Avaliação do Impacto da Ação Maliciosa de Nós no Roteamento em Redes Ad Hoc *

Luiz Gustavo S. Rocha , Luís Henrique M. K. Costa , Otto Carlos M. B. Duarte

[1] Grupo de Teleinformática e Automação
COPPE/EE – Programa de Engenharia Elétrica
Universidade Federal do Rio de Janeiro
`http://www.gta.ufrj.br/`

{lgrocha,luish,otto}@gta.ufrj.br

Abstract. *Meeting security requirements is essential to spread the use of ad hoc networks in hostile environment applications. This paper analyzes attacks that exploit the vulnerabilities of the ad hoc routing mechanisms. The attacks are based on the malicious behavior of some network nodes, regarding the forwarding of control messages. AODV is the routing protocol studied. AODV is a reactive protocol where each node act as a router and routes are setup on demand, therefore the malicious behavior of some nodes may affect the whole network performance. The paper presents the results of the malicious nodes' action and identifies the most sensitive attack points that degrade the total network performance regarding the data packet delivery rate.*

Resumo. *O atendimento aos requisitos de segurança é essencial para disseminar o emprego das redes ad hoc nas aplicações em ambientes hostis. Este artigo trata de ataques às vulnerabilidades do mecanismo de roteamento em redes ad hoc. Os ataques são baseados no comportamento malicioso de nós integrantes da rede em relação às mensagens de controle. O AODV é o protocolo de roteamento estudado. O AODV é um protocolo reativo onde cada nó age como roteador e as rotas são constituídas sob demanda, sendo assim o comportamento malicioso de alguns nós pode afetar o desempenho de toda a rede. O artigo apresenta os resultados da ação desses nós e identifica os pontos mais sensíveis aos ataques que degradam o desempenho global da rede em termos da taxa de entrega de pacotes de dados.*

1. Introdução

A cada ano percebe-se um aumento no emprego das tecnologias de comunicação sem fio para as mais diversas finalidades. A vantagem básica destas tecnologias é a eliminação de cabos tornando o dispositivo móvel, mas ainda existem limitações operacionais, como o alcance de rádio e a alimentação do dispositivo. Além das restrições físicas, o fator segurança pode limitar o uso das MANETs (*Mobile Ad hoc Networks*) em aplicações que envolvam risco de ataques contra a sua operação.

*Este trabalho foi realizado com recursos da CAPES, CNPq, FAPERJ, COFECUB e FUJB.

A segurança é uma característica fundamental para viabilizar a expansão e a consolidação do leque de aplicações das redes *ad hoc*. Para tanto são necessários mecanismos que impeçam a ação de nós com comportamento malicioso que intentam atacar a rede das diversas maneiras atualmente possíveis. As vulnerabilidades dos mecanismos básicos de operação constituem uma boa oportunidade de interferir na rede através da inserção, modificação ou eliminação de informações, como por exemplo, do roteamento. Nas redes *ad hoc* todos os nós atuam como roteadores, diferentemente do que acontece nas redes tradicionais, o que torna o mecanismo de roteamento mais vulnerável a falhas e a ataques. Daí a importância de se avaliar o funcionamento de protocolos de roteamento sob condições adversas de operação. Além disso, a operação de modo reativo dos protocolos de roteamento é uma novidade e portanto as vulnerabilidades e mecanismos de segurança para tais contextos devem ser melhor investigados.

Este artigo visa quantificar os efeitos de ataques ao protocolo de roteamento de uma rede *ad hoc* na forma de mau comportamento dos nós da rede com relação às mensagens de roteamento, tomando-se como exemplo o protocolo AODV. Esses ataques têm o objetivo de, minando o roteamento, prejudicar a operação da rede. A partir das avaliações do impacto dos tipos de ataques pode-se elaborar uma estratégia de minimizar a degradação de desempenho da rede tornando-a assim mais robusta contra o comportamento inadequado de alguns dos nós.

Este artigo é organizado da seguinte forma. Na Seção 2 são explicitadas as características do roteamento em redes *ad hoc* e em especial as do protocolo AODV. A Seção 3 descreve alguns aspectos de segurança em termos de vulnerabilidades e ataques às rede *ad hoc*. São apresentados na Seção 4 os detalhes do ambiente de simulação criado para a proposta de avaliação e as análises dos resultados obtidos. Por fim, na Seção 5 são apresentadas as conclusões deste trabalho e as possibilidades de trabalhos futuros.

2. Roteamento em Redes Ad Hoc

As redes *ad hoc*, que por definição não possuem qualquer tipo de infra-estrutura, necessitam portanto de um esquema de encaminhamento de informações que seja adequado à conectividade através de múltiplos saltos e à freqüente mudança na topologia. Além disso, numa rede *ad hoc* todos os nós participam das ações de roteamento [Corson and Macker, 1999]. Há dois tipos de protocolos de roteamento *ad hoc*, reativos (*on-demand*) e pró-ativos (*table-driven*) [Royer and Toh, 1999].

A modelagem pró-ativa é a utilizada nas redes fixas tradicionais e que posteriormente foi adaptada para o ambiente sem fio. Os protocolos de roteamento pró-ativos agem mantendo, em cada nó, informações atualizadas da rota para se chegar a todos os outros nós da rede. Estas informações são armazenadas em tabelas nos nós que constituem a rede. A maneira como são formadas, atualizadas e o número de entradas nestas tabelas de roteamento variam e dão origem aos diversos tipos de protocolos pró-ativos, cada um com uma característica peculiar. Um exemplo é o DSDV (*Destination-Sequenced Distance-Vector*) [Perkins and Bhagwat, 1994], um mecanismo de roteamento pró-ativo baseado no algoritmo clássico de Bellman-Ford. O DSDV serve de base de funcionamento para uma série de outros protocolos [Royer and Toh, 1999].

A outra abordagem, reativa, age criando rotas somente quando necessário. As rotas são solicitadas pelos nós de origem, por isto é também referenciada como *source-initiated*. O processo de descoberta de rotas na rede é iniciado sob demanda. Em seguida, o procedimento de manutenção da rota é feito até que esta não seja mais necessária, ou que o destino se torne inalcançável por alguma falha no caminho. Os processos de descoberta e manutenção das rotas diferenciam os vários protocolos de roteamento reativos. A modelagem reativa é uma novidade nas redes *ad hoc* que foi motivada pelas suas características de mobilidade e escassez de recursos (bateria, memória e banda passante) nos nós. Um exemplo é o AODV (*Ad Hoc On-Demand Distance Vector*) [Perkins et al., 2002] [Perkins et al., 2001]. O AODV foi escolhido para este trabalho por ser um dos mais difundidos e estudados na literatura. O AODV encontra-se atualmente em fase de padronização no grupo de trabalho MANET do IETF (*Internet Engineering Task Force*) [Perkins et al., 2002].

2.1. Protocolo de Roteamento AODV

Quando um nó deseja se comunicar com outro nó numa rede operada com AODV, dá-se início ao processo de descoberta de rotas com a inundação de pacotes de pedidos de rota (*route request* - RREQ). Estes pacotes são retransmitidos em *broadcast* por todos os nós da rede. Quando o nó destino, ou um nó que conhece uma rota para o destino, recebe o pedido, esse envia um pacote de resposta (*route reply* - RREP), que é transmitido em *unicast* pelo caminho reverso ao seguido pelo pedido. As falhas são relatadas através da transmissão de pacotes de erro de rota (*route error* - RERR).

As rotas descobertas são mantidas em tabelas de roteamento tradicionais de uma entrada por destino, apenas as rotas em uso são armazenadas. Os números de seqüência, que cada pacote de roteamento carrega e que são mantidos em cada destino, servem para determinar a rota mais atual e evitar *loops*. Além disso um mecanismo de *soft state* faz a expiração das rotas não utilizadas recentemente.

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 maneira análoga, a transmissão de pacotes RREP, que utiliza a rota reversa do pedido, pelo nó destino ou por outro com rota suficientemente atualizada para o destino, 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 pode então iniciar um novo processo de descoberta de rota.

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 da rede. O uso do *hello* é previsto na especificação, mas pode ser dispensado no caso da camada MAC fornecer esta funcionalidade. Mais detalhes sobre o protocolo de roteamento AODV podem ser vistos em [Royer and Toh, 1999], [Perkins et al., 2001] e em [Perkins et al., 2002].

3. Segurança em Redes Ad Hoc

Os requisitos de segurança de redes *ad hoc* estão intrinsecamente ligados ao tipo de cenário de aplicação da tecnologia [Vanhala, 2000, Kärpijoki, 2001]. Cabe ressaltar que os mecanismos de segurança 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 [Hubaux et al., 2001]. As idéias para esses mecanismos para redes *ad hoc* descendem das abordagens tradicionais dos problemas de segurança das redes de comunicação convencionais. Portanto, ainda se fazem presentes as idéias de protocolos de autenticação, assinaturas digitais, chaves criptográficas e outras [Haas and Zhou, 1999].

Pode-se distinguir essencialmente dois grandes conjuntos de vulnerabilidades, vulnerabilidades dos mecanismos básicos e vulnerabilidades dos mecanismos de segurança [Hubaux et al., 2001]. A primeira pode ser tratada 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 [Marti et al., 2000]. A segunda diz respeito as falhas nos próprios mecanismos que deveriam proteger a rede das ameaças, que podem ser, por exemplo, a quebra de uma chave criptográfica ou um erro num protocolo de autenticação [Kärpijoki, 2001].

Os ataques podem ser classificados como ativos ou passivos e internos ou externos [Kärpijoki, 2001]. Tais ataques visam basicamente a descoberta de informações antes inacessíveis e 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 da rede, podendo inclusive vários destes nós comprometidos operarem em grupo. 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 de operação não intencional [Deng et al., 2002] ou em ações maliciosas por parte de elementos da rede [Vanhala, 2000, Hubaux et al., 2001].

Este trabalho modela e analisa um ataque passivo, interno e em grupo montado contra uma rede operando com roteamento AODV. Essa ameaça é especialmente efetiva num ambiente distribuído, como em uma rede *ad hoc*, onde todos os nós cooperam agindo como roteadores. Sendo o mecanismo de roteamento básico para a operação da rede, ações maliciosas no roteamento podem até constituir um DoS (*Denial of Service attack*), revelando a importância de trabalhos como este. Análise semelhante para o protocolo DSR pode ser encontrada em [Marti et al., 2000].

4. Simulação e Resultados

Foi utilizado o simulador *ns-2* versão *2.1b9a*, amplamente difundido no meio da pesquisa em redes, juntamente com a extensão de mobilidade e redes sem fio desenvolvida pelo *Monarch Research Group* que modela o padrão IEEE 802.11 nas camadas física, enlace e MAC no modo DCF (*Distributed Coordination Function*) e o protocolo de roteamento

AODV, entre outros.

O cenário de simulação possui uma rede formada por 60 nós móveis. O modelo de mobilidade dos nós segue o *random waypoint* numa área retangular de 1200m x 500m e velocidade média 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 de 512 *bytes* em CBR (*Constant Bit Rate*) com taxa de 4 pacotes por segundo sendo 30 o número de pares fonte/destino.

O ambiente descrito acima, semelhante ao utilizado em [Perkins et al., 2001] para comparação de desempenho, visa representar as situações reais que possam ocorrer na utilização das redes *ad hoc* e se soma ao modelo de ataque ao funcionamento da rede que se propõe avaliar. O ataque ao roteamento de uma rede *ad hoc* pode se dar apenas pelo mau comportamento dos nós em relação às mensagens de roteamento e tem por objetivo degradar, ou até impedir, a entrega dos pacotes de dados. O ataque parte da ação não colaborativa de nós maliciosos com relação às mensagens 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 três tipos de mensagens do roteamento AODV.

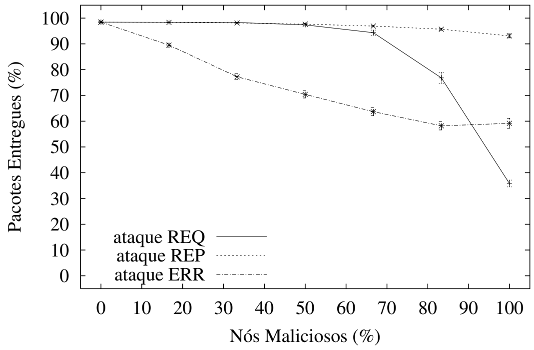
O ataque às mensagens de *route error* (ataque ERR) é implementado pelo agente MAL-ERR que verifica nos nós onde está atuando o recebimento de pacotes RERR e não os repassam aos nós antecessores como deveria em seu funcionamento normal. O comportamento não colaborativo (ataque REP) em relação às mensagens *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, mas no recebimento 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 de forma a não propagar e responder pedidos de rota, a não ser pedidos próprios, agindo assim de forma não colaborativa também.

Os ataques são executados separadamente, sendo que em cada simulação um certo número de nós é criado com um dos agentes modificados. O objetivo é, representando um ambiente perfeitamente factível, avaliar a efetividade dos ataques em relação ao número de nós maliciosos e ao grau de mobilidade na rede, utilizando como métrica a taxa total de entrega de pacotes de dados na rede.

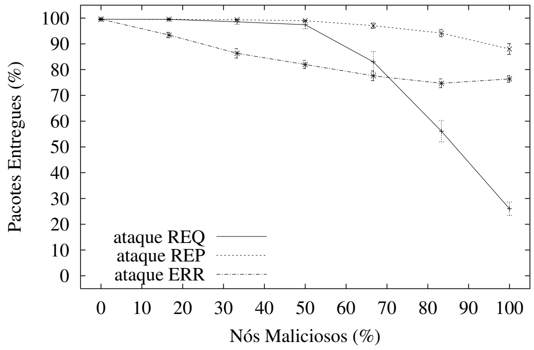
Os resultados estão expressos na forma de três gráficos (Figuras 1(a), 1(b) e 1(c)), sendo que cada um deles apresenta três curvas referentes aos três tipos de ataque (REQ, REP e ERR). O eixo das abscissas (x) é a porcentagem de nós comprometidos no ataque, o das ordenadas (y) a porcentagem de pacotes de dados entregues. Cada gráfico é para um tempo de pausa diferente (0, 300 e 600 segundos) dentro do tempo de simulação total de 600s. O erro médio dos pontos nos três gráficos é de 1,15% com desvio padrão de 1,55.

Numa observação mais geral, comprova-se que o grau de mobilidade influencia e até muda o comportamento das três curvas dos três gráficos, ou seja, o efeito dos diferentes tipos de ataque varia de acordo com a mobilidade dos nós na rede.

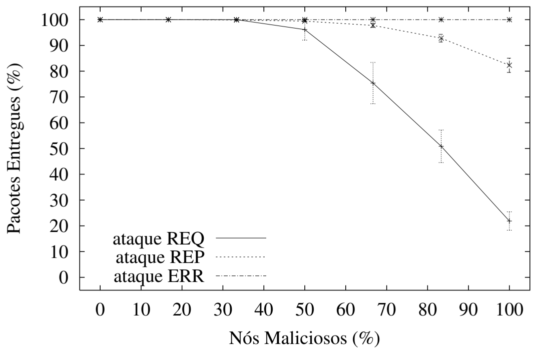
O primeiro ponto dos gráficos (x = 0) corresponde à situação onde não há nós maliciosos e portanto não há ataques, sendo assim todas as curvas nos três gráficos coincidem, como esperado. O valor desses pontos, em torno de 99% de pacotes entregues, indica uma condição muito leve na carga da rede, já que os enlaces operam à taxa nominal de 11Mb/s e o tráfego de dados úteis é de apenas 16Kb/s.



(a) sem pausa.



(b) tempo de pausa de 300s.



(c) sem movimentação.

Figura 1: Efetividade dos ataques ao protocolo de roteamento AODV.

Em um cenário de maior mobilidade a conectividade entre os nós varia muito, o que faz com que fonte e destino ora estejam em contato direto, ora estejam conectados por caminhos de vários saltos. Esse ambiente exige muito do roteamento fazendo várias chamadas aos processos de descoberta, de manutenção e de falhas das rotas. Neste ambiente, representado na Figura 1(a), observa-se que o ataque ERR é muito prejudicial podendo baixar a taxa de entrega a 60%. Isto se deve ao grande número de sinalização de falhas nas rotas que existe em um ambiente de alta mobilidade. Com o ataque ERR as mensagens RERR não chegam até as fontes. O ataque REP é inofensivo neste ambiente dada a alta mobilidade que leva a uma intensa variação nas rotas, logo de qualquer forma um pacote RREP não é válido por muito tempo. O ataque REQ passa a ser efetivo quando mais de 70% dos nós estão comprometidos e impedem a propagação de pedidos de rota. Com menos nós maliciosos o cenário de grande mobilidade não permite influência destes nós devido às grandes chances de se estabelecer rotas pelos nós comuns. Se mais de 80% da rede está comprometida neste ataque torna-se muito difícil o estabelecimento de rotas de múltiplos saltos, restando apenas a conexão com os nós destinos que por ventura entrem no alcance dos nós fontes (correspondente a rotas de um salto), isto leva a taxa de entrega a valores em torno de 35%.

Num ambiente sem mobilidade, como o representado na Figura 1(c), tudo passa a depender do sorteio da posição dos nós em cada um dos cenários de simulação. Como não há movimentação não há influência do ataque ERR devido à inexistência de notificações de falhas nas rotas. Um dado nó sempre estará no alcance de uns e nunca estará no alcance de outros, a conectividade da rede não varia. Sendo assim, as rotas com múltiplos saltos não se modificam durante a simulação. Somente quando mais de 50% da rede se encontra comprometida é que passamos a observar uma influência dos ataques REP e REQ. Estando mais da metade dos nós comprometidos o efeito do ataque REQ é bem mais notado do que do ataque REP, o ataque REQ pode descer a taxa de entrega para até 20%. Nessa situação é bem mais difícil o estabelecimento de rotas devido ao comportamento de mais da metade da rede com relação às mensagens de pedido de rota e ao estado fixo dos nós em todo o tempo de simulação. No ataque REP a pior situação leva a uma taxa de entrega de 80%, já que há uma certa probabilidade de que origem e destino estejam diretamente alcançáveis. Neste caso, mesmo com 100% de nós maliciosos, rotas com apenas um salto não são atingidas pelo ataque, que tem então baixa efetividade.

Observa-se que a Figura 1(b) é um estágio de transição entre as Figuras 1(a) e 1(c), posto que representa um ambiente onde na média em metade do tempo os nós se movem e na outra não. O objetivo em obtê-la e apresentá-la é certificar-se dos resultados nos extremos, alta mobilidade e nenhuma mobilidade, exprimindo e verificando a maneira que se passa de um extremo ao outro.

Em resumo, o ataque às mensagens de *reply* (REP) é o menos sensível às variações no grau de mobilidade da rede, sendo o mais sensível o ataque às mensagens de *error* (ERR). O mais sensível em relação ao número de nós maliciosos é o ataque às mensagens de *request* (REQ), e o menos sensível o ataque REP. Logo num ambiente de intensa movimentação dos dispositivos o ataque às mensagens de erro é o mais efetivo. Por outro lado num ambiente de baixa movimentação o ataque aos pedidos de rota é o mais efetivo. Com relação a densidade de nós envolvidos no ataque, em todos os casos, quanto mais nós comprometidos mais efetivo se torna o ataque.

5. Conclusão

Neste trabalho foi avaliado o impacto das ações maliciosas de nós numa rede *ad hoc* sobre as mensagens de roteamento do protocolo AODV, em termos da métrica taxa de entrega de pacotes total na rede em função da mobilidade, 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.

Os resultados obtidos demonstram a necessidade de mecanismos capazes de impedir ou minimizar o comportamento não cooperativo entre os nós com relação as mensagens de roteamento. Devido à variabilidade da eficácia dos tipos de ataques em função do grau de mobilidade da rede e da densidade de nós comprometidos no ataque certos tipos de mensagens devem ter prioridade de proteção. Isto leva à necessidade de soluções que contemplem as mensagens de roteamento com imunidade, soluções não únicas, mas adaptáveis às diferentes configurações da rede.

Como para cada ambiente um tipo de ataque é mais prejudicial, as mensagens de erro no roteamento devem receber prioridade de imunização em cenários de alta mobilidade, já em cenários com baixa mobilidade as mensagens de pedidos de rota devem ser priorizadas na imunização.

Como trabalhos futuros propõe-se a investigação de outros tipos de ataques e ainda de mecanismos capazes de inviabilizar tais ataques imunizando as mensagens de roteamento. Tais mecanismos devem ser compatíveis com as restrições encontradas, principalmente a escassez de banda e de energia do dispositivo móvel, e ainda, que não prejudiquem o desempenho da rede. Esses mecanismos podem ser baseados em redundância por múltiplos caminhos ou compensações por serviços prestados ao roteamento.

Referências

Corson, S. and Macker, J. (1999). *Mobile Ad hoc Networking (MANET) - Routing Protocol Performance Issues and Evaluation Considerations*. http://www.ietf.org/rfc/rfc2501.txt.

Deng, H., Li, W., and Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communications Magazine*, 40(10):70–75.

Haas, Z. J. and Zhou, L. (1999). Securing ad hoc networks. *IEEE Network Magazine*, 13(6):24–30.

Hubaux, J., Buttyan, L., and Capkun, S. (2001). The quest for security in mobile ad hoc networks. In *ACM International Symposium on Mobile Ad Hoc Networking and Computing - MobiHoc*.

Kärpijoki, V. (2001). Security in ad hoc networks. Technical report, Department of Computer Science, Helsinki University of Technology.

Marti, S., Giuli, T. J., Lai, K., and Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *ACM International Conference on Mobile Computing and Networking - MobiCom*.

Perkins, C. E., Belding-Royer, E. M., and Das, S. R. (2002). *Ad Hoc On-Demand Distance Vector (AODV) Routing*. http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-12.txt.

Perkins, C. E. and Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM Conference of the Special Interest Group on Data Communication - SIGCOMM*.

Perkins, C. E., Royer, E. M., Das, S. R., and Marina, M. K. (2001). Performance comparison of two on-demand routing protocols for ad hoc networks. *IEEE Personal Communications*, 8(1):16–28.

Royer, E. M. and Toh, C.-K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications*, 6(2):46–55.

Vanhala, A. (2000). Security in ad hoc networks. Technical report, Department of Computer Science, University of Helsinki.