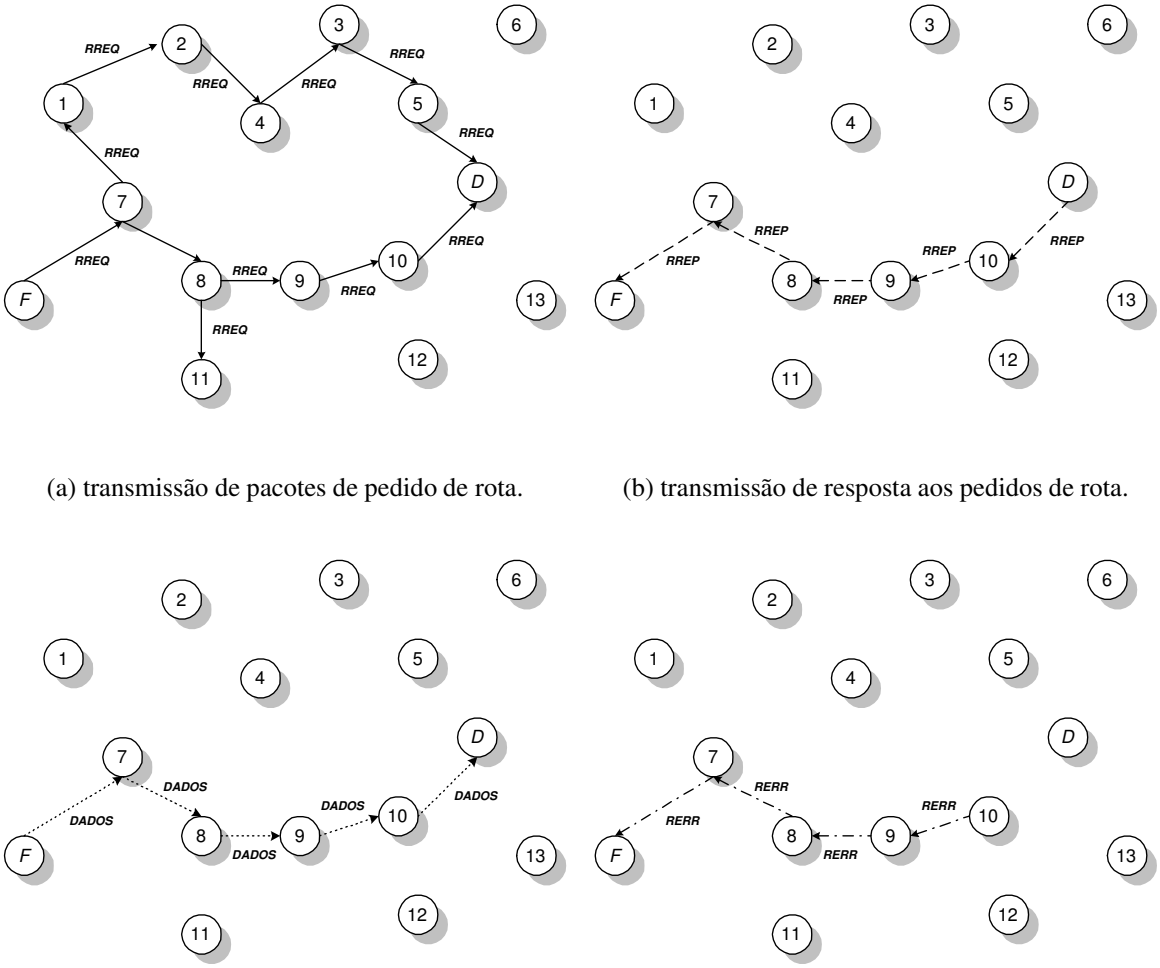
2.1.1 O protocolo de roteamento AODV

O protocolo de roteamento AODV (*Ad Hoc On-Demand Distance Vector*) [3] funciona sob demanda, é não hierárquico e toda a operação é iniciada pela fonte de dados. Quando um nó deseja se comunicar com outro nó dá-se início ao processo de descoberta de rotas com a difusão (*broadcast*) de pacotes de pedido de rota (*route request* - RREQ), conforme a Figura 3.1(a). Esses pacotes de pedido de rota são retransmitidos por todos os vizinhos do nó fonte que, por sua vez, retransmitem a todos os vizinhos e assim por diante, obedecendo a um critério variável de número máximo de retransmissões, característica conhecida como *Expanding Ring Search*. Essa característica de controle visa evitar a inundação desnecessária de pacotes de pedidos de rota na rede.

Quando o nó destino recebe o pacote de pedido de rota, envia um pacote de resposta (*route reply* - RREP), que é transmitido em *unicast* pelo caminho reverso ao criado pelo pedido de rota, conforme a Figura 3.1(b). Outro nó, que não seja o destino, mas que tenha uma rota atualizada para aquele destino também pode responder ao pedido de rota. As falhas no processo de encaminhamento de informações pela rota criada são relatadas através da transmissão de pacotes de erro de rota (*route error* - RERR), conforme a Figura 3.1(d). Assim todos os dispositivos que constituem a rede podem ter participação ativa nos processos de roteamento e encaminhamento de pacotes, agindo como roteadores ou *relay nodes*.

No processo de transmissão do RREQ os nós intermediários guardam a rota reversa do pedido para utilização futura e descartam pedidos repetidos graças aos números de seqüência de cada pacote. De maneira análoga, a transmissão de pacotes RREP pelo nó destino ou por outro com rota suficientemente atualizada para o destino, que utiliza a rota reversa do pedido, leva os nós intermediários a armazenar rotas para o destino requerido. As falhas de enlaces no caminho entre a fonte e o destino são sinalizadas pelos nós intermediários aos seus antecessores pelos pacotes RERR até que se atinja a fonte, que deve então iniciar um novo processo de descoberta de rota.

O termo *Distance Vector* diz respeito ao algoritmo utilizado para estimar a menor distância, em termos do número de saltos, de um nó até os outros. Cada nó da rede



(a) transmissão de pacotes de pedido de rota.

(b) transmissão de resposta aos pedidos de rota.

(c) troca de pacotes de dados.

(d) transmissão de pacotes de erro na rota.

Figura 2.1: Funcionamento do protocolo de roteamento AODV.

(i) armazena, para cada destino da rede (x) a partir de cada vizinho seu (j), uma série de vetores de distâncias ($\vec{d}_{ij}^{x}$) e escolhe sempre para cada destino a rota com a menor distância . Cada nó da rede agindo assim garante que as transmissões serão feitas pelas rotas mais curtas disponíveis naquele momento.

As rotas descobertas são mantidas em tabelas de roteamento tradicionais de uma entrada por destino, apenas as rotas em uso são armazenadas e um mecanismo de *soft state* faz a expiração das rotas não utilizadas recentemente, o objetivo deste esquema é a adaptação do mecanismo às mudanças na topologia da rede e adicionalmente a melhor utilização dos recursos do dispositivo e da rede. Outra característica do AODV é o número

de seqüência que cada pacote de roteamento carrega e que é associado a cada entrada da tabela de roteamento e serve para determinar a informação de roteamento mais atual e evitar *loops* na construção das rotas, contornando o problema de contagem infinita do algoritmo de vetor de distâncias. O número de seqüência é colocado em cada pacote por seu nó originador, que é responsável por incrementá-lo monotonicamente a cada nova informação de roteamento recebida ou gerada.

Cada entrada nas tabelas de roteamento do nós AODV armazena as seguintes informações:

- IP do Destino – endereço IP do nó destino da rota;
- Número de Seqüência – número de seqüência associado a entrada na tabela;
- Validade do Número de Seqüência – indicador da validade do número de seqüência da entrada na tabela;
- Interface de Rede – interface de rede utilizada para enviar pacotes por essa rota;
- Contagem de Saltos – número de saltos necessários para alcançar o destino;
- Próximo Salto – endereço IP do nó vizinho para onde serão encaminhados os pacotes com esse destino;
- Lista de Precursores – lista de nós vizinhos que encaminham pacotes para o destino por essa rota;
- Tempo de Vida – tempo a partir do qual essa rota irá expirar se ociosa;
- Flags de Roteamento – usadas para representar alguns situações da entrada, como reparabilidade, validade e origem;
- Estado da Rota – validade das informações dessa entrada na tabela.

Outro aspecto do protocolo AODV é o emprego de mensagens *hello* que são periodicamente transmitidas em *broadcast* com TTL 1 e visam informar à vizinhança a presença do nó, permitindo conhecimento da conectividade local da rede. O uso do *hello* é previsto

na especificação, mas pode ser dispensado no caso da camada MAC fornecer esta funcionalidade. Somente os nós que fazem parte de uma rota ativa transmitem *hello*. Mais detalhes sobre o protocolo de roteamento AODV podem ser vistos em [3], [8], [13] e em [14].

No documento de especificação do AODV [3] aparece como uma escolha apropriada para medida de segurança o emprego do IPsec AH [15]. O IPsec AH (*Authentication Header*) é um mecanismo que prevê integridade e autenticação da origem de datagramas IP através do preenchimento de um cabeçalho de autenticação padronizado inserido depois do cabeçalho IP, mas que depende dos nós compartilharem uma associação segura prévia e apropriada e não contempla pacotes de roteamento.

2.2 Segurança em redes ad hoc

As idéias para os mecanismos de segurança em redes ad hoc descendem das abordagens tradicionais dos problemas de segurança das redes convencionais (fixas e cabeadas). Portanto neste novo contexto, ainda se fazem presentes as idéias de protocolos de autenticação, assinaturas digitais, chaves criptográficas e outras [2, 5, 16]. Os requisitos de segurança de redes ad hoc estão intrinsecamente ligados ao tipo de cenário de aplicação da tecnologia [17, 18], uma sala de aula não necessita do mesmo nível de segurança destinada a um destacamento militar em incursão no terreno inimigo [19]. Cabe ressaltar que os mecanismos de segurança devem estar consoantes com as restrições encontradas nos sistemas de comunicação móvel sem fio, tais como escassez de recursos de rádio, pouca memória, baixa capacidade de processamento e duração restrita da bateria do dispositivo [20].

Devido a essa nova caracterização do contexto de aplicação as abordagens dos problemas de segurança tornaram-se mais complexas e demandam um maior esforço na sua implementação. Nas redes ad hoc podemos separar em dois grupos os tipos de mensagens ou pacotes que circulam pelos nós, sendo: os de dados e os de roteamento. Como esses dois grupos apresentam características e comportamentos diferentes não se pode abordar ambos da mesma forma no que diz respeito à segurança. As aplicações e as características

do ambiente ad hoc não permitem soluções simples como criptografar todos os pacotes indistintamente. E mesmo que assim fosse os esquemas de criptografia necessitam de mecanismo de gerenciamento de chaves criptográficas que são ainda mais complexos de se implementar em ambientes como esses.

Pode-se distinguir dois grandes conjuntos de vulnerabilidades a ataques nas redes ad hoc: o conjunto das vulnerabilidades dos mecanismos básicos de operação da rede e o conjunto das vulnerabilidades dos mecanismos de segurança [20]. O primeiro pode ser tratado basicamente por esquemas de criptografia, ou seja, os mecanismos básicos de operação da rede, onde o roteamento é o mais crítico deles, passariam a trocar informações criptografadas. O sistema torna-se vulnerável em relação aos mecanismos básicos quando, de alguma forma, é possível injetar, modificar ou replicar informações errôneas sobre a operação da rede, ou ainda, comportar-se de forma maliciosa e não cooperativa objetivando a degradação ou interrupção da operação da rede [10, 21]. O segundo conjunto de vulnerabilidades inclui as falhas dos próprios mecanismos que deveriam proteger a rede das ameaças. Um exemplo de vulnerabilidade deste tipo é a quebra de uma chave criptográfica [1, 2] ou a falha no protocolo de autenticação [18].

Os ataques podem ser classificados como ativos ou passivos e internos ou externos [6, 10, 18]. Os ataques, independentemente de sua classificação, têm como objetivo a descoberta de informações antes inacessíveis ou o impedimento da realização dos serviços da rede. A primeira classificação diz respeito ao comportamento do elemento que implementa o ataque que atua erroneamente ou deixa de atuar sobre as informações da rede, já a segunda refere-se ao elemento envolvido no ataque ser ou não membro autorizado/autenticado da rede. O mais severo dos ataques é o ativo interno onde o nó torna-se comprometido e realiza um ataque dito protegido, já que ele é um membro autorizado/autenticado da rede. Pode-se inclusive ter vários destes nós comprometidos operando em grupo tornando o ataque mais eficiente e danoso. A ameaça de impedimento de serviço constitui um grande risco num sistema distribuído, como em uma rede ad hoc, e pode ter sua origem numa falha não intencional de operação [16] ou em ações maliciosas por parte de elementos da rede [17, 20].

Podemos destacar algumas vulnerabilidades no protocolo AODV [14], das quais os

nós maliciosos podem se aproveitar para interferir e degradar o desempenho da rede, como:

- personificação de RREQ – enviar pedidos de rota forjando ser outro nó;
- personificação de RREP – enviar resposta a pedidos de rota forjando ser outro nó;
- personificação de RERR – sinalizar erros nas rotas forjando ser outro nó;
- falsificação de campos – falsificar as informações dos campos dos pacotes de roteamento, como os números de seqüência e números de saltos;
- inatividade seletiva – não encaminhar pacotes de dados ou roteamento inadvertidamente.

Os protocolos de roteamento que tentam lidar com o problema de nós maliciosos na rede podem ser divididos em diferentes classes de acordo com seu funcionamento [22], sendo: os preventivos, os detectores e os tolerantes. Os preventivos tentam a todo custo evitar a ação de tais nós maliciosos, mas se por algum motivo os controles conseguem ser burlados os protocolos não conseguem lidar com a presença e ação destes nós. Os detectores tentam sinalizar o quanto antes qualquer atitude suspeita por parte dos nós para que possam ser tomadas as medidas necessárias afim de evitar o começo de um ataque. Já os tolerantes tentam prover meios de continuar operando mesmo na presença de nós maliciosos visando minimizar o efeitos das ações maliciosas sobre os outros nós. A diferença fica por conta do custo, em termos de recursos dos nós e da rede, que a implementação de protocolos de cada uma dessas classes possa exigir.

Em termos gerais uma implementação de um protocolo de roteamento seguro e confiável deve apresentar essencialmente as seguintes características:

- impossibilitar que a sinalização de roteamento seja mascarada;
- impedir que mensagens de roteamento que foram maliciosamente fabricadas trafeguem na rede;

- não permitir que as mensagens de roteamento tenham seus parâmetros alterados durante seu trânsito pela rede, a não ser aqueles previsto na especificação do protocolo;
- nós maliciosos não podem interferir na computação e avaliação das métricas de roteamento;
- os nós malicioso devem ser excluídos da participação nas ações de roteamento.

Com relação às ações maliciosas deferidas pelos nós comprometidos no ataque a redes ad hoc por meio do mecanismo de roteamento, podemos agrupá-las em função dos seus objetivos principais da seguinte maneira [23]:

- ruptura de rotas;
- invasão de rotas;
- isolamento de nós;
- consumo indevido de recursos;
- impedimento de serviço.

Este trabalho modela e analisa um ataque passivo, interno e em grupo montado contra uma rede operando com o protocolo de roteamento AODV. Essa ameaça é especialmente danosa num ambiente distribuído, como em uma rede ad hoc, onde todos os nós cooperam entre si agindo como roteadores e encaminhadores de pacotes. Ações maliciosas no roteamento disparadas por vários nós podem constituir um DDoS (*Distibuted Denial of Service attack*). A proposta é avaliar o dano causado por ações não -colaborativas no nível do roteamento para levantar as características necessárias para estabelecer um mecanismo de segurança contra ações maliciosas de nós no roteamento AODV sem introduzir impacto significativo no desempenho da rede e que opere em conjunto com outros sistemas de segurança, como autenticação e criptografia.

2.2.1 Trabalhos Relacionados

Análises e propostas semelhantes à que realizamos, mas para o protocolo DSR, podem ser encontradas em [21], [24] e [22].

Em [21] Marti *et al.* apresentam dois mecanismos auxiliares ao roteamento, o *WatchDog* e o *PathRater*, que são responsáveis por minimizar os impactos de nós maliciosos na rede com resultados satisfatórios, embora sejam vulneráveis devido principalmente a possibilidade de geração de alarmes falsos. O *WatchDog* faz uso da escuta promíscua realizada pelas interfaces de rede dos nós operando com protocolo de roteamento DSR para verificar o comportamento dos vizinhos com relação a retransmissão dos pacotes a eles enviados. O *PathRater* faz uso das informações recolhidas pelo *WatchDog* sobre os nós vizinhos para atribuir notas ao comportamento desses vizinhos e utilizar tais notas como métrica de roteamento ao invés de somente considerar o tamanho das rotas. Nós maliciosos agindo em conluio podem driblar esses controles e prejudicar o roteamento na rede.

Papadimitratos e Hass em [24] e [25] não consideram as mensagens de erro nas associações seguras entre fonte e destino que o protocolo prevê, deixando a solução vulnerável. A autenticação é feita somente nas extremidades das rotas e na parte não variável dos pacotes. Como veremos adiante problemas relacionados às mensagens de erro têm grande impacto no desempenho do protocolo de roteamento, dependendo do cenário de movimentação dos dispositivos. Os mesmos autores apresentam em [26] o SMT (*Secure Message Transmission*), um protocolo eficiente para segurança na transmissão de pacotes de dados nos moldes do anterior, mas fica na dependência de funcionar sobre um protocolo de roteamento seguro. Essas duas propostas são complementares e constituem uma solução para segurança em redes ad hoc, mas que ainda é incompleta e vulnerável.

Em [22], Xue e Nahrstedt propõem uma modificação no algoritmo de roteamento, baseando-se no DSR, para considerar o desempenho fim-a-fim do roteamento que visa especificamente evitar os nós maliciosos na construção e utilização das rotas baseando-se em redundância, mas que tenta manter uma baixa sobrecarga de mensagens de controle. O BMR (*Bypassing Misbehaving nodes Routing*) trabalha em duas etapas, a fase de teste

e a fase de entrega. A fase de testes parte avaliando, segundo uma heurística determinada, as rotas das menores para as maiores, em termos do número de saltos até o destino. É escolhida a primeira nessa seqüência com o melhor desempenho em relação a taxa de perdas e atraso dos pacotes. O desempenho é avaliado segundo um modelo que é fornecido e alimentado com os parâmetros medidos na fase de teste, a saída sinaliza quando a rota não é satisfatória. A rota escolhida é efetivamente utilizada na fase de entrega. A solução pressupõem uma associação segura entre fonte e destino, de forma que eles possam autenticar a identidade um do outro e prevê o emprego de múltiplas respostas a pedidos de rota. Outro ponto negativo da solução pode ser com relação a variação brusca no comportamento de alguns nós entre a fase de testes e a fase de entrega.

Outra análise em termos mais abrangentes relativa a falhas no roteamento aparece em [27] onde Awerbuch *et al.* apresentam um mecanismo de roteamento sustentável mesmo em presença de falhas, intencionais ou não, de um grupo de nós da rede. O mecanismo baseia-se na construção e consulta a uma lista de pesos dados aos enlaces que constituem as rotas segundo as falhas apresentadas por cada enlace. A solução tenta prover a sustentabilidade do mecanismo de roteamento, mesmo em condições adversas de ataques bizantinos. Os ataques bizantinos incluem a formação intencional de *loops* e rotas não ótimas e o descarte seletivo de pacotes de dados e controle. O comportamento bizantino é o desvio inadvertido, intencional ou não do padrão especificado de comportamento de um sistema. O protocolo de roteamento sob -demanda proposto opera em três fase, sendo: a descoberta de rotas com prevenção de falhas, a detecção de falhas bizantinas e o gerenciamento dos pesos dos enlaces. A fase de descoberta de rotas emprega inundação de pedidos de rota e de respostas e esses pedidos e utiliza a lista prévia de pesos dos enlaces para selecionar as melhores rotas. A fase seguinte utiliza o reconhecimento de recebimento de pacotes de dados (*acks*) para avaliar e atribuir pesos aos enlaces que constituem a rota utilizada. A fase final é o gerenciamento do histórico dessas listas de pesos criadas para os enlaces que serve como entrada na fase de descoberta de rotas. O mecanismo proposto é eficiente do ponto de vista da segurança, mas pode causar grande sobrecarga de processamento e de pacotes de controle, devido a verificação dos *acks* e inundações de pacotes de controle na fase de descoberta de rotas, respectivamente.

Há ainda alguns outros trabalhos que tratam da segurança no roteamento em redes

ad hoc como em SEAD [28] para o protocolo DSDV, em Ariadne [29] para o protocolo DSR e em ARAN [30].

O Ariadne , de Johnson *et al.*, baseia-se em mecanismos de autenticação como o TESLA (*Timed Efficient Stream Loss-Tolerant Authentication*). A autenticação do TESLA baseia-se na adição de MACs (*Message Authentication Codes*) em mensagens para autenticação em *broadcast*. Os MACs são calculados baseados em chaves assimétricas devido a necessidade de verificação da autenticidade das mensagens por todos os nós ponto a ponto. Para ser mais eficiente o TESLA alcança a assimetria necessária nas chaves através da geração de cadeias de chaves unidirecionais (*one -way hash chains*) ao invés de empregar protocolos como o RSA [31], sob pena da necessidade de sincronismo entre os relógios dos dispositivos. A exigência de sincronismo vem da necessidade de estabelecer um cronograma conhecido por todos para a publicação das chaves, como será visto adiante.

O TESLA, assim como outros mecanismos de autenticação, tem como premissa um certo nível de sincronização entre os dispositivos móveis. A sincronização é considerada por alguns autores uma hipótese irreal para as redes ad hoc devido a suas características de esparcidade e comportamento dos enlaces, além de introduzir uma significativa sobrecarga e atraso devido às trocas de mensagens necessárias. Trabalhos como o de Sun *et al.* em [32] têm como objetivo driblar esse problema da aplicação dos algoritmos clássicos de sincronização às redes ad hoc através de novas abordagens que consideram o compromisso entre o nível de sincronismo e o consumo de recursos da rede [32, 33]. Ainda como ponto negativo o Ariadne, assim como o SRP, não protege as mensagens de erro.

No SEAD (*Secure Efficient Distance Vector Routing for Ad Hoc*), Perrig *et al.* apresentam um mecanismo de roteamento seguro inspirado no DSDV, baseado em *hash chains* ao invés de criptografia assimétrica e na abordagem por vetores de distância. Nesta proposta ainda persiste o problema de alguma sincronização necessária entre os nós e da publicação autenticada dos elementos da cadeia. O objetivo é manter ao longo das atualizações das informações de roteamento na rede a autenticidade dos valores do número de saltos, do próximo salto e dos números de seqüência e da origem dessas informações através de MACs (*Message Authentication Codes*).

Em síntese, as funções *hash* (H - *one-way hash functions*), como as implementadas pelos algoritmos MD5 [34] e a SHA-1 [35], são operações que mapeiam uma entrada aleatória de tamanho variável, denominada semente, numa chave com um número fixo de bits a partir do qual é matematicamente impossível reverter a operação, ou seja, a partir da chave descobrir a semente. A aplicação sucessiva dessas funções (H) gera a cadeia de chaves. Essas seqüências de chaves podem ser utilizadas para calcular os MACs (*Message Authentication Codes*) de pacotes de informação ou de roteamento. Para se verificar a integridade de uma informação autenticada por uma chave da cadeia, deve-se conhecer a função que gerou a cadeia e a chave gerada imediatamente antes a da que foi utilizada na autenticação do informação que deve ser a mais última da cadeia. Quando uma chave da cadeia é publicada todas as outras chaves geradas após a publicação podem ser descobertas. Por isso a publicação das chaves é feita no sentido contrário ao da geração da cadeia de chaves. Como vantagem, as operações envolvendo *hash chains* são menos computacionalmente custosas, e por conseqüência mais rápidas, do que as que envolvem critografia assimétrica [14, 28].

O ARAN (*Authenticated Routing for Ad Hoc Networks*) [30], de Belding-Royer *et al.*, tenta resolver algumas falhas de segurança apresentadas pelos protocolos AODV e DSR. O mecanismo baseia-se num processo preliminar de certificação e realiza autenticação salto a salto das mensagens de roteamento, introduzindo autenticidade e integridade às mensagens de roteamento, mas tem como ponto fraco a necessidade de um servidor central confiável para certificação. Além disso cada pacote de controle do roteamento que é encaminhado por algum nó deve ser assinado por esse nó. Esse procedimento consome tempo e recurso computacional e ainda causa um aumento progressivo no tamanho do pacote de roteamento a cada salto.

Há ainda para o protocolo AODV a proposta do SAODV [14, 36] de Zapata, que se baseia em assinaturas digitais e *hash chains* para garantir a integridade das informações de roteamento não variáveis salto a salto e variáveis, respectivamente. Segundo os autores essa proposta também pode ser estendida para outros protocolos de roteamento. Mas essa proposta também depende do suporte de um sistema de gerenciamento de chaves eficiente e não contempla o problema de nós maliciosos com comportamento não colaborativo. A proposta baseia-se na utilização de assinaturas digitais para assegurar as informações das

mensagens de roteamento não variáveis ao longo da rota. A autenticação baseada em assinaturas digitais é realizada entre os nós localizados nas extremidades das rotas, ou seja, entre a fonte e o destino. As cadeias *hash* são utilizadas para autenticar as informações dos pacotes de roteamento que são variáveis a cada salto. A verificação dessas informações é verificada salto a salto. Para agregar tais informações de controle foram criadas extensões nos pacotes AODV denominadas Extensões de Assinaturas e até essa parte do pacote é assinada para garantir sua integridade.

Capítulo 3

Implementação e Simulação

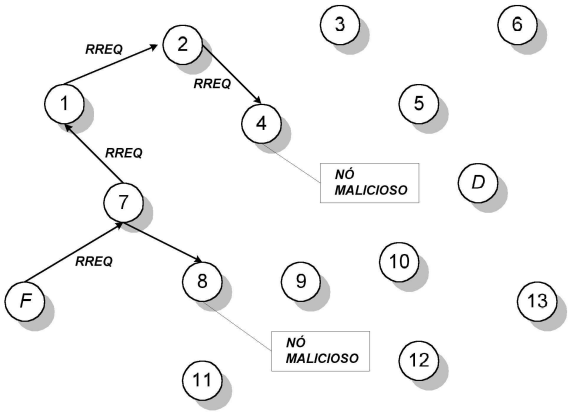
OS ataques ao roteamento de uma rede ad hoc podem ser implementados de diversas formas. Umas dessas formas, sutil, é o mal comportamento dos nós em relação às mensagens de roteamento, com o objetivo de degradar a entrega dos pacotes de dados na rede ou tornar indisponível determinado serviço oferecido pela rede [37]. Esse tipo de ataque foi implementado nesse trabalho e suas conseqüências e impactos avaliados por meio de simulações.

3.1 Ataques Implementados

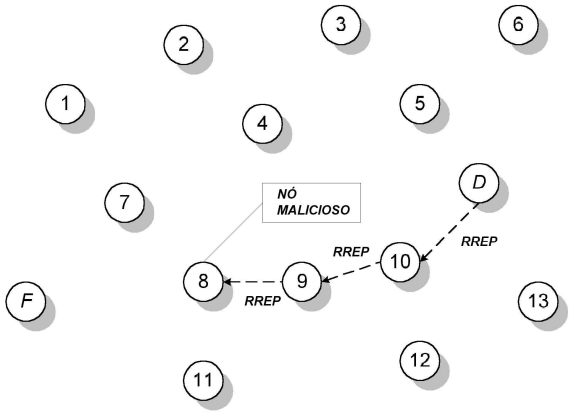
Os ataques analisados nesse trabalho partem da ação não colaborativa de nós maliciosos com relação aos pacotes de informação e de controle no nível do agente de roteamento. Para simular tal comportamento foram criados novos agentes de roteamento a partir do agente AODV original. Esses novos agentes têm características especiais em relação a cada um dos tipos de pacotes do roteamento AODV.

O ataque às mensagens de *route error* (ataque ERR) é implementado pelo agente MAL-ERR que verifica nos nós onde está atuando o recebimento de pacotes RERR e não os repassam aos nós antecessores, como deveria ser feito em funcionamento normal, conforme mostra a Figura 3.1(d). O comportamento não colaborativo (ataque REP) em relação às mensagens *route reply* recebidas é implementado pelo agente MAL-REP. O

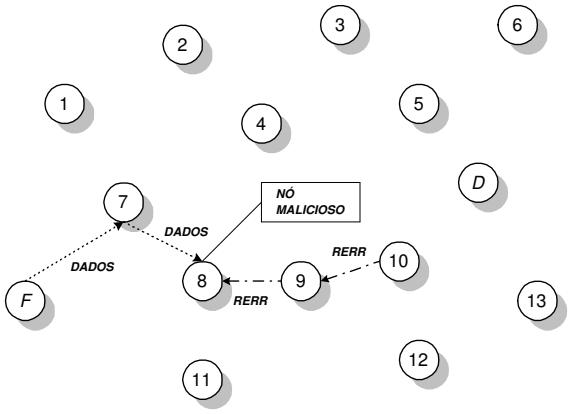
ataque REP impede o repasse de pacotes RREP que utilizem o nó em questão como rota, conforme a Figura 3.1(b). No entanto, um nó que implementa o agente MAL-REP aproveita as informações desses pacotes para benefício próprio, atualizando suas rotas. O ataque às mensagens de *route request* (ataque REQ) é feito pelo agente MAL-REQ. Este agente não propaga e nem responde pedidos de rota, a não ser pedidos próprios, agindo assim de forma não -colaborativa também, conforme mostra a Figura 3.1(a). O ataque tipo DATA é implementado pela agente MAL-DATA que impede o encaminhamento de pacotes de dados pelos nós com esse agente, exceto quando o nó é a fonte dos dados, conforme mostra a Figura 3.1(c).



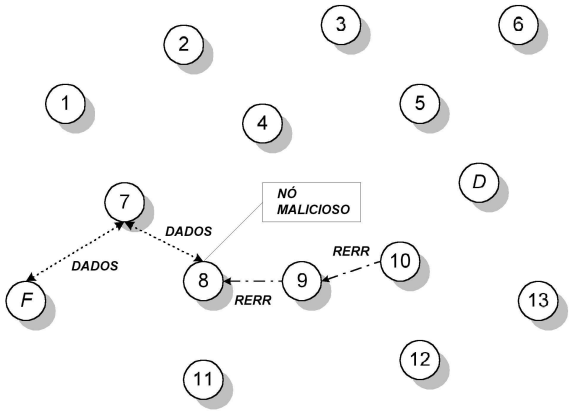
(a) ação do agente MAL-REQ nos nós.



(b) ação do agente MAL-REP nos nós.



(c) ação do agente MAL-DATA nos nós.



(d) ação do agente MAL-ERR nos nós.

Figura 3.1: Ação maliciosa dos nós no roteamento AODV.

A implementação desses ataques requer apenas uma alteração de software no me-

canismo de roteamento de cada nó malicioso, que pode ser feita em qualquer um dos dispositivos móveis. Então pode-se classificar o ataque como feito no nível da camada de rede. Como será visto posteriormente esses ataques têm grande impacto sobre a operação da rede. Outros tipos de ataque, até mais eficientes do ponto de vista dos atacantes, podem ser disparados contra uma rede sem fio no nível do camada física. Porém tais ataques na camada física requerem alterações de hardware e de software específico, o que torna sua implementação mais complexa.

Os ataques implementados são executados separadamente, sendo que em cada simulação um certo número de nós é criado com um dos agentes modificados, sempre do mesmo tipo. O objetivo é avaliar o impacto dos ataques no desempenho da rede em relação ao número de nós maliciosos, ao grau de mobilidade e à carga na rede, utilizando como métrica a taxa total de entrega de pacotes de dados, o atraso médio dos pacotes de dados entregues e a sobrecarga de pacotes de roteamento (número de pacotes de roteamento transmitidos). A partir dessa avaliação deseja-se definir linhas gerais de uma estratégia para minimizar o impacto desses ataques na rede que tenha o mínimo custo de operação, não exigindo muitos recursos da rede.

3.2 Ambiente de Simulação

Utilizou-se para as simulações o *ns-2* (*Network Simulator* 2) [38]. O *ns-2* é um simulador orientado a eventos discretos para serviços e protocolos de rede. Essa ferramenta, amplamente disseminada no âmbito da pesquisa em redes de comunicações, é fruto do projeto VINT (*Virtual InterNet Testbed*), que é uma colaboração entre vários centros de excelência da área.

O simulador *ns-2* permite a configuração dos cenários de simulação em termos da topologia da rede, movimentação dos nós, parâmetros das camadas física e de enlace, filas nas interfaces das camadas, protocolos das camadas e aplicações.

O simulador *ns-2* foi utilizado juntamente com a extensão de mobilidade e redes sem fio desenvolvida pelo *MONARCH - Mobile Networking Architectures Research Group*

[39], que implementa o padrão IEEE 802.11 [40], bem como o protocolo de roteamento AODV e outros.

O padrão para redes sem fio IEEE 802.11 [40] define a camada física (PHY) e subcamada de controle de acesso ao meio (MAC), abrangendo as redes sem fio infra-estruturadas e as redes sem fio ad hoc. Para as redes infra-estruturadas o modo de operação é o PCF (*Point Coordination Function*) e nas redes ad hoc o modo de operação é o DCF (*Distributed Coordination Function*), a diferença entre os modos de operação está em como se dá o acesso ao meio. Com relação a camada física são definidos três padrões de transmissão, espalhamento de espectro por salto em freqüência (FHSS), espalhamento de espectro por seqüência direta (DSSS) e infravermelho.

O cenário de simulação é constituído por uma rede de 60 nós móveis. O modelo de mobilidade dos nós segue o *random waypoint* numa área retangular de 1200m x 500m e velocidade máxima de 20m/s com diferentes tempos de pausa. O raio de alcance dos rádios dos dispositivos é de 250m. O tráfego é composto por pacotes UDP de 512 *bytes* em CBR (*Constant Bit Rate*) com taxa de 4 ou 8 pacotes por segundo sendo 10 ou 30 o número de pares fonte-destino. O tempo de simulação é de 600 segundos. Os valores dos parâmetros assumidos para compor as simulações são baseados em valores recorrentemente encontrados nos outros trabalhos que abordam o tema de roteamento em redes ad hoc. A prática de assumir os mesmos valores para esses parâmetros tem como objetivo permitir uma comparação entre os resultados obtidos.

O padrão de movimentação utilizado segue o modelo *random waypoint* que prevê o posicionamento inicial dos dispositivos aleatoriamente na área especificada obedecendo a uma distribuição uniforme. Então cada móvel sorteia uma posição de destino dentro da área especificada para a simulação e movimenta-se até esse destino em linha reta com uma velocidade constante. A velocidade de deslocamento do móvel é aleatoriamente escolhida seguindo uma distribuição uniforme entre zero e a velocidade máxima especificada. Quando a posição destino é alcançada o móvel pára e espera um tempo de pausa especificado e então inicia outro processo de deslocamento para outro destino com outra velocidade. Este procedimento de movimentação se repete para todos os dispositivos da rede até que seja atingido o tempo final de simulação.

Nessas simulações foram adotados três diferentes tempos de pausa com o objetivo de retratar a rede em diferentes condições de mobilidade dos nós, a saber: 0 segundos, 300 segundos e 600 segundos, sendo o tempo de simulação total de 600 segundos. A tabela abaixo (3.1) resume os parâmetros adotados nas simulações deste trabalho.

Tabela 3.1: Conjunto de parâmetros de simulação.

Parâmetro	Valor
tamanho da rede	60 dispositivos
capacidade	11Mbps
área	1200m x 500m
velocidade máxima	20m/s
alcance do rádio	250m
tamanho do pacote	512 *bytes*
taxa de transferência	4 e 8 pacotes/s
pares fonte-destino	10 e 30
tempo de pausa	0s, 300s e 600s
tempo de simulação	600s

Capítulo 4

Resultados e Análises

Os resultados [41] estão expressos em gráficos (Figuras de 4.1 a 4.18), sendo que cada um deles apresenta 4 curvas referentes aos quatro tipos de ataque (REQ, REP, ERR e DATA). O eixo das abscissas (x) é a porcentagem de nós comprometidos no ataque, o eixo das ordenadas (y) a métrica considerada, a saber: taxa de entrega de pacotes de dados, atraso médio dos pacotes de dados e sobrecarga de pacotes de roteamento.

Como visto anteriormente, o ataque REQ é aquele que tem como alvo as mensagens de pedido de rota (*route request* - RREQ). O ataque REP tem como alvo as mensagens de resposta a pedidos de rota (*route reply* - RREP). O ataque ERR é aquele que tem como alvo as mensagens de erro nas rotas (*route error* - RERR). O ataque DATA tem como alvo os pacotes de dados.

A taxa de entrega de pacotes da rede é soma de todos os pacotes de dados entregues com sucesso nos nós de destino dividida pela soma de todos os pacotes de dados originados pelos nós fonte, expressa em porcentagem. O atraso médio de pacotes é a soma do tempo gasto da geração a entrega bem sucedida de pacotes de dados, dividido pela quantidade desses pacotes. A sobrecarga de roteamento é o número de pacotes de roteamento que trafegaram na rede. As métricas aqui avaliadas também são as comumente encontradas em trabalhos de avaliação de desempenho de redes.

O primeiro conjunto de gráficos (Figuras de 4.1 a 4.9) refere-se a um cenário de tráfego difuso de enlaces menos carregados e conexões mais distribuídas (4 pacotes por

segundo em 30 pares fonte-destino com duração das fontes aleatória menor e no máximo igual ao tempo de simulação).

O segundo conjunto (Figuras de 4.10 a 4.18) refere-se a um tráfego mais concentrado de enlaces mais carregados e conexões menos distribuídas (8 pacotes por segundo em 10 pares fonte -destino com duração das fontes igual ao tempo de simulação).

Em cada conjunto de figuras há três gráficos diferentes para cada métrica analisada. Cada gráfico é referente a um tempo de pausa diferente, sendo esses 0, 600 e 300 segundos, ou seja, movimentação em todo o tempo de simulação, sem movimentação em todo o tempo de simulação e uma quantidade intermediária de movimentação.

Foram calculadas margens de erro com intervalos de confiança de 95% relativos às médias das medidas feitas nas simulações. Estas margens de erro estão expressas nos gráficos obtidos através de barras verticais.

Como esperado pode-se observar que o primeiro ponto dos gráficos ($x = 0$) corresponde à situação onde não há nós maliciosos e portanto não há ataques e sendo assim todas as 4 curvas em todos os gráficos neste ponto são coincidentes, refletindo os valores das métricas analisadas nas condições normais de operação da rede.

Com relação à métrica parcela de pacotes de dados entregues (Figuras 4.1, 4.2, 4.3, 4.10, 4.11 e 4.12) demonstrou-se mais efetivo o ataque direto aos pacotes de dados (ataque DATA) no nível do agente de roteamento, em todos os casos analisados. A variação da carga na rede não introduz mudança significativa no comportamento das curvas, ou seja, no efeito dos ataques, introduzindo apenas uma diferença de nível nas curvas para o ambiente de maior tráfego em todos os ataques. Mas com relação à mobilidade, em ambos os casos de carga, há uma mudança no comportamento das curvas expresso por uma variação significativa no efeito dos ataques à resposta dos pedidos de rota (ataque REP) e à notificação de erro (ataque ERR), com maior visibilidade no ataque ERR, que se torna mais efetivo em ambientes de alta mobilidade.

No que diz respeito à métrica atraso médio dos pacotes de dados entregues (Figuras 4.4, 4.5, 4.6, 4.13, 4.14 e 4.15), uma carga maior na rede varia muito o comportamento das curvas, especialmente em ambientes de alta mobilidade, introduzindo um atraso sig-

nificativo no tempo de chegada dos pacotes. Ao contrário da métrica taxa de entrega, nesta análise o ataque DATA é o menos efetivo em todos os casos. No ambiente de baixa mobilidade a variação no efeito dos diferentes tipos de ataques é mínima. Neste ambiente o ataque REP é ligeiramente mais efetivo. No ambiente de alta mobilidade essa variação no efeito fica bem evidente, onde o ataque aos pedidos de rota (ataque REQ) é o mais efetivo, seguido do ataque REP no ambiente com menos carga na rede e também do ataque ERR na rede mais carregada. Podemos observar um declínio no atraso médio dos pacotes em alguns tipos de ataque que se justifica pela diminuição no número de pacotes de dados entregues em função do ataque em questão.

Com relação à métrica de sobrecarga média de pacotes de roteamento (Figuras 4.7, 4.8, 4.9, 4.16, 4.17 e 4.18) a maior mobilidade na rede aumenta significativamente o número de pacotes de roteamento. A carga mais pesada aumenta o número de pacotes de roteamento no ambiente de alta mobilidade (Figura 4.18), mas diminui no ambiente de baixa mobilidade (Figura 4.16). Isto se deve ao fato de, mesmo com maior tráfego na rede, no ambiente de baixa mobilidade, há menos pacotes de roteamento pois as conexões têm tempos de duração maior e são menos numerosas exigindo menos processos de descoberta e manutenção de rotas. Ao contrário, no ambiente de alta mobilidade ou tráfego com maior número de conexões com duração menor, mais pacotes de roteamento são necessários seja pela necessidade de descobrir rotas para os dados com diferentes destinos ou redescobrir e manter as rotas em função da mobilidade dos nós. Destaca-se o ataque REP como o mais efetivo nos ambientes de menor tráfego seguido de perto pelo ataque ERR nos ambientes de maior tráfego. Deve-se observar a diferença entre as escalas do eixo y das Figuras 4.7 e 4.16 e das Figuras 4.9 e 4.18 que é devido à necessidade de um maior número de pacotes de roteamento nos ambientes de intensa movimentação.

Considerando as observações realizadas, a proposta de um mecanismo de segurança para ataques de não-cooperativismo entre os nós deve considerar a variabilidade do efeito dos ataques nas diferentes configurações da rede segundo as diferentes métricas avaliadas. Os resultados desse trabalho demonstram que qualquer proposta de mecanismo de proteção diferenciada para os pacotes por tipo de ambiente pode ser ineficiente. Proteger um certo tipo de pacote em determinado ambiente não garante melhores valores em todas as métricas e em ambientes com característica de mobilidade ou carga diferentes.

Por outro lado, um esquema de segurança pode se basear na capacidade da interface de rede dos dispositivos móveis poder operar em modo de escuta promíscua, verificando se seus vizinhos estão agindo corretamente na retransmissão de seus pacotes de dados e de roteamento. Quando houver detecção de mau comportamento por um nó, esse adiciona a identificação desse nó mau em uma lista local juntamente com o tipo de comportamento malicioso apresentado e passa a evitar o nó malicioso em suas comunicações. Um mecanismo temporizado tiraria o nó mau da quarentena após um certo tempo, prevendo que o nó comprometido volte a operar normalmente. Pode-se também evitar que a interface do nó opere todo o tempo em escuta promíscua, fazendo apenas uma escuta periódica ou de pacotes que o mecanismo sinalizar com mais importantes. Para diminuir o número de possíveis falso-positivos uma janela de tempo de escuta deve ser feita antes de inserir o nó malicioso em quarentena.

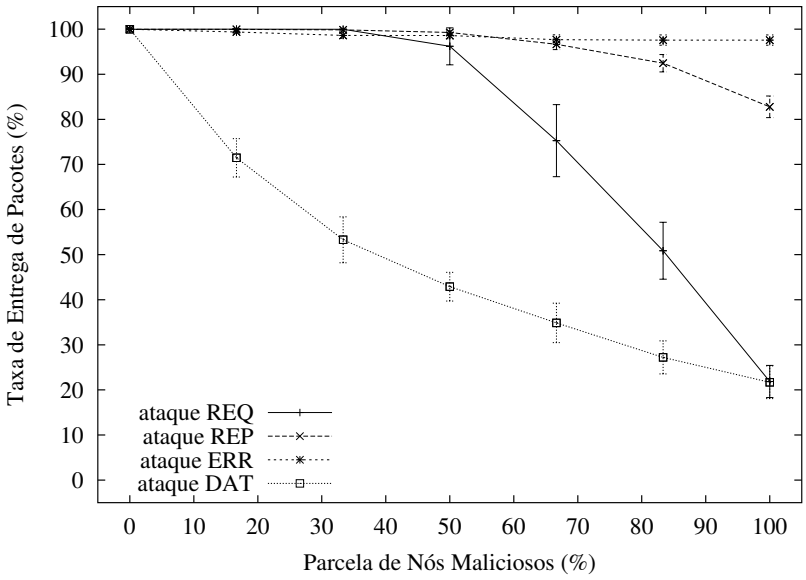


Figura 4.1: Severidade dos ataques para métrica taxa de entrega de pacotes com tempo de pausa de 600s e tráfego de 4 pcts/s em 30 pares fonte-destino.

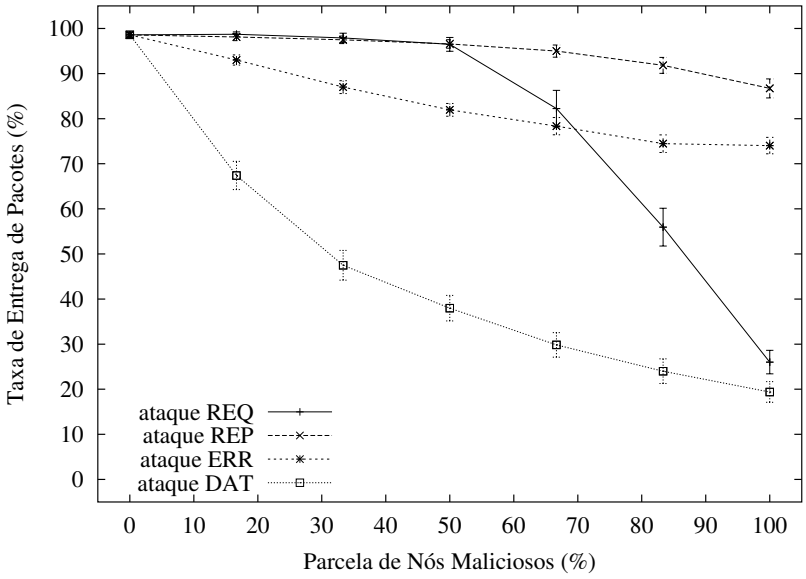


Figura 4.2: Severidade dos ataques para métrica taxa de entrega de pacotes com tempo de pausa de 300s e tráfego de 4 pcts/s em 30 pares fonte-destino.

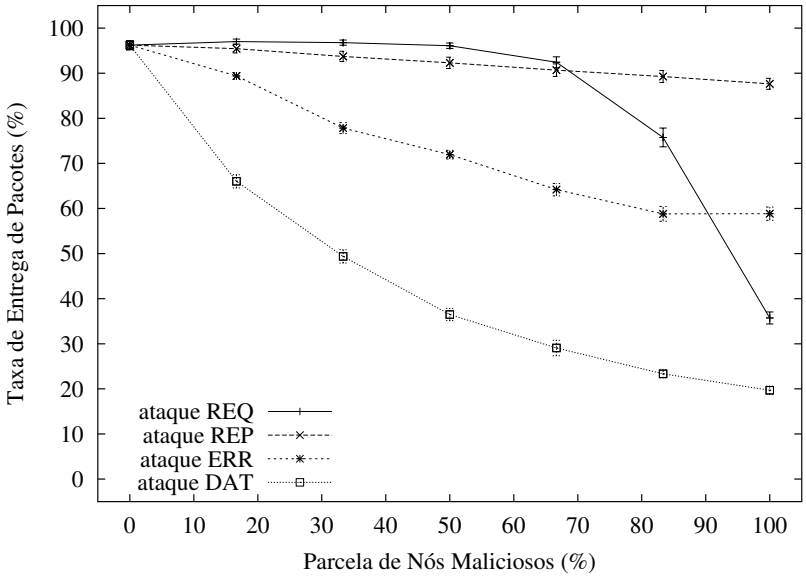


Figura 4.3: Severidade dos ataques para métrica taxa de entrega de pacotes com tempo de pausa de 0s e tráfego de 4 pcts/s em 30 pares fonte-destino.

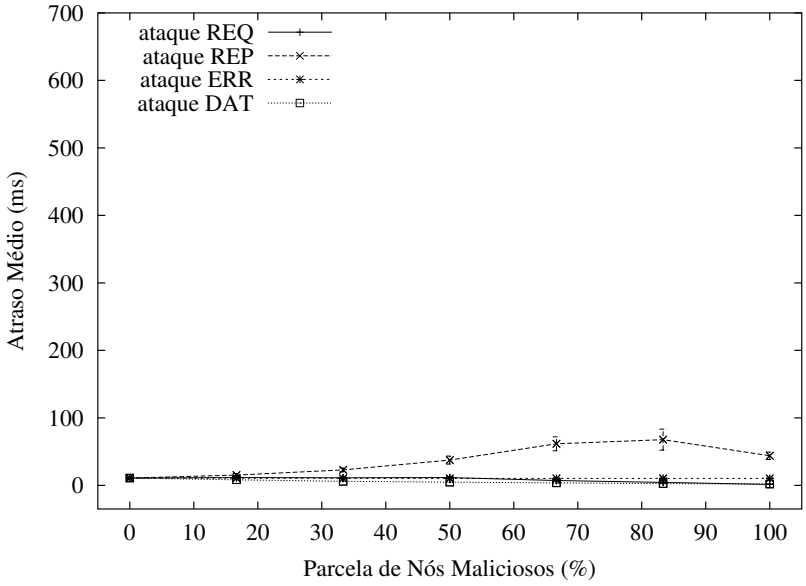


Figura 4.4: Severidade dos ataques para métrica atraso médio de pacotes com tempo de pausa de 600s e tráfego de 4 pcts/s em 30 pares fonte-destino.

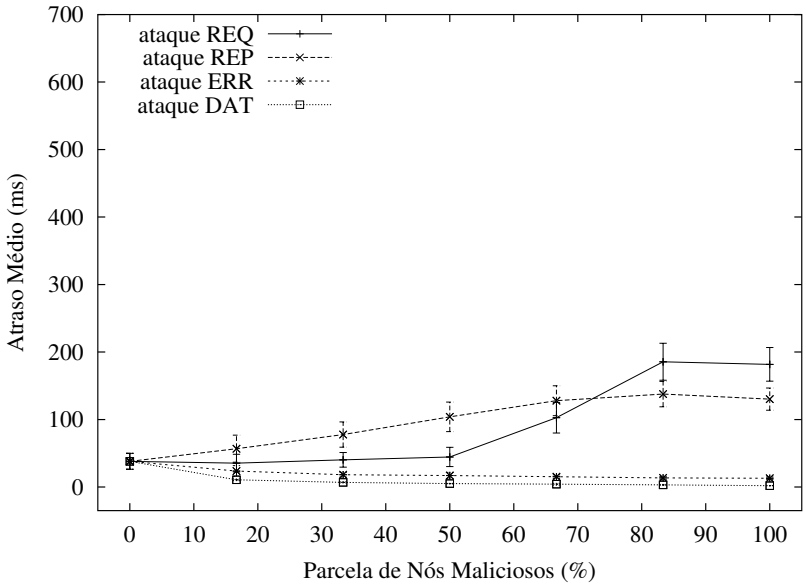


Figura 4.5: Severidade dos ataques para métrica atraso médio de pacotes com tempo de pausa de 300s e tráfego de 4 pcts/s em 30 pares fonte-destino.

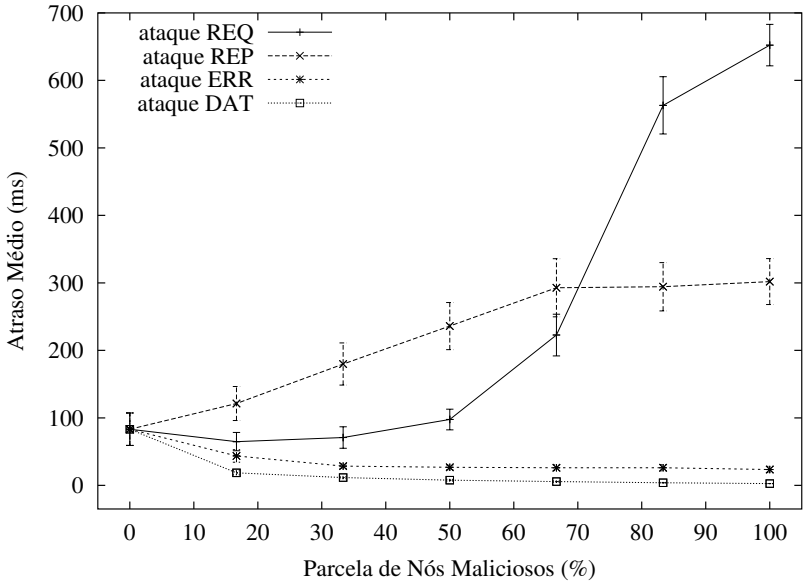


Figura 4.6: Severidade dos ataques para métrica atraso médio de pacotes com tempo de pausa de 0s e tráfego de 4 pcts/s em 30 pares fonte-destino.

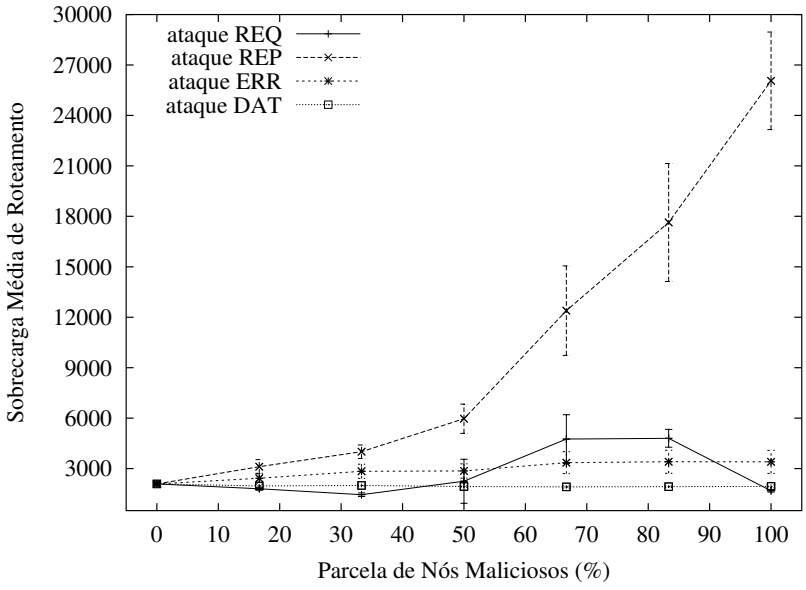


Figura 4.7: Severidade dos ataques para métrica sobrecarga de roteamento com tempo de pausa de 600s e tráfego de 4 pcts/s em 30 pares fonte-destino.

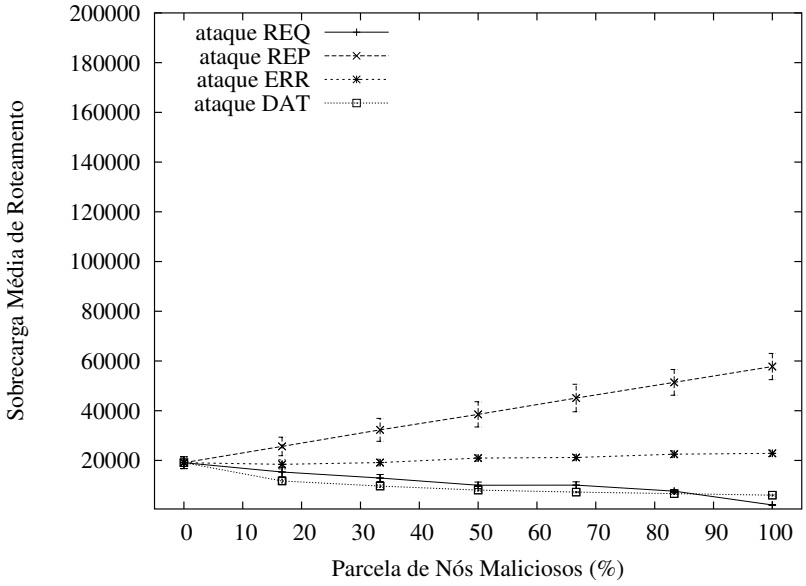


Figura 4.8: Severidade dos ataques para métrica sobrecarga de roteamento com tempo de pausa de 300s e tráfego de 4 pcts/s em 30 pares fonte-destino.

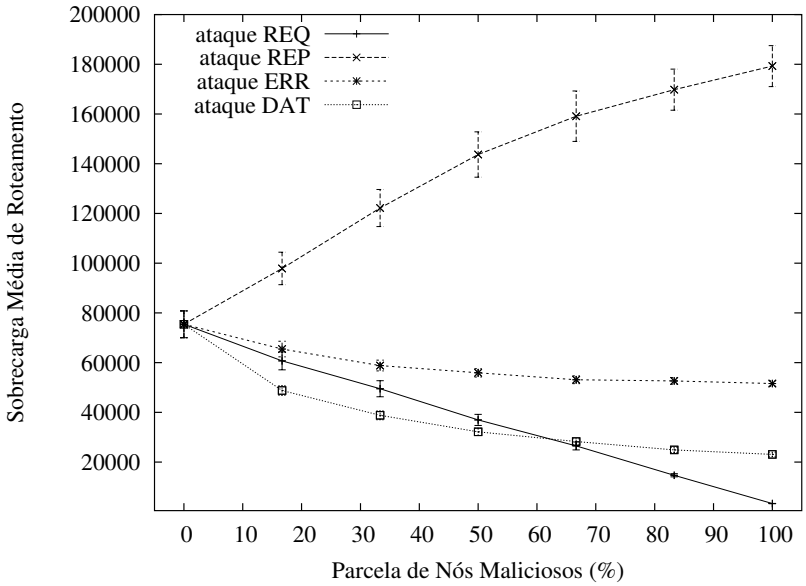


Figura 4.9: Severidade dos ataques para métrica sobrecarga de roteamento com tempo de pausa de 0s e tráfego de 4 pcts/s em 30 pares fonte-destino.

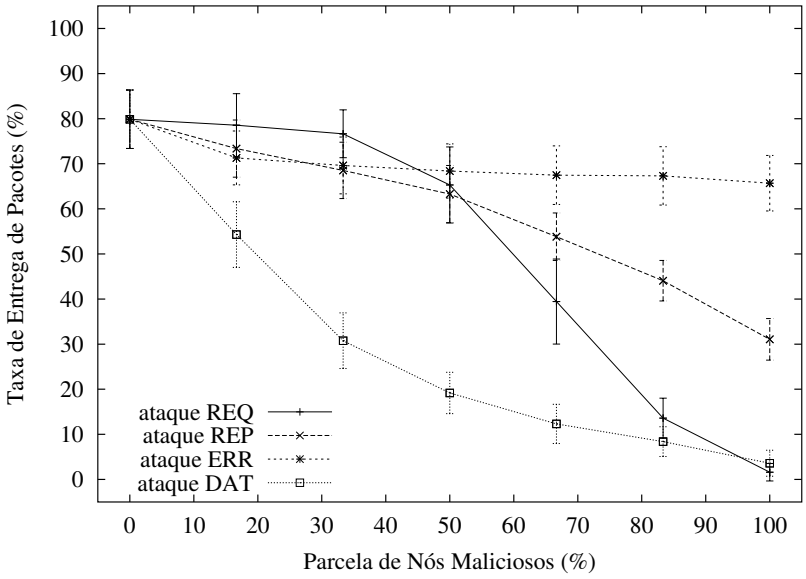


Figura 4.10: Severidade dos ataques para métrica taxa de entrega de pacotes com tempo de pausa de 600s e tráfego de 8 pcts/s em 10 pares fonte-destino.

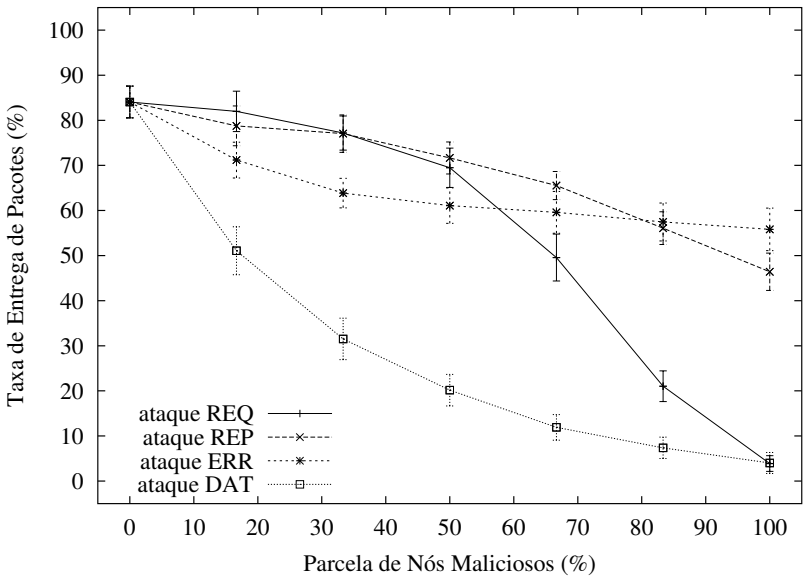


Figura 4.11: Severidade dos ataques para métrica taxa de entrega de pacotes com tempo de pausa de 300s e tráfego de 8 pcts/s em 10 pares fonte-destino.

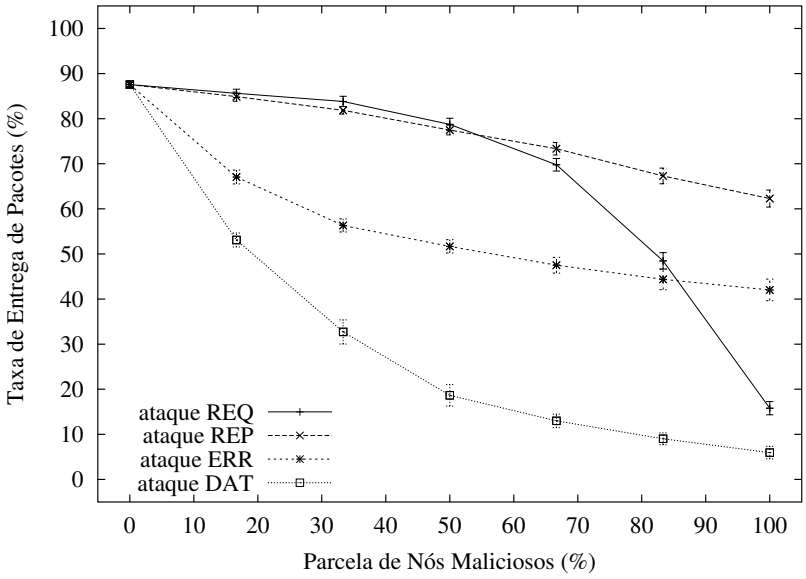


Figura 4.12: Severidade dos ataques para métrica taxa de entrega de pacotes com tempo de pausa de 0s e tráfego de 8 pcts/s em 10 pares fonte-destino.

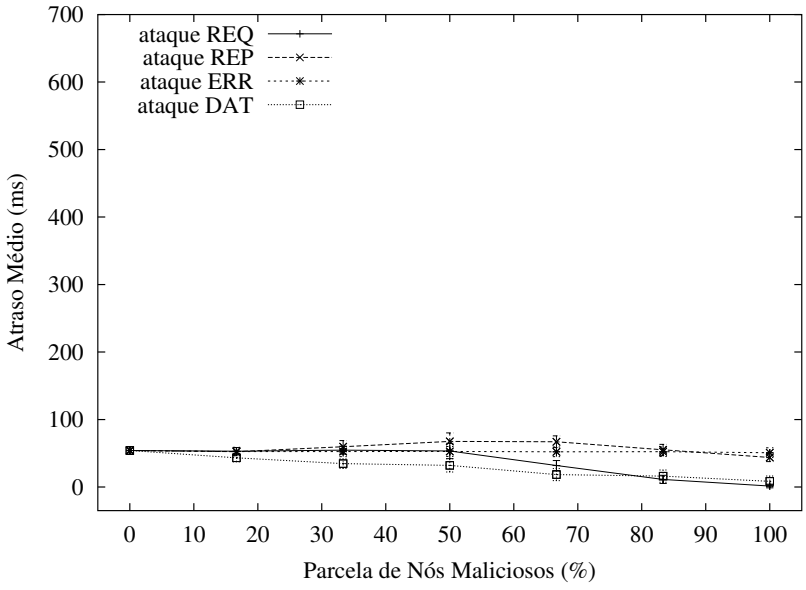


Figura 4.13: Severidade dos ataques para métrica atraso médio de pacotes com tempo de pausa de 600s e tráfego de 8 pcts/s em 10 pares fonte-destino.

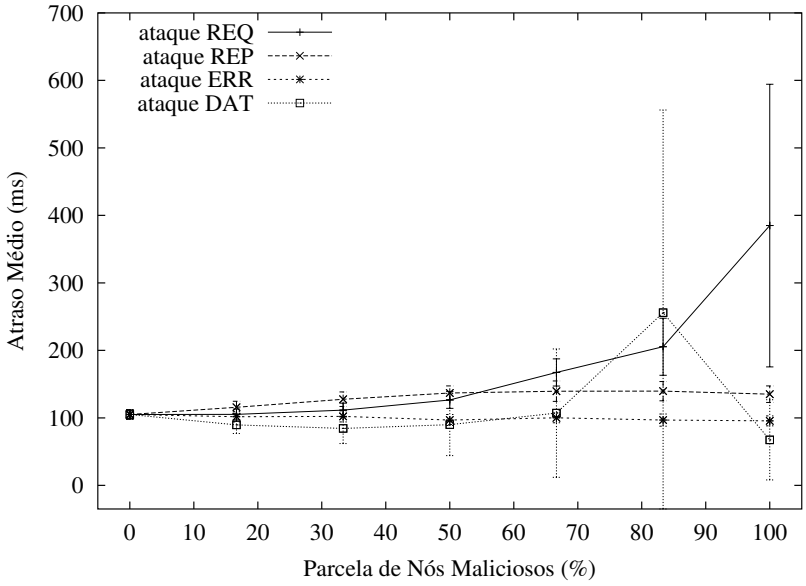


Figura 4.14: Severidade dos ataques para métrica atraso médio de pacotes com tempo de pausa de 300s e tráfego de 8 pcts/s em 10 pares fonte-destino.

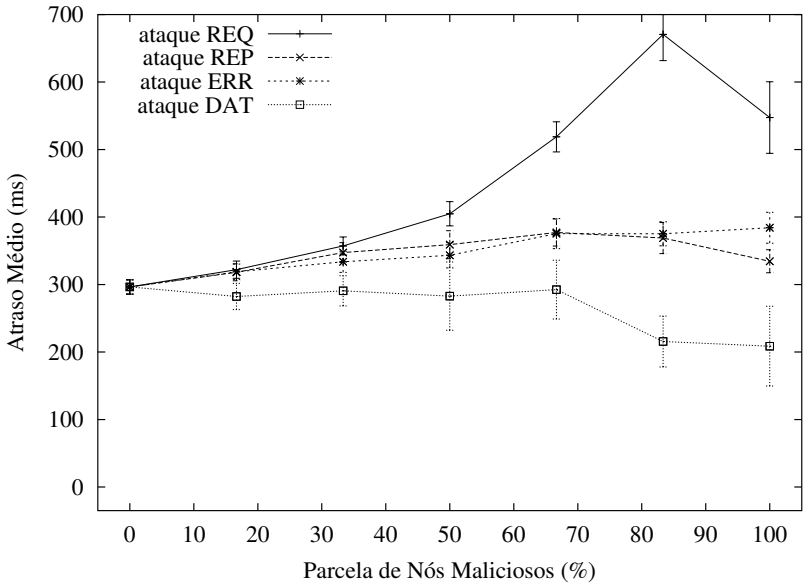


Figura 4.15: Severidade dos ataques para métrica atraso médio de pacotes com tempo de pausa de 0s e tráfego de 8 pcts/s em 10 pares fonte-destino.

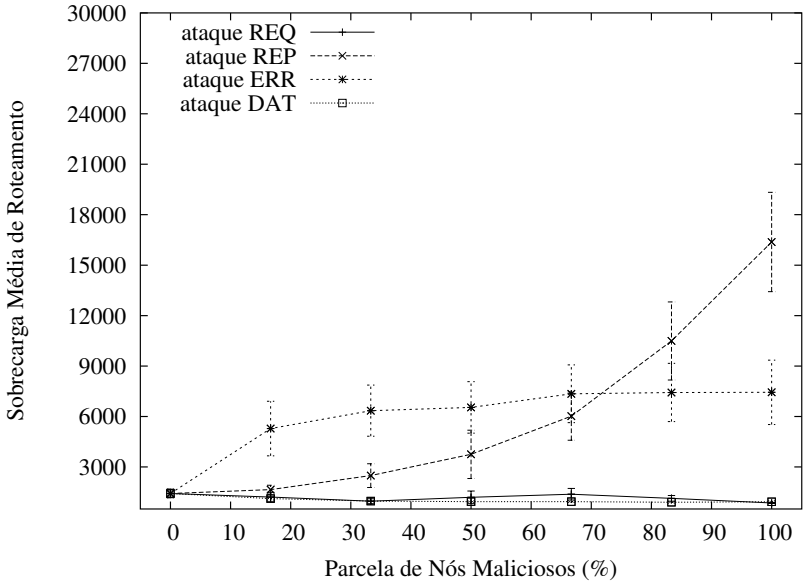


Figura 4.16: Severidade dos ataques para métrica sobrecarga de roteamento com tempo de pausa de 600s e tráfego de 8 pcts/s em 10 pares fonte-destino.

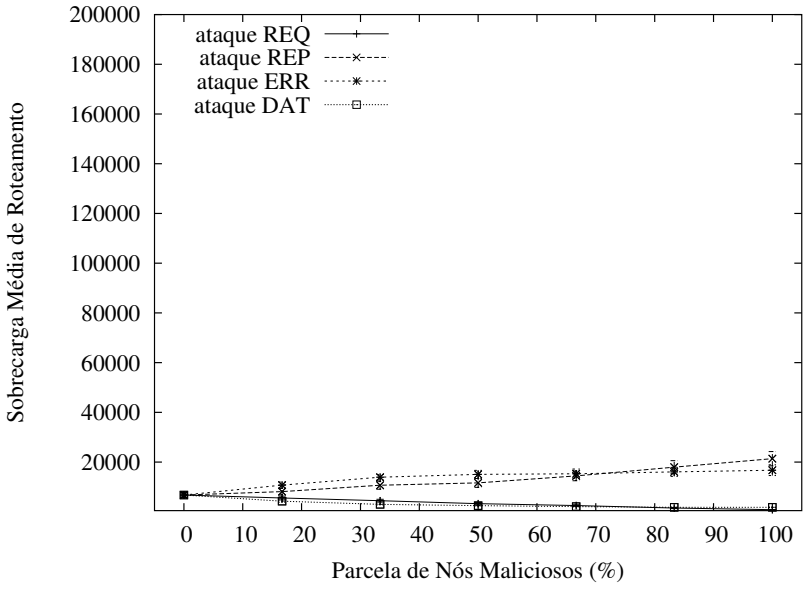


Figura 4.17: Severidade dos ataques para métrica sobrecarga de roteamento com tempo de pausa de 300s e tráfego de 8 pcts/s em 10 pares fonte-destino.

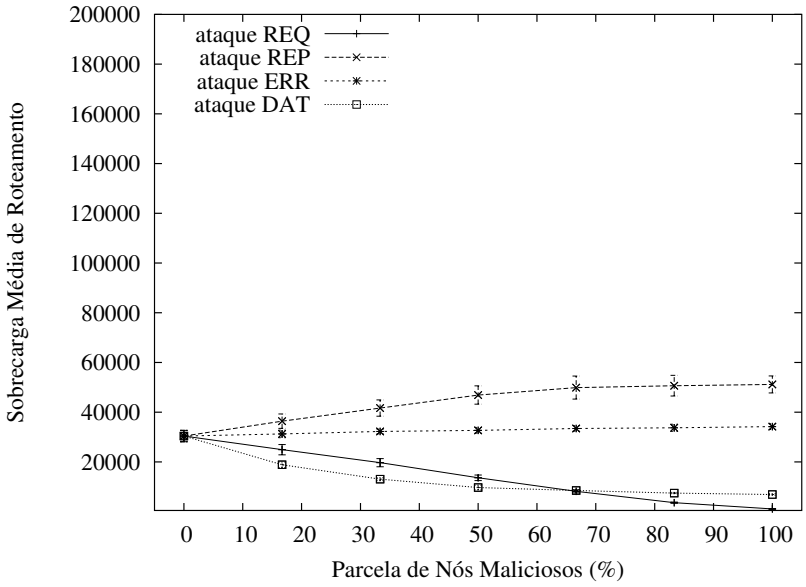


Figura 4.18: Severidade dos ataques para métrica sobrecarga de roteamento com tempo de pausa de 0s e tráfego de 8 pcts/s em 10 pares fonte-destino.

Capítulo 5

Conclusões

AS redes sem fio representam um avanço tecnológico muito significativo na área de sistemas de comunicações. Suas características levaram a seu emprego em diversas setores, permitindo e agilizando a troca de informações entre pessoas e dispositivos. No entanto, a segurança para essa troca de informações é essencial para viabilizar seu emprego em determinadas aplicações. Para se alcançar os níveis de segurança, já atingido pelas redes fixas cabeadas, muito ainda precisa-se evoluir. Daí a importância em abordar tal aspecto e é nesse sentido que se concentram os trabalhos em segurança para redes sem fio.

Maior ainda se torna o desafio de conferir os mesmos níveis de segurança encontrados nas redes tradicionais às redes sem fio se essas forem do tipo ad hoc. A escassez de recursos, como bateria, processamento e banda, aliados a falta de infra-estrutura e constantes mudanças na topologia da rede definem o conjunto de características para as quais os esquemas de segurança estão sendo desenvolvidos e adaptados.

Neste trabalho foi analisado o impacto das ações maliciosas de nós sobre os pacotes de roteamento do protocolo AODV e os pacotes de dados numa rede ad hoc em termos das métricas taxa de entrega de pacotes de dados, atraso médio dos pacotes de dados entregues e sobrecarga de pacotes de roteamento. Essas métricas foram avaliadas em função da carga na rede, da mobilidade dos nós, do tipo de ataque e da densidade de nós comprometidos. O ambiente de simulação juntamente com os modelos de ataque criados

representam situações possíveis de serem encontradas nas aplicações desta tecnologia de comunicação e visa avaliar o emprego dessa tecnologia em ambientes hostis, bem como, esboçar as características desejáveis de um mecanismo de segurança que minimize o efeito desses ataques.

Em um ambiente de intensa movimentação, um ataque de 50% dos nós às mensagens RERR é capaz de baixar a taxa de entrega de aproximadamente 40%, enquanto um ataque visando as mensagens RREQ e RREP baixa a taxa apenas de 5%. Independentemente da movimentação, se o alvo for os pacotes de dados, o mesmo número de atacantes baixa em média 50% a taxa de entrega. Considerando o atraso na entrega dos pacotes, no ambiente de forte movimentação, ataques de pouco mais da metade dos nós às mensagens RREP podem triplicar o atraso ou aumentá-lo em 50% no caso de ataques às mensagens RREQ. Com relação à sobrecarga de roteamento, é possível dobrar o número de pacotes de roteamento com menos da metade dos nós comprometidos num ataque às mensagens RERR no cenário com mais carga e num ataque às mensagens RREP no cenário com menos carga, ambos em ambientes de baixa movimentação. Alguns resultados aqui obtidos vão contra outros trabalhos que não consideravam as mensagens de erros como potenciais fontes de ataques e que aqui provaram ter efeito bastante significativo no desempenho da rede quando são alvos de ataques.

Baseando-se nos resultados obtidos, fica demonstrada a necessidade de mecanismos capazes de impedir ou minimizar o comportamento não-cooperativo entre os nós da rede com relação às mensagens de roteamento e aos pacotes de dados. Devido à variabilidade da eficácia dos diferentes tipos de ataques nas diversas situações avaliadas, não seria eficiente um mecanismo de proteção diferenciada para cada tipo de pacote em cada tipo de ambiente, embora essa abordagem possa parecer menos custosa para a rede. Logo, um mecanismo que atue sobre todos os pacotes no nível do agente de roteamento é mais robusto e flexível para agir adequadamente em qualquer ambiente sob qualquer ataque. Este mecanismo pode se utilizar de um esquema que não crie mensagens extras na rede para sinalizar os ataques podendo apenas gerenciá-los localmente, evitando o desperdício de recursos e a degradação do desempenho da rede.

A estratégia a ser seguida para implementação deste mecanismo de segurança deve

fazer uso da escuta promíscua que as interfaces de rede podem proporcionar aos nós da rede. Com a escuta promíscua os nós poderão verificar e classificar sua vizinhança com relação a retransmissão de seus pacotes de dados e roteamento. A partir dessa classificação, que detectará o mau comportamento de possíveis nós atacantes, os nós podem estabelecer uma lista de nós vizinhos suspeitos. Se for observado que o nó vizinho em questão apresenta o comportamento malicioso recorrentemente, o nó classificador poderá colocá-lo numa espécie de quarentena e não mais utilizá-lo com rota de saída para outros destinos. O nó classificador também poderá sinalizar para seus outros vizinhos a entrada daquela vizinho em quarentena. Também será gerado um pacote RERR para os nós que tentarem encaminhar pacotes através do nó malicioso. Para evitar problemas de falso - positivos a escuta promíscua e a entrada e saída de nós da quarentena estariam associadas a janelas de tempo. Esses mecanismos temporizados evitariam punir nós que apresentarem falhas não intencionais temporárias. Essa estratégia de minimização dos efeitos das ações maliciosas de alguns nós geraria baixa sobrecarga e pequeno consumo de recursos da rede, pois tenta tratar localmente as adversidades, e por fim melhoraria o desempenho da rede.

Este novo mecanismo de segurança para ataques de não-cooperativismo entre os nós deve ser compatível com as restrições encontradas na rede, principalmente a escassez de banda, de energia e da capacidade de processamento do dispositivo móvel e ainda operar conjuntamente com os mecanismos baseados em assinaturas digitais que garantem a integridade dos pacotes que circulam na rede. Sendo assim, torna-se necessário um estudo sobre a implementação dessa proposta, avaliando sua eficiência e seu impacto sobre o funcionamento da rede. O mecanismo de segurança, apesar do consumo de recursos que ele venha obrigatoriamente a fazer, deve proporcionar a rede um desempenho superior aquele obtido quando a rede encontra-se sob ataque, a fim de justificar seu emprego.

Como trabalhos futuros ficam a implementação e análise de desempenho da estratégia aqui apresentada, visando ajustar e descobrir os melhores parâmetros a serem empregados nessa solução.

Embora muitas propostas de mecanismos de segurança sem fio ad hoc tenham sido apresentadas na literatura nenhuma abrange todas as vulnerabilidades que podem ser ex-

ploradas ou tem o desempenho desejável. As melhorias gradativamente alcançadas nos hardwares e softwares desse dispositivos móveis estarão permitindo cada vez mais soluções de segurança mais robustas sem causar impacto significativo no desempenho da rede e com cada vez mais transparência para o usuário.

Referências Bibliográficas

[1] ANTON, E. R. Análise de desempenho de protocolos para estabelecimento de chave de grupo em redes ad hoc. Tese de Mestrado, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil, 2003.

[2] HAAS, Z. J., E ZHOU, L. Securing ad hoc networks. *IEEE Network Magazine 13*, 6 (novembro/dezembro de 1999), 24–30.

[3] PERKINS, C. E., BELDING-ROYER, E. M., E DAS, S. R. *Ad Hoc On-Demand Distance Vector (AODV) Routing*, julho de 2003. IETF RFC 3561.

[4] CORSON, S., E MACKER, J. *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*, janeiro de 1999. IETF RFC 2501.

[5] SCHILLER, J. H. *Mobile Communications*. Addison-Wesley, 2000.

[6] VENKATRAMAN, L., E AGRAWAL, D. P. Strategies for enhancing routing security in protocols for mobile ad hoc networks. *Journal of Parallel and Distributed Computing 63*, 2 (fevereiro de 2003), 214–227.

[7] ROCHA, L. G. S., E DUARTE, O. C. M. B. Aspectos e mecanismos de segurança em redes ad hoc. In *Workshop em Qualidade de Serviço, Segurança, Mobilidade e Aplicações - WQoSM* (novembro de 2002).

[8] ROYER, E. M., E TOH, C. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications 6*, 2 (abril de 1999), 46–55.

[9] PERKINS, C., E BHAGWAT, P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications* (agosto de 1994), pp. 234–244.

[10] WANG, W., LU, Y., E BHARGAVA, B. K. On security study of two distance vector routing protocols or mobile ad hoc networks. In *IEEE International Conference on Pervasive Computing and Communications - PerCom* (março de 2003), pp. 179–190.

[11] CLAUSEN, T., E JACQUET, P. *Optimized Link State Routing Protocol (OLSR)*, outubro de 2003. IETF RFC 3626.

[12] JOHNSON, D. B., E MALTZ, D. A. E. *The Dynamic Source Routing protocol for mobile ad hoc networks*, 2002. Internet Draft, draft-ietf-manet-dsr-06.txt.

[13] PERKINS, C. E., ROYER, E. M., DAS, S. R., E MARINA, M. K. Performance comparison of two on-demand routing protocols for ad hoc networks. *IEEE Personal Communications 8*, 1 (fevereiro de 2001), 16–28.

[14] ZAPATA, M. G. *Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing*, agosto de 2001. Internet Draft, draft-guerrero-manet-saodv-00.txt.

[15] KENT, S. *IP Authentication Header (AH)*, março de 2004. Internet Draft, draft-ietf-ipsec-rfc2402bis-07.txt.

[16] DENG, H., LI, W., E AGRAWAL, D. P. Routing security in wireless ad hoc networks. *IEEE Communications Magazine 40*, 10 (outubro de 2002), 70–75.

[17] VANHALA, A. Security in ad hoc networks. Relatório técnico, Department of Computer Science, University of Helsinki, 2000.

[18] KARPIJOKI, V. Security in ad hoc networks. Relatório técnico, Department of Computer Science, Helsinki University of Technology, 2001.

[19] PEREIRA, I. C. M. Análise do roteamento em redes móveis ad hoc em cenários de operações militares. Tese de Mestrado, COPPE/UFRJ, Rio de Janeiro, RJ, Brasil, 2004.

[20] HUBAUX, J., BUTTYAN, L., E CAPKUN, S. The quest for security in mobile ad hoc networks. In *ACM International Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc* (outubro de 2001).

[21] MARTI, S., GIULI, T. J., LAI, K., E BAKER, M. Mitigating routing misbehaviour in mobile ad hoc. In *IEEE/ACM International Conference on Mobile Computing and Networking* (agosto de 2000), pp. 255–265.

[22] XUE, Y., E NAHRSTEDT, K. Bypassing misbehaving nodes in ad hoc routing. Relatório técnico, Department of Computer Science, University of Illinois at Urbana-Champaign, 2003.

[23] NING, P., E SUN, K. How to misuse AODV: A case study of insider attacks against modile ad hoc routing protocols. Relatório técnico, Computer Science Department, North Carolina State University, 2003.

[24] PAPADIMITRATOS, P., E HAAS, Z. *The Secure Routing Protocol (SRP) for Ad Hoc Networks*, dezembro de 2002. Internet Draft, draft-papadimitratos-secure-routing-protocol-00.txt.

[25] PAPADIMITRATOS, P., E HAAS, Z. J. Secure routing for mobile ad hoc networks. In *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference - CNDS* (janeiro de 2002).

[26] PAPADIMITRATOS, P., E HAAS, Z. J. Secure data transmission in mobile ad hoc networks. In *ACM Workshop on Wireless Security - WiSe* (setembro de 2003).

[27] AWERBUCH, B., HOLMER, D., NITA-ROTARU, C., E RUBENS, H. An on-demand secure routing protocol resilient to byzantine failures. In *ACM Workshop on Wireless Security - WiSe* (setembro de 2002), pp. 21–30.

[28] HU, Y.-C., JOHNSON, D. B., E PERRIG, A. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks 1*, 1 (julho de 2003), 175–192.

[29] HU, Y.-C., PERRIG, A., E JOHNSON, D. B. Ariadne: a secure on-demand routing protocol for ad hoc networks. In *ACM International Conference on Mobile Computing and Networking - MobiCom* (setembro de 2002), pp. 12–23.

[30] SANZGIRI, K., DAHILL, B., LEVINE, B. N., SHIELDS, C., E BELDING-ROYER, E. M. A secure routing protocol for ad hoc networks. In *IEEE International Conference on Network Protocols - ICNP* (novembro de 2002), pp. 78–88.

[31] RIVEST, R. L., SHAMIR, A., E ADLEMAN, L. M. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM 21*, 2 (julho de 1978), 120–126.

[32] SHEU, J.-P., CHAO, C.-M., E SUN, C.-W. A clock synchronization algorithm for multi-hop wireless ad hoc networks. In *International Conference on Distributed Computing Systems - ICDCS* (março de 2004), pp. 574–581.

[33] MEIER, L., BLUM, P., E THIELE, L. Internal synchronization of drift-constraint clocks in ad hoc sensor networks. In *ACM International Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc* (maio de 2004), pp. 90–97.

[34] RIVEST, R. *The MD5 message-digest algorithm*, abril de 1992. IETF RFC 1321.

[35] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - (NIST). *Secure hash standard*, maio de 1993. Federal Information Processing Standards - (FIPS), Publication 180-1.

[36] GUERRERO, M., E ASOKAN, N. Securing ad hoc routing protocols. In *ACM Workshop on Wireless Security (WiSe) in conjunction with MobiCom* (setembro de 2002), pp. 1–10.

[37] ROCHA, L. G. S., COSTA, L. H. M. K., E DUARTE, O. C. M. B. Avaliação do impacto da ação maliciosa de nós no roteamento em redes ad hoc. In *Workshop em Segurança de Sistemas Computacionais - WSeg* (maio de 2003), pp. 69–76.

[38] FALL, K., E VARADHAN, K. *ns Notes and Documentation*. UC Berkeley, LBL, USC/ISI, and Xerox PARC (The VINT Project), 2002. `http://www.isi.edu/nsnam/ns/ns-documentation.html`.

[39] MONARCH PROJECT. *The Rice Monarch Project – Wireless and Mobility Extensions to ns-2*, novembro de 2000. `http://www.monarch.cs.rice.edu/cmu-ns.html`.

[40] IEEE. *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications - Part II*. Standart IEEE 802.11, 1999. `http://standarts.ieee.org/getieee802/802.11.html`.

[41] ROCHA, L. G. S., COSTA, L. H. M. K., E DUARTE, O. C. M. B. Analyzing the impact of misbehaving nodes in ad hoc routing. In *IEEE Latin American Network Operations and Management Symposium - LANOMS* (setembro de 2003), pp. 5–12.