Uma Comparação das Abordagens Topológica e de Posicionamento nos Protocolos de Roteamento Seguro para Redes *Ad Hoc* Móveis

Nelcileno Virgílio de Souza Araújo[1]
Ed' Wilson Tavares Ferreira[2]
Ruy de Oliveira[3]

Resumo: Nos últimos anos, o crescimento de aplicações para redes *ad hoc* móveis tem apresentado vários desafios para fornecer uma comunicação segura entre os nós móveis dessas redes, tais como: ausência de um ponto central de gerenciamento, algoritmos de roteamento cooperativo, topologia dinâmica da rede e escassez de recursos computacionais e energéticos dos nós. Este trabalho realiza um levantamento bibliográfico sobre duas abordagens (topológica e de posicionamento) de protocolos de roteamento seguro e apresenta as suas vantagens e desvantagens a partir de requisitos que avaliam tanto a questão da segurança quanto o desempenho da rede.

Palavras-chave: Redes ad hoc móveis, segurança, protocolos de roteamento.

Abstract: The growth of applications for mobile *ad hoc* networks (Manet) in recent years has presented many challenges to provide a secure communication between their nodes, such as: absence of a management central point, cooperative routing algorithms, dynamic network topology and the scarcity of computational and energy resources from the nodes. This work makes a survey about two approaches (topological and positioning) of secure routing

1 Mestre em Engenharia Elétrica, pela Universidade Federal de Uberlândia; professor assistente I do Instituto de Computação, da Universidade Federal de Mato Grosso (UFMT). E-mail: nelcileno@yahoo.com.br.

2 Mestre em Engenharia Elétrica, pela Universidade Federal de Uberlândia; professor do Depto de Informática do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso – Campus Cuiabá. E-mail: edwilson@inf.cefetmt.br.

3 Doutor em Ciência da Computação, pela *University of Bern*-Suíça; professor do Depto de Informática do IFMT – Campus Cuiabá. E-mail: ruy@cba.ifmt.edu.br.

protocols and shows the advantages and disadvantages of them according to the requirements that evaluate as the issue of security as network performance.

Keywords: Manet, security, routing protocol.

Introdução

Redes *ad hoc* móveis (Manet – *Mobile ad hoc Network*) é um tipo de rede sem fio em que os nós móveis são capazes de transmitir sem o auxílio de uma infra-estrutura de rede ou qualquer administração centralizada. No que se refere às aplicações, esta tecnologia tem como alvo ambientes de campo de batalha, serviços de emergência e desastres em que os pontos – tanques, carros de polícia, helicópteros e outros – estão em movimento, sem a existência de uma rede fixa interligando-os e os recursos oferecidos são limitados.

As características que definem um ambiente de uma Manet podem aumentar as suas vulnerabilidades a ataques e ameaças. Por exemplo, o meio aberto por onde as mensagens são encaminhadas é mais suscetível à escuta, pois a topologia dinâmica da rede dificulta a utilização de sistemas de segurança centralizados, a cooperação distribuída dos protocolos de roteamento para a tomada de decisão torna a rede mais vulnerável a ataques de negação de serviço e os recursos limitados dos nós exigem soluções com baixo consumo de recursos. Dessa forma, qualquer solução de segurança empregada numa Manet deve procurar limitar essas vulnerabilidades.

Mecanismos de segurança em Manet podem ser divididos em três categorias: roteamento seguro – em que a segurança é implementada no protocolo de roteamento; sistemas de detecção de intrusão – ajudam na detecção de nós mal comportados através de mecanismo de análise de comportamento dos nós; e sistemas de reputação – utilizam a cooperação existente entre os nós de uma Manet para definir a reputação deles.

Este trabalho enfoca mecanismos de segurança, baseado em roteamento seguro, a partir de uma comparação entre a abordagem topológica, em que a tomada de decisão de roteamento se baseia na topologia da

rede, e a abordagem posicionamento, em que o cálculo das rotas ocorre de acordo com a posição geográfica dos nós.

A comparação estabelecida neste artigo dar-se-á através da análise dos seguintes requisitos: adaptação à mudança de topologia, escalabilidade, *overhead* de pacote, *overhead* de processamento, tipo de ambiente aplicado e robustez contra nós mal comportados. Além disso, foram selecionados três protocolos de roteamento para cada abordagem: Aran (SANZGIRI et al., 2005), Ariadne (HU, PERRIG e JOHNSON, 2002a), Sead (idem, 2002b) compondo o grupo do roteamento seguro orientado à topologia, e Spaar (CARTER e YASINSAC, 2002), SGF/SGLS (SONG, WONG e LEUNG, 2007) e AO2P (WU e BHARGAVA, 2005) compondo o grupo do roteamento seguro orientado a posicionamento.

O restante do artigo está assim organizado: seção II discute as principais formas de ataque na camada de rede de uma Manet; na seção III, os protocolos de roteamento seguro selecionados são apresentados, enfocando seu funcionamento, vantagens e desvantagens e a seção IV fornece uma comparação entre os dois princípios de roteamento, definindo o perfil de cada um e qual o cenário mais favorável para sua implantação.

Tipos de Ataques em uma Manet

Os nós, em uma Manet, podem assumir tanto o papel de terminal quanto de roteador. Eles podem movimentar-se aleatoriamente e organizar-se de forma arbitrária. O roteamento, em uma rede *ad hoc,* funciona num modelo de encaminhamento multi-salto, em que os nós intermediários encaminham os pacotes originados do nó fonte em direção ao nó destino. Contudo, a ausência de mecanismos de segurança propicia aos nós executarem qualquer tipo de ação enquanto encaminha os pacotes. Sendo assim, a presença de nós mal comportados, isto é, os que alteram, descartam ou inserem pacotes, pode corromper o roteamento da rede, prejudicando a disponibilidade (FONSECA e FESTAG, 2006).

Existem diversos tipos de ataques contra Manet que podem ser enquadrados nas seguintes categorias (ibid.; MANDALAS et al., 2005):

– Fabricação de roteamento: os nós adulteram a informação de roteamento fornecida por eles, causando problemas, tais como: *loops* de roteamento, particionamento da rede, direcionamento do tráfego, geração de falsas mensagens de erro, privação de sono e outros.

– Encaminhamento seletivo: um nó privilegia o encaminhamento de alguns pacotes em detrimento de outros. Normalmente, os pacotes favorecidos são aqueles pelos quais tem interesse. Por isso, esse tipo de ataque também é conhecido como ataque do nó egoísta.

– *Sinkhole*: um nó persuade os seus vizinhos a acreditar que está na melhor rota ao destino pretendido, fazendo com que propaguem essa notícia ao restante da rede. Por conseqüência, todo o tráfego contido na rede passará por ele. Um caso especial desse tipo de ataque é o *wormhole,* em que o nó malicioso faz conluio com um nó externo e transmite os pacotes secretamente para este.

– Falsificação: um nó se passa por outro para acessar informações de seu interesse. Quando pode assumir várias identidades, este ataque é denominado *Sybil*. Essa é a forma mais perigosa de ataque, pois reduz a eficiência dos sistemas de segurança.

A seguir, faremos uma breve descrição sobre os principais sistemas de segurança baseados em roteamento seguro.

Protocolos de Roteamento Seguro

Quando se pensa em mecanismo de segurança baseado em roteamento seguro, trabalhamos no oferecimento dos seguintes serviços para a Manet: confidencialidade ou privacidade, autenticação, integridade e não repúdio.

O roteamento seguro pode ser realizado de duas formas pelos nós: protegendo informações de roteamento baseado na topologia da rede (protocolo de roteamento orientado a topologia), ou o posicionamento geográfico dos nós (protocolo de roteamento baseado em posicionamento).

Abordagem Topológica

A seguir, apresentamos o funcionamento, vantagens e desvantagens de alguns protocolos de roteamento seguro que utilizam a topologia da rede para gerar informação de roteamento.

Aran

O Aran é um protocolo reativo originado a partir do AODV (PERKINS e ROYER, 1999) que implementa criptografia assimétrica por meio de certificados digitais.

No início, cada nó gera, antecipadamente, uma chave com a autoridade certificadora (CA) através de uma banda não utilizada pela rede. A seguir, solicita um certificado para a CA que será utilizado para proteger a troca de informações de roteamento, prevenindo ataques de fabricação de roteamento.

Quando um nó fonte pretende construir uma rota, envia um pacote de descoberta (RDP – *Route Discovery Packet*) assinado para descobrir um caminho. Este pacote transporta o identificador do RDP, o endereço do destino, o certificado do nó origem e uma chave de sessão para evitar ataques de *replay*. Cada nó intermediário, ao receber o pacote RDP do seu antecessor, executa os seguintes passos: valida a assinatura, remove o certificado e assinatura e grava o endereço na tabela de roteamento. A seguir, assina a mensagem original e anexa a ela seu próprio certificado.

Ao receber o primeiro pacote RDP, o destino responde com um pacote de resposta (REP – *Reply Packet*) que é enviado de volta pelo caminho reverso até o nó origem. O REP contém o seu identificador, o endereço da origem, o certificado do nó destino e a chave de sessão da origem. O processo de encaminhamento do REP pelos nós intermediários é semelhante ao realizado na transmissão da mensagem RDP. Quando REP chega na origem, o nó valida a rota construída pela checagem da assinatura do nó destino e a chave de sessão enviada por ele.

Contudo, se um nó recebe dados de uma rota já desativada, uma mensagem de erro autenticada é gerada e enviada para fonte e os nós nesse caminho, para que atualizem suas tabelas de rotas.

SANZGIRI et al. (2005) apontam um desempenho do Aran tão efetivo quanto o AODV na descoberta e manutenção de rotas. Entretanto, a escalabilidade da rede é um ponto vulnerável dessa solução, já que causa um aumento no *overhead* de pacotes e na latência da descoberta de rota.

Ariadne

É um protocolo baseado no DSR (JOHNSON, MALTZ e BROCH, 2001) que, na construção e manutenção de rota, utiliza criptografia simétrica para prover autenticação e integridade das mensagens de sinalização (REQ, REP e ERR), podendo ser implementado segundo os seguintes modelos: distribuição de par de chaves entre todos os nós, cadeias *hash* para autenticação dos nós e assinaturas digitais.

Os autores Hu, Perrig e Johnson (2002a) e Fonseca e Festag (2006) destacam a simplicidade do modelo de cadeias *hash* por utilizar uma variação de infra-estrutura de chave pública do protocolo Tesla (PERRIG et al., 2002) para autenticar os nós. A chave pública funciona com um mecanismo de sincronização de relógios para revelar as chaves. Caso um nó receba a chave de um transmissor num intervalo de tempo menor que o esperado, implica que a chave já foi divulgada e pode ser um ataque de fabricação de roteamento.

O funcionamento do protocolo Ariadne com cadeias *hash* é semelhante ao DSR. Quando um nó não encontra um caminho na sua *cache* de rotas, transmite uma mensagem de solicitação de rota (REQ – *Route Request*) em direção ao destino pretendido. Cada salto autentica uma nova informação de roteamento na REQ, além de inserir sua identificação na lista de nós percorrida. O nó destino guarda a mensagem de resposta (REP – *Route Reply*) até os nós intermediários poderem revelar as suas chaves e, após a revelação, ele valida que nenhuma das chaves foi publicada anteriormente, incluindo um código de autenticação de

mensagem (MAC). Para evitar que nós intermediários removam outros nós da lista, estes devem realizar a função *hash* por salto e anexá-la no cabeçalho do pacote.

Quando um nó não tem sucesso na entrega de pacotes após uma determinada quantidade de tentativa de retransmissões, uma mensagem de erro (ERR – *Route Error*) autenticada é transmitida para o nó origem. Todos os nós ao longo do caminho também autenticam essa mensagem até alcançar a origem.

Ariadne protege o DSR de ataques de fabricação de roteamento e *sinkhole*. Com relação ao desempenho, pode-se perceber que o encaminhamento de mensagens de sinalização muito grande e o atraso na revelação das chaves provocam um maior processamento e um aumento do retardo fim-a-fim do processo de descoberta de rota que acaba gerando uma diminuição na taxa de entrega de pacotes.

Sead

É um protocolo pró-ativo baseado no DSDV (PERKINS e BHAGWAT, 1994) que implementa o mecanismo de segurança por meio de cadeias e árvores *hash*. Além disso, ambientes onde os nós possuem restrições de recursos são apropriados para o uso deste protocolo de roteamento seguro.

O principal objetivo do Sead é proteger a rede contra múltiplos ataques não coordenados que geram informação de roteamento incorreta. Sendo assim, o seu alvo é autenticar as mensagens de atualização de roteamento do protocolo DSDV.

Cada nó, ao transmitir sua mensagem de atualização, seleciona um elemento da cadeia *hash* gerada e autentica a métrica e o número seqüencial de cada entrada na sua tabela de rotas. Para prevenir que um nó malicioso reivindique uma métrica maior ou igual à autenticada, o nó prioriza a métrica de menor valor numa rota. Desta forma, os nós sucessores devem ter métricas maiores que a recebida.

Quando um nó recebe uma mensagem de atualização, para cada entrada existente há uma checagem da métrica e do número seqüencial

com o último valor de *hash* recebido. Se a entrada for válida, a informação é processada, senão ignorada.

A fim de prevenir ataques de loops de roteamento, o Sead autentica os nós transmissores através de mecanismos de transmissão autenticada (Tesla, Hors, Tik), bem como, o uso de árvores *hash* com *packet leashes* amarra o autenticador ao endereço do nó transmissor, para combater ataques de *replay*.

A taxa de entrega de pacotes do Sead supera o protocolo DSDV, mesmo gerando maior overhead de pacotes. Além isso, propicia a construção de tabelas de roteamento num tempo menor, permitindo um bom desempenho em ambientes de alta mobilidade.

Abordagem de Posicionamento

Será feita uma revisão bibliográfica sobre alguns protocolos de roteamento seguro que empregam o posicionamento geográfico para tomada de decisão de roteamento.

Spaar

O Spaar é um protocolo de roteamento seguro, baseado em posicionamento que protege a rede de nós maliciosos em um ambiente hostil-gerenciado, ou seja, não expõe a topologia da rede para nenhum elemento autenticado ou não-autenticado e também tenta minimizar os danos causados por nós comprometidos.

O mecanismo de segurança do Spaar é implementado em dois níveis. No primeiro nível, a comunicação entre a autoridade certificadora e os nós é criptografada através de um par de chaves pública/privada. Já o outro nível fica responsável por criptografar a comunicação entre o nó e seus vizinhos imediatos, também com criptografia assimétrica.

Inicialmente, cada nó transmite uma mensagem Hello criptografada para os vizinhos imediatos. Eles decriptam a chave pública do transmissor, armazenam na sua tabela de vizinhos e respondem enviando a mesma

mensagem. O nó transmissor recebe essa resposta e armazena a chave pública, a posição e a faixa de transmissão decriptada de cada um deles na tabela de vizinhos. A seguir, o transmissor gera um par de chaves pública/privada, também conhecida como chave do grupo de vizinhos. Esta guarda a parte privada para criptografar os pacotes a serem enviados aos vizinhos e envia a parte privada para os vizinhos decriptarem os pacotes recebidos.

A manutenção da tabela de vizinhos é feita através do envio de mensagens de atualização de rota pelos nós, utilizando a chave do grupo de vizinhos para protegê-la. Essas mensagens são transportadas em conjunto com as mensagens de roteamento (RREQ, RREP) e localização (*location request* e *location reply*).

Para prevenir ataques de *replay*, as mensagens de roteamento vêm "seladas" com o número seqüencial do transmissor, para que os nós receptores possam validar a não replicação.

Quando um nó deseja descobrir uma rota, ele divulga uma mensagem de solicitação de rota (RREQ – *Route Request*) criptografada para os seus vizinhos. Aquele que estiver mais próximo do destino armazena o endereço do transmissor no seu cache de rota, assina e transmite a mensagem para o próximo salto em direção ao destino.

Ao receber a mensagem RREQ, o destino manda de volta à fonte a mensagem de resposta (RREP – *Route Reply*) criptografada que atravessa cada nó intermediário ao longo do caminho reverso. Quando o nó fonte recebe a mensagem RREP, ele atualiza a sua tabela destino com a nova posição do destino.

Cada nó mantém uma tabela com a lista dos destinos mais recentemente acessados a qual é conhecida como tabela destino. Caso esteja vazia, o nó fonte transmite uma mensagem *location request* para que os vizinhos informem a localização do destino. Qualquer vizinho que possua a posição envia de volta uma mensagem *location reply,* e essa troca de mensagens é feita com a utilização da chave do grupo de vizinhos para proteger a comunicação.

Se um dado é recebido por uma rota desativada, uma mensagem de erro é gerada e propagada de volta ao nó fonte. Ela é assinada e cripto-

grafada ao longo de cada salto para que os nós intermediários possam atualizar as tabelas de roteamento.

O protocolo SPAAR protege o posicionamento com autenticação, privacidade e integridade via criptografia assimétrica. Essa informação protegida favorece a redução do *overhead* de roteamento e, por outro lado, dobra o overhead de processamento já que se aplicam dois níveis de proteção.

SGF/SGLS

GLS (JANNOTTI et al., 2000) é um serviço de localização distribuída que, combinado com o encaminhamento geográfico, permite o seu uso em ambientes com alta densidade de nós. Ele divide a Manet em regiões (*grid*) que são subdivididas em regiões menores, sucessivamente, até o nó ficar cercado por seus vizinhos imediatos. Cada nó, em um nível de região, avisa os seus vizinhos da sua localização. A busca pela localização de um nó também utiliza o ordenamento dos vizinhos imediatos e a hierarquia de regiões para encontrar o servidor de localização que lhe informe a posição do destino pretendido. Contudo, as mensagens de controle (*location update*, *location query* e *location reply*) podem sofrer ataques de fabricação de roteamento, pois não existe nenhum mecanismo de proteção para elas. Com o intuito de protegê-las, o protocolo SGLS/SGF implanta técnicas de segurança sobre o GLS original, tais como: Tik (*TESLA with Instant Key*), Tesla (*Timed Efficient Stream Loss-tolerant Authentication*), Mac (*Message Authentication Code*), assinatura digital e sistema de reputação.

O protocolo SGLS/SGF é dividido em três módulos. O primeiro módulo (encaminhamento geográfico seguro) fica responsável por autenticar os nós transmissores ao longo do caminho através do uso do protocolo Tik com sincronização de tempo restrita e a mensagem por meio do Mac. A segunda parte (SGLS) oferece autenticação das mensagens de controle via assinatura digital. A última parte trata do sistema de reputação local (LRS – *Local Reputation System*) utilizado como uma alternativa para a criptografia assimétrica evitar ataques de adulteração e descarte de mensagens,

sem aumentar muito o overhead de roteamento. Trata-se de uma extensão do sistema de incentivo e punição Confidant (BUCHEGGER e LEBOUDEC, 2002) para protocolo de roteamento, baseado em posicionamento.

O LRS proposto pelos autores assume que, periodicamente, cada nó envie o relatório de reputação para os seus vizinhos por meio de mensagens Hello e gerencie a reputação dos seus vizinhos locais. A reputação pode ser obtida pela observação pessoal do comportamento dos vizinhos imediatos (reputação de primeira mão) ou pela observação de terceiros sobre o comportamento de outros nós da rede (reputação de segunda mão).

SGLS/SGF tem a capacidade de prevenir ataques de replay, injeção falsificada, descarte e adulteração de mensagens. Com relação ao desempenho, ele mantém uma alta taxa de entrega de pacotes apesar da presença de ataques de descarte. Por outro lado, possui um custo de overhead de roteamento e *jitter* fim-a-fim muito maior que a estratégia tradicional (GLS).

AO2P

A perda de privacidade em algoritmos de roteamento baseado em posicionamento se deve, principalmente, pela extensiva revelação da posição.

O protocolo AO2P procura fornecer privacidade através de uma comunicação anônima entre os nós da rede, porém não trabalha com troca de mensagens de posição para determinar o próximo salto na construção de uma rota. Ao invés disso, utiliza um mecanismo de competição de acesso ao canal onde os nós receptores são divididos em diferentes classes segundo a proximidade deles em relação à posição do destino. O receptor que esteja mais próximo ao destino é associado à classe de maior prioridade e, geralmente, vence a competição pelo acesso ao canal, resultando em rotas com uma quantidade menor de saltos.

Uma vez a rota construída, falsos identificações (ID) e endereços temporários de camada de acesso ao meio são gerados pelos nós do caminho, de modo a não revelar suas identidades e preservar o anonimato. Para preservar a privacidade da posição do destino, um mecanismo de gerenciamento de posição segura oculta a ligação entre a identidade real

do destino e a sua posição. Infelizmente, o AO2P não oferece mecanismo de segurança nativo para o encaminhamento das mensagens de dados.

Denominado VHR, o serviço de localização de nós no AO2P funciona dentro de regiões ao redor de pontos fixos distribuídos pela MANET e é onde ficam os nós e os servidores de localização. Cada nó atualiza sua posição ao servidor local dentro do seu VHR. Já as mensagens de controle do serviço de localização usam o protocolo AO2P, não precisando que o nó processe a atualização da posição baseado em tempo de seus vizinhos.

Para resolver o problema da revelação da localização do destino à rede no protocolo AO2P, uma melhoria é introduzida. Ao invés de usar a posição real do destino, um ponto de referência é fornecido à mensagem RREQ. Quando um nó deseja saber a posição do destino, uma função *hash* é aplicada no ponto de referência para obter a localização real. Essa técnica é chamada R-AO2P.

O AO2P preserva a privacidade da comunicação sem aumentar significativamente o overhead de processamento na rede, mesmo em ambiente com alta densidade de nós e alta mobilidade dos nós destinos. Contudo, é vulnerável a nós maliciosos que utilizam um mecanismo mais agressivo de competição para se tornar o próximo salto ao abrir caminho para ataques de fabricação de roteamento e *sinkhole*.

Na próxima seção, será apresentada uma discussão e comparação entre estes dois modelos de roteamento seguro em redes ad hoc móveis.

Topologia x Posicionamento

Para iniciar a comparação entre os protocolos de roteamento seguro, é definido primeiramente quais os critérios utilizados para realizá-la.

O primeiro critério trata da capacidade de o protocolo em manter uma boa taxa de entrega de pacotes mesmo em ambientes de alta mobilidade. Esse critério é conhecido como *adaptabilidade* e pode ser classificado em três níveis: bom – quando o protocolo não perde o desempenho; médio – o protocolo faz a entrega dos pacotes, mas há uma diminuição no desempenho; e ruim – o desempenho cai tanto que chega

a dificultar a tarefa de entrega de pacotes (FONSECA e FESTAG, 2006).

A *escalabilidade* é um critério referente à capacidade de o protocolo aumentar a quantidade de nós sem que haja perda de desempenho. Ela pode ser classificada como: bom – quando novos nós são inseridos e o desempenho da rede não diminui; médio – a rede suporta novos pontos até um tamanho razoável sem perder desempenho; e ruim – a inserção de novos nós causa degradação na rede (ibid.).

O próximo critério, também chamado de *overhead de pacotes*, lida com o efeito que a geração de pacotes grande e a alta quantidade de mensagens sinalização causam no consumo da banda. Ele pode ser classificado como: baixo – o protocolo não gera tráfego adicional quando comparado com sua versão básica ou se gerou não há aumento no consumo da largura de banda; médio – ocorre a geração de algum tráfego adicional e, por conseqüência, um crescimento do consumo da banda; e alto – há uma alta geração de tráfego adicional causando um consumo muito grande da banda (ibid.).

O quarto critério, denominado *overhead de processamento*, também trata de overhead, mas com relação ao processamento das mensagens de roteamento. Existem três categorias para classificá-lo: baixo – requer baixo processamento dos recursos utilizados; médio – exige um pouco mais do processamento, porém não afeta a disponibilidade do nó; e alto – o processamento é alto e prejudica a disponibilidade do nó (ibid.).

O critério *tipo de ambiente* trata dos requisitos de segurança implementado no protocolo e pode ser classificado em: aberto – protege a rede contra ataques de fabricação de roteamento e *sinkhole*; aberto-gerenciado – além de satisfazer os requisitos de segurança de um ambiente aberto, deve impedir nós não autorizados de participarem do roteamento; e hostil-gerenciado – abrange os requisitos de segurança dos dois outros ambientes e não expõe a topologia da rede no processo de construção de rota (DAHILL et al., 2001).

Por último, o critério *robustez contra nós mal comportados* indica o tipo de nó que o protocolo tem como alvo no processo de segurança.

Ele pode ser: malicioso – nó externo a rede que tentam corrompê-la; comprometido – nó autenticado que foi tomado por um inimigo para executar um ataque (MANDALAS et al., 2005).

A seguir, será apresentada a Tabela 1 em que as duas abordagens são comparadas segundo os critérios vistos anteriormente.

Tabela 1. Comparação dos Protocolos de Roteamento Seguro.

Critérios	**Topologia**			**Posicionamento**		
	Aran	**Ariadne**	**Sead**	**Spaar**	**SGF/ SGLS**	**AO2P**
Adaptabilidade	Boa	Médio	Boa	Boa	Boa	Boa
Escalabilidade	Médio	Médio	Boa	Boa	Boa	Boa
Overhead de pacotes	Médio	Baixo	Alto	Médio	Médio	Baixo
Overhead de processamento	Alto	Médio	Médio	Alto	Baixo	Baixo
Tipo de ambiente	A	A-G	A-G	H-G	H-G	H-G
Robustez contra nós mal comportados	M	M	M	M/C	M/C	M/C

Na Tabela 1, o campo "Tipo de ambiente" tem as seguintes representações: "A" – ambiente aberto, "A-G" – ambiente aberto-gerenciado e "H-G" – ambiente hostil-gerenciado. No campo "Robustez contra nós mal intencionados", as representações "M" e "M/C" possuem, respectivamente, os seguintes significados: maliciosos e comprometidos.

Como pode ser visto na Tabela 1, os protocolos de roteamento, baseado em posicionamento, possuem um desempenho superior à abordagem topológica. Isso se deve principalmente ao mecanismo de encaminhamento geográfico que permite uma redução significativa na quantidade de mensagens de sinalização, levando a um custo menor de overhead de pacotes.

Um outro ponto positivo é o uso de técnicas de segurança com a finalidade de não provocar um consumo exagerado dos recursos do nó

(*overhead* de processamento). Ao se programar técnicas menos onerosas, tais como criptografia simétrica, sistemas de incentivo e punição e sistemas detectores de intrusão, podem-se obter protocolos de roteamento que não sobrecarreguem significativamente os nós da rede. Por outro lado, essas técnicas podem oferecer falsas reputações ou mensagem de alerta quando nós mal-intencionados promovem ataques de negação de serviço, a fim de indisponibilizar um ou mais nós legítimos. Para resolver esse problema, deve-se pensar num novo quesito para avaliação, o grau de cooperação entre os nós, pois somente com uma alta cooperação entre eles podem-se obter tanto mensagens de alerta como mensagens de reputação com precisão confiável.

Escalabilidade é outro ponto de grande desvantagem da abordagem topológica, pois os protocolos reativos, normalmente, já exigem bastante tráfego de sinalização para o processo de descoberta de rotas. Além disso, há o tráfego adicional das técnicas de segurança utilizadas e, como é inerente às redes sem fio terem limitação de largura de banda, acaba levando a Manet ao congestionamento.

Com relação aos requisitos de segurança fornecido pelo ambiente, a abordagem de posicionamento satisfaz mais requisitos que a topológica devido a não divulgação da informação geográfica para nós legítimos ou mal-intencionados. Contudo, os sistemas de posicionamento seguro devem possuir servidores de localização que ofereçam a posição somente ao solicitante legítimo e devem estar bem distribuídos na Manet, para que não haja sobrecarga em alguns pontos enquanto outros ficam com os recursos ociosos.

A robustez de um protocolo contra nós mal intencionados está diretamente ligada à combinação de vários sistemas de segurança, tais como: sistemas criptográficos, sistemas de detectores de intrusão e sistemas de reputação, propiciando um processo de detecção e isolamento de nós mal-comportados mais confiáveis. Portanto, a abordagem de posicionamento oferece maior robustez ao apresentar protocolos que combinam sistemas criptográficos e de reputação, bem como serviço de comunicação anônima.

Conclusão

Em Manet, nós móveis cooperam para formar uma rede sem qualquer infra-estrutura, tais como pontos de acesso ou estações base. Ao invés disso, os nós encaminham pacotes entre eles, permitindo a comunicação para fora da faixa de transmissão. A mobilidade dos nós e, fundamentalmente, a capacidade limitada do meio sem fio, junto com a cooperação entre os nós para tomar decisões de roteamento e os efeitos de transmissão (atenuação, propagação multicaminho e interferência) combinam para criar significativos desafios de segurança para a operação dos protocolos de roteamento em redes *ad hoc*.

Sendo assim, qualquer solução para vencer esses desafios deve satisfazer a maior parte desses requisitos. Para definir quem melhor oferece roteamento seguro com um bom desempenho, este artigo se baseou em uma comparação das abordagens topológica e posicionamento, levando em conta seis critérios de avaliação: adaptabilidade, escalabilidade, *overhead* de pacotes, *overhead* de processamento, tipo de ambiente e robustez contra nós mal-intencionados.

A abordagem posicionamento demonstrou-se superior à topológica devido à sua característica de não revelar a topologia da rede para outros nós. Isso resultou em alta adaptabilidade e escalabilidade, baixo *overhead* de pacotes e processamento, bem como na capacidade de ser aplicada em ambientes com alto requisito de segurança, como é o hostil-gerenciado que propicia a localização e o combate a nós maliciosos e comprometidos. Contudo, o sucesso dessa abordagem está diretamente ligado ao oferecimento de um serviço de localização distribuído que não causa muito retardo fim-a-fim na descoberta da posição de um nó. Há também a utilização de outros sistemas de segurança (sistemas de detecção de intrusão e sistemas de reputação), como apoio na tomada de decisão de roteamento, que ajudam os protocolos a serem mais robustos e a propiciarem um ambiente mais seguro. Por tudo isso, esse tipo de abordagem é indicado para redes com alta densidade de nós.

Apesar de todas as desvantagens apresentadas no item Topologia x Posicionamento, a abordagem topológica também cumpre o seu papel de prover segurança em uma rede, mesmo apresentando algumas limitações. Esse tipo de abordagem é mais indicado para redes com baixa e média densidade de nós e com mais recursos computacionais a serem consumidos. Dessa forma, o processo de descoberta de rota sofre menor retardo fim-a-fim.

Ao se projetar um protocolo de roteamento seguro, deve-se pensar em mecanismos de segurança que consumam o mínimo possível os recursos dos nós móveis. Por isso, é recomendado priorizar sistemas criptográficos simétricos para prover privacidade. Além disso, o uso de sistemas detectores de intrusão e sistemas de reputação, para analisar o comportamento dos membros da rede, auxilia o protocolo a combater ataques colaborativos (MANDALAS et al., 2005).

Como trabalhos futuros, sugere-se implementar e analisar o desempenho de protocolos de roteamento seguro que combinem com sistemas de detectores de intrusão, bem como realizar um confrontamento entre os sistemas de reputação e sistemas detectores de intrusão, a fim de detectar qual tem o melhor desempenho em conjunto com os protocolos de roteamento seguro.

Referências

BUCHEGGER, S.; LEBOUDEC, J-Y. Performance analysis of the Confidant Protocol. In: ACM INTERNATIONAL SYMPOSIUM ON MOBILE AD HOC NETWORKING AND COMPUTING, 3., 2002, Lausanne-Suíça. *Proceedings...* Lausanne-Suíça: ACM, jun. 2002.

CARTER, S.; YASINSAC, A. Secure position aided *ad hoc* routing protocol. In: IASTED INTERNATIONAL CONFERENCE ON COMMUNICATIONS AND COMPUTER NETWORK, 2002, Cambridge-Inglaterra. *Proceedings...* Cambridge-Inglaterra, nov. 2002.

DAHILL, B. et al. *A secure routing protocol for ad hoc networks*. Massachusetts-EUA: University of Massachusetts, 2001. (University of Massachusetts Technical Report 01-37.)

FONSECA, E.; FESTAG, A. *A survey of existing approaches for secure ad hoc routing and their applicability to vanets*. Düsseldorf-Alemanha: NEC Network Laboratories, mar. 2006. (NEC Technical Report NLE-PR-2006-19.)

HU ,Y. C.; PERRIG, A.; JOHNSON, D. B. Araidne: a secure on-demand routing protocol for ad hoc networks. In: ACM INTERNATIONAL CONFERENCE ON MOBILE COMPUTING AND NETWORKING, 8., 2002, Hingham-USA. *Proceedings...* Hingham-USA: ACM, set. 2002a.

_____. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. In: IEEE WORKSHOP ON MOBILE COMPUTING SYSTEMS AND APPLICATIONS, 4., 2002, New York-USA. *Proceedings...* New York-USA: IEEE, jun. 2002b.

JANNOTTI, J. Li et al. A scalable location service for geographic ad hoc routing. In: ACM ANNUAL INTERNATIONAL CONFERENCE ON MOBILE COMPUTING AND NETWORKING, 6., 2000, New York-USA. *Proceedings...* New York-USA: ACM, aug. 2000.

JOHNSON, D. Bi; MALTZ, D. A.; BROCH, J. DSR: the dynamic source routing protocol for multihop wireless ad hoc networks. *Ad Hoc Networking*, New York-USA: Addison-Wesley Professional, p. 139-172, 2001.

MANDALAS, K. et al. A survey of several cooperation enforcement schemes for manets. In: IEEE INTERNATIONAL SYMPOSIUM ON SIGNAL PROCESSING AND INFORMATION TECNOLOGY, 5., 2005, Atenas-Grécia. *Proceedings...* Atenas-Grécia: IEEE, 2005. p. 466-471.

PERKINS, C. E.; ROYER, E. M. Ad hoc on-demand distance vector routing. In: IEEE WORKSHOP ON MOBILE COMPUTING SYSTEMS AND APPLICATIONS, 2., 1999, New Orleans-USA. *Proceedings...* New Orleans-USA: IEEE, 1999.

_____.; BHAGWAT, P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *Computer Communications Review*, New York-USA, v. 24, n. 4, p. 234-244, out. 1994.

PERRIG, A. et al. The Tesla broadcast authentication protocol. *Cryptobytes*, [s.l.], v. 5, n. 2, p. 2-13, 2002.

SANZGIRI, K., et al. Authenticated routing for ad hoc networks. *IEEE Journal on selected areas in communications*, New York-USA, v. 23, n. 3, p. 598-610, Mar 2005.

SONG, J-H.; WONG, V. W. S.; LEUNG, V. C. M. Secure position based routing protocol for mobile ad hoc networks. *Elsevier ad hoc Networks*, New York-USA, v. 5, p. 76-86, 2007.

WU, X.; BHARGAVA, B. AO2P: ad hoc on-demand position private routing protocol. *IEEE Transactions on Mobile Computing*, New York-USA, v. 4, n. 4, jul./ago. 2005.