Um Arcabouço para Autoconfiguração Segura e Eficiente do Serviço de Roteamento em Redes Mesh*

Helber Silva[1,2], Michele Nogueira[2], Raimir Holanda[1], Aldri Santos[2]

[1]MIA – Universidade de Fortaleza (UNIFOR) – Fortaleza – CE – Brasil

[2]NR2/PPGInf – Universidade Federal do Paraná (UFPR) – Curitiba – PR – Brasil

{helber,michele,aldri}@inf.ufpr.br, raimir@unifor.br

Abstract. *Wireless mesh networks intend to support the use of applications on different domains that require high levels of both security and performance. However, the operation of these networks can be compromised because of security vulnerabilities on wireless medium sharing and cooperative communication, which allow actions from attackers. This work proposes a framework, called SECOM, that considers security and performance capabilities to self-configuration of essential services, such as routing, in wireless mesh networks. SECOM takes into account criteria from different defense lines (preventive, reactive and tolerant) and performance criteria to adapt services efficiently even in face of attacks or intrusions. Simulation results of a path selection scheme based on SECOM to the routing service show gains on security and performance with low cost of latency under Blackhole attacks.*

Resumo. *As redes mesh sem fio vêm oferecendo o suporte ao uso de aplicações de diferentes áreas que exigem altos níveis de segurança e de desempenho simultaneamente. Contudo, o funcionamento dessas redes pode ser comprometido devido às vulnerabilidades de segurança no compartilhamento do meio sem fio e na comunicação cooperativa, que permitem ações de atacantes. Este trabalho propõe um arcabouço, chamado SECOM, que considera segurança e desempenho para a autoconfiguração de serviços essenciais, como o roteamento, em redes mesh sem fio. SECOM leva em conta critérios de diferentes linhas de defesa (preventiva, reativa e tolerante) e de desempenho para adaptar os serviços de modo eficiente mesmo diante de ataques ou intrusões. Resultados de simulações de um esquema de seleção de caminhos baseado no SECOM para o serviço de roteamento mostram os ganhos de segurança e de desempenho obtidos a um baixo custo de latência diante de ataques Blackhole.*

1. Introdução

As redes em malha (*mesh*) sem fio são compostas por dois tipos de dispositivos (nós), os *clientes mesh* e os *roteadores mesh*. A infraestrutura das redes *mesh* possui vantagens sobre outras redes sem fio, como a fácil instalação, o baixo custo dos equipamentos e a rápida configuração. Além disso, as redes *mesh* podem ser implementadas usando diferentes tecnologias de comunicação sem fio, incluindo o IEEE 802.11, IEEE 802.16, tecnologia celular ou uma combinação delas [Akyildiz and Wang 2005].

*Projeto número 3180/08 apoiado pela FUNCAP - Edital TI 06/2008

Essas redes têm proporcionado o suporte ao desenvolvimento de aplicações para diferentes áreas, como a área financeira e a de saúde, que exigem altos níveis de segurança e de desempenho [Heegaard and Trivedi 2009]. No entanto, as redes *mesh* ainda possuem vulnerabilidades visto que o compartilhamento do meio sem fio e a comunicação cooperativa possibilitam a ação de ataques ou intrusões, como as interferências (*jamming*) e a bisbilhotagem (*eavesdropping*) [Glass et al. 2008, Lima et al. 2009]. Por outro lado, os clientes e os roteadores *mesh* possuem limitações de desempenho que precisam ser consideradas para que a rede mantenha o funcionamento dos seus serviços essenciais [Bruno et al. 2005, Campista et al. 2008]. Logo, a segurança e o desempenho são requisitos cruciais nessas redes.

Soluções para gerenciar os serviços essenciais do funcionamento de redes *mesh* têm tratado segurança [Martignon et al. 2009, Khan et al. 2010] e desempenho [Al-Mashaqbeh et al. 2009, Shillingford and Poellabauera 2010] de forma independente, o que dificulta a garantia do funcionamento desses serviços diante de diferentes ameaças. Este trabalho propõe um arcabouço para a autoconfiguração de serviços essenciais em redes *mesh* a fim de prover segurança e desempenho. O arcabouço, chamado SECOM (*SElf-COnfiguration of Mesh networks*), define blocos funcionais que consideram medidas de segurança e de desempenho na adaptação dos serviços. O SECOM possibilita a reconfiguração desses serviços através da ação coordenada e adaptativa entre as linhas de defesa preventiva, reativa e tolerante, e de dados sobre o desempenho das camadas.

Como um estudo de caso, o arcabouço SECOM foi aplicado no desenvolvimento de um esquema de seleção de caminhos para o serviço de roteamento em redes *mesh* de modo a torná-lo mais seguro e eficiente diante de ataques ou intrusões. O esquema proposto utiliza critérios de desempenho e das linhas de defesa preventiva, reativa e tolerante, assim como lógica *fuzzy* para inferir, analisar e decidir o melhor caminho. Além disso, ele usa mecanismos de redundância nas camadas de rede e de enlace, como a diversidade de caminhos e as condições de rádios e canais.

O esquema de seleção de caminhos foi avaliado na presença de nós maliciosos executando o ataque *Blackhole* visto que esse ataque provoca um grande impacto no roteamento em redes *mesh*. Os atacantes *Blackhole* prejudicam o roteamento ao não encaminharem os pacotes de dados enviados por outros nós [Seth and Gankotiya 2010]. A análise considerou métricas de segurança e de desempenho diante de diferentes quantidades de atacantes. Os resultados obtidos indicam melhorias da taxa de entrega de pacotes e redução do impacto da ação do ataque *Blackhole* com um baixo custo de latência.

O restante do artigo está organizado como segue. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 detalha o arcabouço proposto no trabalho. Na Seção 4, o arcabouço SECOM foi aplicado no desenvolvimento de um esquema de seleção de caminhos. A Seção 5 mostra as avaliações de segurança e de desempenho do esquema proposto. Por fim, a Seção 6 conclui o trabalho e apresenta direções futuras.

2. Trabalhos Relacionados

Diversos trabalhos para aumentar o desempenho de redes *mesh* têm sido propostos. O arcabouço *Configurable Mesh Routing* (CMR) [Shillingford and Poellabauera 2010], por exemplo, realiza o balanceamento entre energia e eficiência em redes com restrições de energia. Os seus componentes usam regras para selecionar os melhores ca-

minhos em termos de energia que atendam os requisitos de Qualidade de Serviço (QoS) das aplicações. A arquitetura *Cross-Layer Enhanced and Adaptive Routing* (CLEAR) [Al-Mashaqbeh et al. 2009] baseia-se nas interferências e no congestionamento nos canais para determinar os caminhos que usam menos transmissões e retransmissões na entrega de dados. Já Carvalho e Rezende [Carvalho and Rezende 2010] propuseram um algoritmo que seleciona caminhos de maior vazão considerando a diversidade de rádios e a largura do canal. Esse algoritmo aplica uma métrica que favorece os enlaces com múltiplos rádios que usam canais mais estreitos. No entanto, essas propostas desconsideram medidas de segurança, sendo ineficientes diante de ataques.

Entre as soluções propostas para aumentar a segurança dos serviços essenciais de redes *mesh* está a arquitetura SAMNAR [Lima et al. 2008], que define uma ação coordenada e adaptativa entre as defesas preventiva, reativa e tolerante para prover serviços sobreviventes. Contudo, essa arquitetura não considera informações de desempenho do ambiente, como contenções e interferências na camada de enlace, diante das ameaças. A arquitetura MobiSec [Martignon et al. 2009] controla o acesso de novos clientes e roteadores através da autenticação com um servidor central, criptografando os dados para garantir a sua confidencialidade. Apesar do uso de criptografia, MobiSec não detecta ou isola um atacante que consiga participar do roteamento.

Já Khan *et al.* [Khan et al. 2010] desenvolveram um protocolo de roteamento que busca selecionar caminhos mais confiáveis a partir dos pacotes de controle que coletam a reputação dos nós intermediários. Esse protocolo, no entanto, não usa criptografia para proteger o valor de reputação nos pacotes, possibilitando a um atacante alterar esse valor para atrair o tráfego de dados. Yuan *et al.* [Yuan et al. 2005] propuseram um esquema de seleção de caminhos baseado em segurança e desempenho contra ataques de negação de serviço (DoS). Entretanto, ele não foi concebido como um arcabouço ou uma arquitetura para a adaptação das redes *mesh*.

3. O Arcabouço de Autoconfiguração de Segurança e Desempenho

O arcabouço proposto, chamado SECOM (*SElf-COnfiguration of Mesh networks*), executa as operações de gerência dos serviços de forma descentralizada nos nós da rede com base no paradigma *In-Network Management* (INM) [Pras et al. 2007, Brunner et al. 2009]. O SECOM também considera a integração entre as defesas preventiva, reativa e tolerante definida pela arquitetura SAMNAR. As defesas preventivas empregadas em redes, como mecanismos de criptografia, *firewalls* e controle de acesso, tentam impedir ataques. As defesas reativas tentam detectar e reagir às intrusões usando mecanismos, como sistemas de reputação e de detecção de intrusão. Já as defesas tolerantes, como as redundâncias, tentam minimizar os prejuízos causados por ataques ou intrusões e recuperar serviços comprometidos.

A Figura 1 apresenta os componentes do arcabouço SECOM. A entidade gerente e os agentes interagem diretamente com os blocos funcionais do SECOM ou com a base de dados para executar operações de configuração e de adaptação dos serviços. O gerente controla os agentes, realiza o processamento das informações coletadas do ambiente de rede, analisa o funcionamento dos serviços, e toma as decisões de autoconfiguração. Os agentes realizam as tarefas de coleta de dados para as tomadas de decisão, cooperação com outros nós e a comunicação inter-camadas (*cross-layer*). O SECOM assume que todos os

nós da rede possuem gerentes e agentes, embora seja possível outras configurações, onde, por exemplo, os gerentes estejam apenas nos roteadores *mesh*.

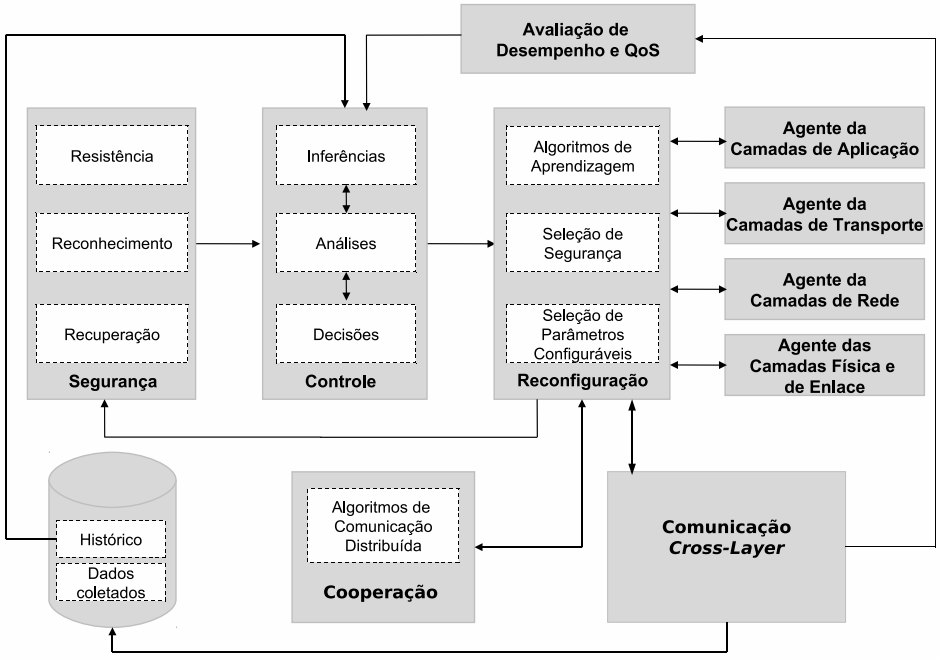

Figura 1. Componentes do arcabouço SECOM

O SECOM inclui blocos funcionais que representam operações de gerência, denominados bloco de controle, bloco de reconfiguração, bloco de cooperação, bloco de segurança, bloco de comunicação *cross-layer*, bloco de avaliação de desempenho e QoS, e blocos referentes às camadas da rede.

O **bloco de controle** corresponde ao núcleo do SECOM e incorpora funcionalidades, como o gerenciamento dos agentes e a análise dos dados e das estatísticas da rede. Outros blocos fornecem evidências para que o bloco de controle realize análises, inferências e decisões sobre a melhor configuração para o nó em um estado específico da rede. Tais decisões consideram questões de segurança, requisitos de desempenho e QoS das aplicações, além de dados coletados em tempo real ou histórico de eventos. Para tanto, o bloco de controle pode usar diferentes algoritmos, tais como os baseados em abordagens probabilísticas [Gillies et al. 2009], ou em inteligência artificial (lógica *fuzzy*, redes neurais e inteligência coletiva) [Dressler 2008]. O bloco de controle envia as decisões tomadas para o bloco de reconfiguração.

O **bloco de reconfiguração** adapta os mecanismos de segurança e as camadas da rede para aumentar a segurança e o desempenho dos serviços com base nas decisões do bloco de controle. Esse bloco possui algoritmos de aprendizagem, mecanismos de segurança e um conjunto de parâmetros configuráveis. Assim, ele define como adaptar os protocolos, os algoritmos, as camadas da rede e os mecanismos de segurança. Como as adaptações devem ser rápidas, os algoritmos de aprendizagem adquirem o conhecimento de decisões e ações anteriores para, assim, modificar as configurações nas camadas e nos mecanismos de segurança. A substituição de protocolos, mecanismos de segurança

ou canais, por exemplo, pode exigir um acordo com outros nós da rede para manter as comunicações. Esse processo é executado pelo bloco de cooperação.

O **bloco de cooperação** possui algoritmos para a comunicação distribuída entre os nós. A cooperação é importante para a coleta de informações que necessitam da interação com outros nós. Tais informações incluem aspectos da camada física, interferências, condições dos canais e dados dos mecanismos de segurança. Ele ainda auxilia o bloco de reconfiguração quando é necessário algum acordo com outros nós para a realização de uma adaptação.

O **bloco de segurança** é composto por mecanismos de segurança que podem ser utilizados pelo nó. Tais mecanismos seguem as linhas de defesa preventiva, reativa e tolerante. Um nó armazena diferentes mecanismos de segurança para cada linha de defesa. Dependendo da decisão do bloco de controle e da seleção do bloco de reconfiguração, um conjunto de mecanismos de segurança é utilizado. O nó aplica simultaneamente ao menos um mecanismo de cada linha de defesa, e o bloco de segurança gerencia a integração entre os mecanismos utilizados.

O arcabouço também define um bloco funcional para cada uma das camadas da rede. Esses blocos adaptam e monitoram as características, os protocolos e as configurações dessas camadas em resposta às decisões do bloco de controle e às escolhas do bloco de reconfiguração. Os agentes executam operações desses blocos funcionais, e o gerente ativa o agente de um bloco apenas quando alguma reconfiguração é necessária. O agente atua até que as suas tarefas finalizem e, caso uma nova reconfiguração seja necessária, o gerente ativa um novo agente.

O **bloco de comunicação *cross-layer*** realiza a comunicação entre as camadas da rede. Ele monitora e coleta os dados relacionados a essas camadas. Os dados coletados e os algoritmos usados no monitoramento provêm indiretamente das decisões do bloco de controle e diretamente do bloco de reconfiguração. O bloco de comunicação *cross-layer* analisa os dados das camadas usando métricas predefinidas, incluindo métricas de desempenho, e alimenta a base de dados. Essas informações incluem interferências entre rádios ou canais, latência na camada de aplicação, taxa de perda de pacotes e outros. O bloco de comunicação *cross-layer* pode coletar os dados e executar processamentos como agregações, por exemplo, ou apenas enviar os dados das métricas de desempenho para o bloco de desempenho e avaliação de QoS.

O **bloco de desempenho e avaliação de QoS** verifica se esses requisitos estão sendo satisfeitos. Em geral, as aplicações definem esses requisitos e as avaliações detectam mudanças no desempenho e nos dados coletados. Os resultados dessas avaliações auxiliam o bloco de controle para a tomada de decisões. Dependendo do estado da rede, o bloco de controle pode ou não dar prioridade aos requisitos das aplicações. Em uma situação crítica de rede, como em um desastre onde a conectividade é essencial para a transmissão de dados, o bloco de controle pode desconsiderar os requisitos de QoS de uma aplicação e dar prioridade à manutenção da conectividade da rede. Por outro lado, se a rede está sendo utilizada para a transmissão de vídeo de um procedimento médico em uma emergência, por exemplo, os requisitos de QoS devem ser garantidos.

As informações utilizadas pelo bloco de controle e por outros blocos provêm da *base de dados*. Ela armazena tanto os dados coletados em determinados momentos da

rede quanto o histórico desses dados. A quantidade de dados armazenados está condicionada à capacidade da base de dados. Logo, dados antigos são removidos seguindo uma política de substituição quando a base de dados atinge o seu limite.

4. Roteamento Seguro e Eficiente

O arcabouço SECOM foi aplicado no serviço de roteamento para redes *mesh*, como um estudo de caso, para torná-lo mais seguro e eficiente diante de ataques ou intrusões. Esse serviço de roteamento define um esquema de seleção de caminhos que leva em conta critérios de segurança e de desempenho para selecionar o melhor caminho. O esquema infere, analisa e decide o melhor caminho através do uso de lógica *fuzzy*. Para isso, o esquema considera informações de segurança das linhas de defesa disponíveis, assim como informações de mecanismos de redundância nas camadas de rede e de enlace, como a diversidade de caminhos e as condições de rádios e canais.

O uso de múltiplos rádios e canais tem sido empregado para melhorar o desempenho das redes visto que contenções e interferências do meio sem fio têm limitado o desempenho do roteamento [Kyasanur et al. 2006]. O esquema de seleção de caminhos proposto baseado no SECOM utiliza o protocolo *Heterogeneous Multi-Channel Link Layer Protocol* (HMCLL) [Bhandari and Vaidya 2009] devido à sua capacidade de gerenciar múltiplos rádios e canais. O HMCLL considera as taxas de interferência obtidas pelos enlaces sem fio para caracterizar um canal, e caracteriza um rádio pelo conjunto de canais que ele pode operar.

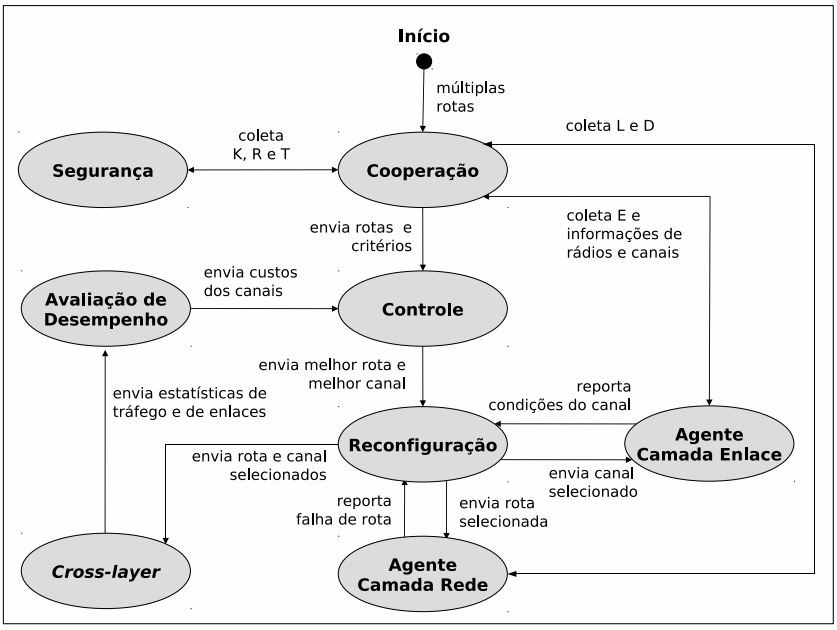

Figura 2. Fluxo de operações entre os blocos funcionais no estudo de caso

A Figura 2 correlaciona os blocos funcionais do SECOM com o esquema de seleção de caminhos, apresentando o fluxo de operações entre os blocos. Esse fluxo se inicia no bloco de cooperação logo após a fase de descoberta de caminhos do protocolo de roteamento. Um nó origem de um fluxo de dados conhece os múltiplos caminhos para os nós com os quais ele deseja se comunicar. Com isso, o nó origem con-

segue coletar os dados referentes às condições dos enlaces dos caminhos e aos critérios de segurança e de desempenho. Esses dados são então enviados para o bloco de controle.

Com base nos critérios recebidos do bloco de cooperação, o bloco de controle seleciona o caminho mais seguro e eficiente, o melhor rádio e o melhor canal, e envia essas decisões para o bloco de reconfiguração. Esse bloco então reconfigura os protocolos das camadas de rede e de enlace através dos agentes dessas camadas. O bloco de reconfiguração ainda usa procedimentos do bloco de comunicação *cross-layer* para correlacionar informações das camadas de rede e de enlace. Como o foco do esquema de seleção de caminhos está sobre essas duas camadas, não são especificadas as interações com as camadas de transporte e de aplicação. As próximas subseções detalham cada procedimento do estudo de caso.

4.1. Os procedimentos de cooperação

No *nível de rede*, os nós origem coletam periodicamente dados sobre cada caminho descoberto pelo protocolo de roteamento usando um procedimento *push-pull*. Nesse procedimento, pacotes de controle, chamados de CPACKs, são enviados através de todos os caminhos conhecidos. Os CPACKs são encaminhados a partir do nó origem até o nó destino, e armazenam os valores de critérios de segurança e desempenho coletados em cada nó intermediário em campos específicos. A definição dos campos e dos valores esperados pelos CPACKs são definidos em [Lima et al. 2008]. Quando os CPACKs alcançam o nó destino, este calcula um código *message digest* dos dados do pacote e assina o código com a sua chave privada usando uma Infraestrutura de Chave Pública provida por uma entidade externa (como detalhado na Subseção 4.3). O nó destino, então, adiciona o código *message digest* no CPACK e o envia ao nó origem pelo mesmo caminho. Porém, no caminho de retorno o CPACK não coleta dados. Caso o CPACK seja perdido devido a colisões ou falta de rotas, por exemplo, o nó origem mantém os valores anteriores dos critérios da rota até que um novo procedimento de cooperação seja concluído.

No *nível de enlace*, o bloco de cooperação também executa procedimentos para a coleta de dados. Como cada enlace de um caminho está associado a um canal, o protocolo HMCLL monitora um *pool* de canais, isto é, um subconjunto de todos os canais disponíveis na rede. Esse processo é realizado através de pacotes de controle que coletam informações que incluem estatísticas sobre cada rádio local, cada canal sobre o qual algum rádio pode operar e sobre as condições de tráfego.

4.2. Os procedimentos de controle

No *nível de rede*, os nós analisam e calculam o grau de segurança e desempenho (PSL) de um caminho usando lógica *fuzzy* (LF) devido ao seu baixo custo computacional. Neste caso, foi definido que o PSL é um valor do intervalo [0.0;1.0]. Para cada caminho conhecido, os nós origem calculam e inferem os valores do PSL após o retorno de CPACKs com os valores de critérios.

As características da rede, assim como as métricas de desempenho e as informações provenientes dos mecanismos de segurança compreendem os valores de critérios a serem utilizados. Neste caso, esses critérios são denominados *critérios convencionais* e *critérios de segurança*. Os critérios convencionais permitem o gerenciamento dos recursos e do desempenho, sendo escolhidos a energia remanescente em um nó (taxa

de energia) e o tamanho do caminho como informações da rede. Outros critérios podem ser considerados, como a vazão do caminho e a estabilidade do enlace. Já os critérios de segurança incluem o tamanho da chave de criptografia, o tempo de expiração do certificado, a reputação do caminho e o grau do caminho.

O cálculo e a inferência do valor do PSL seguem as fases da LF: fuzzificação, inferência e defuzzificação. Os valores dos critérios coletados são normalizados em um intervalo [0.0;1.0] através de funções trapezoidais. Em seguida, regras *fuzzy* são aplicadas para calcular ou realizar inferências a partir do valor do PSL.

As normalizações dos critérios e as regras *fuzzy* derivam do impacto de cada critério no desempenho e na segurança do caminho. A taxa de energia (E) de um caminho é definida como a menor taxa de energia dentre todos os nós que o compõem, sendo classificada como *alta*, *média* e *baixa*. Caminhos com valor de E alta são desejáveis porque os nós participam dos caminhos por mais tempo. Essa estabilidade reduz os processos de redescoberta de caminhos, os quais aumentam a latência e favorecem a participação de atacantes. O tamanho do caminho (L) é a quantidade de nós intermediários entre o nó origem e o nó destino, sendo classificado como *curto*, *médio* ou *longo*. Caminhos curtos são preferíveis porque diminuem a probabilidade da existência de atacantes neles.

Os valores dos critérios de segurança são determinados com base nos menores valores coletados nos nós intermediários. O tempo de expiração do certificado (T) é classificado como *iminente* ou *distante*. Se o certificado expirar em 10s ou menos então T é iminente. Por outro lado, T será distante se o certificado expirar após 60s. Caminhos com valor de T distantes diminuem o risco do certificado ser comprometido enquanto o caminho está ativo. O tamanho da chave de criptografia (K) pode ser *curto* ou *longo*. Se a chave secreta possui 40 *bits* ou menos, o valor de K é curto. Por outro lado, K é longo se o tamanho da chave secreta é maior ou igual a 128 *bits*. Assim, os caminhos com valor de K longos são mais seguros devido à maior resistência do sistema de criptografia.

A reputação de um caminho (R) pode ser *boa* ou *má*, dependendo do comportamento dos nós intermediários. Se o valor de R for maior ou igual a 0.8, então o caminho tem boa reputação. Em contrapartida, ele possui má reputação se R estiver dentro do intervalo [0.0;0.8[. Assim, os caminhos com boa reputação são preferíveis porque possuem menos nós reconhecidos como maliciosos pelo sistema de reputação. O grau do caminho (D) é classificado como *pouco*, *normal* e *muito*, com base no grau dos nós intermediários. O grau de um nó é definido como a quantidade de vizinhos diretos. Quanto maior é o valor de D, maiores são a probabilidade de haver caminhos redundantes até um nó destino e a tolerância a quebras de caminhos.

Após a normalização dos valores dos critérios, o nó aplica um conjunto de regras *fuzzy* sobre eles para calcular o grau de segurança e desempenho do caminho [Lima et al. 2008]. Assumindo a independência entre os critérios considerados, o comportamento das regras *fuzzy* define o grau de segurança e desempenho do caminho, sendo generalizado como:

$$PSL = E \times K \times R \times D \times \frac{1}{L} \times \frac{1}{T} \quad (1)$$

Essa regra significa que o PSL de um caminho é diretamente proporcional à

taxa de energia do caminho, ao tamanho da chave de criptografia utilizada pelos nós, à reputação e ao grau do caminho. Entretanto, ele é inversamente proporcional ao tamanho do caminho e ao tempo de expiração dos certificados digitais.

No *nível de enlace*, o protocolo HMCLL seleciona os canais a serem utilizados com base em informações coletadas pelos seus pacotes de controle. Ele assume que um nó possui ao menos dois rádios, sendo um deles utilizado para a transmissão e o outro para a recepção de dados. Cada um dos rádios opera em um canal diferente. Assim, cabe ao bloco de controle selecionar o melhor canal para a recepção de dados, enquanto o canal a ser utilizado pelo rádio de transmissão é determinado pelos vizinhos do nó. O algoritmo de seleção de canais é implementado assumindo que todas as decisões de seleção são sequenciais em diferentes nós. Assim, cada rádio possui um temporizador de redefinição de canais o qual é reagendado seguindo uma distribuição uniforme aleatória. Para cada um dos canais, o nó calcula uma métrica que inclui o somatório de quatro custos: a interferência detectada explicitamente, os conflitos de rádio, a contenção e o custo esperado para a chegada de tráfego. Por fim, o algoritmo seleciona o canal com o menor custo.

4.3. Os procedimentos de segurança

Neste esquema de seleção de caminhos, pelo menos um dos mecanismos de cada linha de defesa deve ser empregado no bloco de segurança. A criptografia e uma Infraestrutura de Chave Pública (ICP) distribuída, como a definida em [Wang et al. 2008], protegem os valores dos critérios de segurança e de desempenho armazenados nos CPACKs. Já um sistema de reputação, como o modelo proposto em [Pirzada and McDonald 2006], calcula o grau de confiabilidade de um nó vizinho com base no seu comportamento prévio no encaminhamento dos pacotes de dados. Por fim, um protocolo de roteamento capaz de manter múltiplos caminhos, como o AOMDV, aumenta a tolerância a ataques.

Dessa forma, esses mecanismos de segurança garantem as propriedades da sobrevivência, isto é, a criptografia e a ICP asseguram a *resistência*; o sistema de reputação assegura o *reconhecimento*; e os múltiplos caminhos asseguram a *recuperação* em resposta à ação de atacantes.

4.4. Os procedimentos de reconfiguração

No *nível de rede*, após o bloco de controle calcular os valores de PSL, o bloco de reconfiguração classifica os caminhos em ordem decrescente pelo valor de PSL. Em seguida, ele seleciona o primeiro caminho da lista para uso e envia essa informação ao agente do bloco da camada de rede, o qual inicia o monitoramento do caminho.

O caminho selecionado é utilizado até que ocorra a quebra de um enlace ou o término de uma nova coleta de dados dos critérios. Se o caminho se quebrar antes, o próximo caminho da lista é selecionado e o agente do bloco da camada de rede é notificado. Contudo, se após um novo procedimento de coleta os novos valores modificam a classificação dos caminhos, o bloco de reconfiguração adaptará o nó para que este utilize o caminho mais seguro e eficiente.

No *nível de enlace*, se o bloco de controle selecionar um canal diferente daquele utilizado em um dado momento, o bloco de reconfiguração executa a troca da frequência do rádio. Após as alterações, o nó envia um pacote de controle anunciando aos seus vizinhos o seu novo canal de recepção.

4.5. Os procedimentos de comunicação *cross-layer*

Após o esquema de seleção de caminhos definir o caminho a ser utilizado, a camada de rede informa às camadas inferiores o nó origem, o nó destino e o próximo salto. Sabendo o próximo salto no caminho, o protocolo HMCLL define o rádio e o canal a serem usados para a transmissão de pacotes. O protocolo HMCLL é considerado como um protocolo da camada intermediária entre as camadas de rede e de enlace, realizando a correlação e a cooperação entre elas.

4.6. Os procedimentos de avaliação de desempenho

O esquema de seleção de caminhos avalia o desempenho dos canais e dos rádios através de estatísticas. Os canais de transmissão podem se tornar um gargalo devido à sobrecarga de tráfego, já os rádios podem se tornar um gargalo em razão da sobrecarga de tráfego na transmissão. Essas informações são coletadas através do bloco de cooperação, no qual o protocolo HMCLL analisa as condições de tráfego para a gerência dos canais e dos rádios.

4.7. Os procedimentos dos agentes das camadas de rede e de enlace

O agente da camada de rede monitora o caminho selecionado no estado de reconfiguração. Em caso de falha do caminho, o nó retorna ao estado de reconfiguração para a escolha de um novo. Da mesma forma, o agente da camada de enlace monitora as condições dos rádios e dos canais através de pacotes de controle. Além disso, esses agentes atualizam a tabela de vizinhos e dos seus canais de recepção.

5. Avaliações

A avaliação do esquema de seleção de caminhos baseado no SECOM foi realizada através de simulações usando o simulador NS-2 versão 2.30. Assume-se uma área de 2.500m x 2.500m, onde 25 roteadores *mesh* são distribuídos em *grid* para compor a malha sem fio. Além disso, 50 clientes *mesh* se movimentam seguindo o modelo de mobilidade *random waypoint*, com velocidade máxima de 1 m/s e sem pausas. Esse modelo foi usado para provocar variações no grau dos nós durante as simulações [Royer et al. 2001].

Na camada de rede, o protocolo de roteamento AOMDV foi modificado para suportar o esquema de seleção de caminhos proposto. O protocolo AOMDV foi usado devido à sua capacidade de manter múltiplos caminhos, diferente do protocolo OLSR, normalmente usado em redes *mesh*. As simulações comparam a versão modificada, que chamamos AOMDV-PSL, com os protocolos AODV e AOMDV originais diante de 0%, 10%, 20%, 30% e 50% de atacantes. Neste caso, tanto o AOMDV quanto o AOMDV-PSL mantêm até 5 caminhos nós-disjuntos, e o AODV mantém apenas um. Os nós maliciosos lançam o ataque *Blackhole* para prejudicar o roteamento descartando todo o tráfego de dados enviado por outros nós.

Na camada de enlace, o protocolo HMCLL é utilizado para gerenciar os rádios e canais. Cada nó da rede é equipado com dois rádios, que operam na banda de 5GHz ISM e seguem o padrão IEEE 802.11a com 12 canais ortogonais entre si. Os rádios têm potência de transmissão de 65 mW (18 dBm) e executam o DCF (*Distributed Coordination Function*) para o acesso ao meio (MAC) sem a troca de pacotes RTS/CTS. A capacidade da fila em cada rádio é de 100 pacotes. Os nós utilizam uma Infraestrutura de Chave Pública como a definida em [Wang et al. 2008] onde cada nó faz a autenticação da chave com

um roteador da malha sem fio, garantindo o controle do acesso de novos clientes. Um sistema de confiabilidade analisa o comportamento de nós vizinhos no encaminhamento de pacotes de dados para atribuir valores de reputação [Pirzada and McDonald 2006].

Um total de 20 nós origem escolhidos aleatoriamente geram tráfego de dados CBR (*Constant Bit Rate*) a uma taxa de 100 pacotes por segundo. Cada pacote de dados possui 512 bytes de carga útil (*payload*), e as sessões ocorrem em instantes aleatórios dentro de um intervalo de 150s de simulação. Cada ponto nos gráficos indica a média de 30 rodadas, com um intervalo de confiança de 95%.

A análise dos ganhos de desempenho e de segurança do esquema de seleção de caminhos no serviço de roteamento utilizou cinco métricas. A taxa de entrega de pacotes (PDR), que mede a proporção de pacotes de dados entregues com sucesso aos nós destino sobre a quantidade total de pacotes de dados enviados pelos nós origem. O atraso fim a fim dos pacotes de dados (E2E *delay*), que calcula o atraso de transmissão dos pacotes de dados entregues corretamente. Essa métrica inclui os atrasos de propagação, enfileiramento nos rádios e retransmissões na camada MAC. A sobrecarga de roteamento (RO), que consiste na quantidade de pacotes de controle transmitidos, e é medida em milhares de pacotes. A taxa de descartes maliciosos (MDR), que é a razão entre a quantidade de pacotes de dados descartados por atacantes e a quantidade total de pacotes de dados descartados na rede. A quantidade de pacotes de dados descartados devido a ataques (APDA), que é medida em milhares de pacotes.

5.1. Resultados e Análises

A Figura 3(a) mostra os resultados para a PDR com a variação do percentual de atacantes na rede. Como esperado, altos percentuais de atacantes diminuem a PDR de todos os protocolos. Entretanto, o AOMDV-PSL alcança os melhores resultados independentemente do percentual de atacantes. A PDR alcançada pelo AOMDV-PSL é em torno de 10% maior do que a PDR obtida pelos protocolos AODV e AOMDV quando o percentual de atacantes é menor do que 20%.

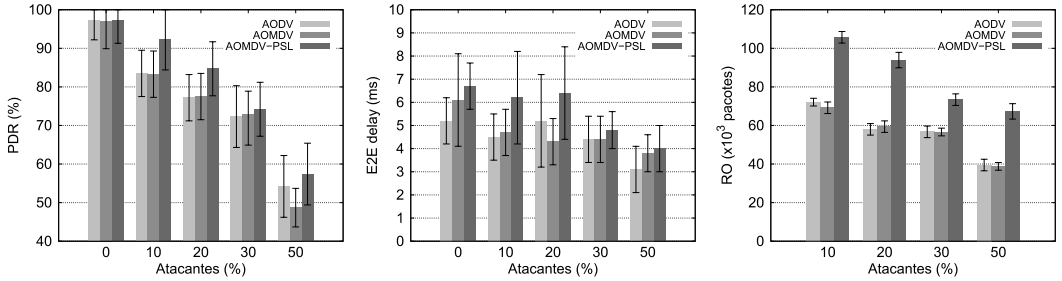

Figura 3. Desempenho *versus* ataque *Blackhole*

Para altos percentuais de atacantes (30% ou acima), a PDR alcançada pelo AOMDV-PSL tende a ser ligeiramente melhor do que a PDR obtida pelo AODV. Esse comportamento ocorre porque o alto percentual de atacantes reduz a quantidade de caminhos seguros, e a tendência é que os protocolos apresentem resultados de PDR similares. Observou-se que o AODV e o AOMDV obtêm desempenhos semelhantes independentemente do percentual de atacantes na rede. Isso ocorre porque o núcleo da rede,

composto pelos roteadores *mesh*, não se altera com frequência. Assim, os enlaces não quebram facilmente, o que diminui o uso de caminhos alternativos do AOMDV.

A Figura 3(b) apresenta os resultados para o E2E *delay*. Nesse caso, são comparadas as latências dos protocolos na entrega de dados quando a rede possui diferentes percentuais de atacantes. Observou-se que o E2E *delay* diminui com o aumento desses percentuais. Isso ocorre devido à redução do tráfego de dados e de controle provocada pelos descartes nos atacantes. Por outro lado, quanto menor é o percentual de atacantes, maior é o E2E *delay* na entrega dos pacotes de dados. Percebeu-se ainda que o E2E *delay* obtido pelo AOMDV-PSL é maior do que aqueles obtidos pelos outros protocolos. Uma análise inicial pode levar à conclusão de que o AOMDV-PSL reduz o desempenho da rede. Contudo, como discutido anteriormente, o AOMDV-PSL entrega mais pacotes de dados aos nós destino do que os outros protocolos, o que mantém por mais tempo o tráfego de dados e de controle na rede.

A Figura 3(c) compara a sobrecarga de roteamento gerada pelos três protocolos quando a rede apresenta diferentes percentuais de atacantes. Como era esperado, o protocolo AOMDV-PSL produz mais pacotes de controle do que os outros protocolos devido ao procedimento de coleta dos valores dos critérios. Ainda verificou-se que a RO diminui com o aumento do percentual de atacantes. Isso ocorre porque o descarte de tráfego de dados nos atacantes diminui a quantidade de pacotes de controle do roteamento na rede.

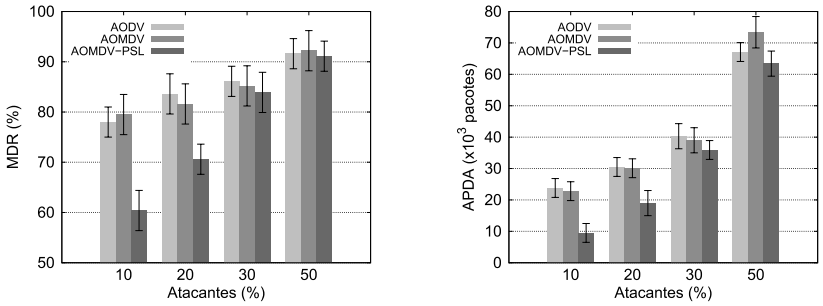

Figura 4. Segurança *versus* ataque *Blackhole*

A Figura 4(a) apresenta o percentual de pacotes de dados descartados para diferentes percentuais de atacantes. Quando a rede possui 10% e 20% de atacantes, o protocolo AOMDV-PSL diminui a perda de pacotes de dados. Os resultados do AOMDV-PSL mostram reduções na MDR de 10% até 20% em comparação aos valores de MDR do AODV e do AOMDV. Isso significa que menos pacotes de dados são descartados pelos atacantes. Quando o percentual de atacantes é maior do que 20%, mais caminhos ficam comprometidos, diminuindo a diferença entre a MDR do AOMDV-PSL e a MDR dos outros protocolos.

A Figura 4(b) confirma esses argumentos relacionados ao comportamento da MDR. Ela mostra que o protocolo AOMDV-PSL reduz a APDA independentemente do percentual de atacantes na rede. Os ganhos de APDA do AOMDV-PSL variam de 36% até 57% em comparação à APDA alcançada pelos outros protocolos quando a rede possui entre 10% e 20% de atacantes.

6. Conclusões

Este trabalho apresentou o arcabouço SECOM para a autoconfiguração de serviços essenciais em redes *mesh* a fim de prover segurança e desempenho simultaneamente. O SECOM busca manter o funcionamento dos serviços essenciais mesmo diante de ataques ou intrusões através da ação coordenada e adaptativa entre as defesas preventiva, reativa e tolerante. Para isso, ele possui blocos funcionais que representam as operações de controle, reconfiguração, cooperação, segurança, comunicação, avaliação de desempenho e gerenciamento das camadas da pilha de protocolos.

O arcabouço SECOM foi aplicado no desenvolvimento de um serviço de roteamento seguro e eficiente para redes *mesh* diante de ataques *Blackhole*. Esse serviço define um esquema de seleção que determina os caminhos com os maiores graus de segurança e desempenho, considerando informações de mecanismos de segurança, condições de rádios e canais, e a diversidade de caminhos. Resultados obtidos via simulação mostram as melhorias do esquema em termos de desempenho e redução do impacto dos ataques *Blackhole* com um baixo custo de latência. Como trabalhos futuros, avaliaremos a eficiência do SECOM contra outros tipos de ataques, melhoraremos os aspectos de cooperação do SECOM para minimizar a sua sobrecarga, e incluiremos outros critérios no esquema de seleção de caminhos.

Referências

Akyildiz, I. and Wang, X. (2005). A survey on wireless mesh networks. *IEEE Communications Magazine*, 43(9):23–30.

Al-Mashaqbeh, G. A., Al-Karaki, J. N., and Bataineh, S. M. (2009). Clear: A cross-layer enhanced and adaptive routing framework for wireless mesh networks. *Wireless Personal Communications*, 51(3):449–482.

Bhandari, V. and Vaidya, N. H. (2009). Channel and interface management in a heterogeneous multi-channel multi-radio wireless network. Technical report, UIUC, Illinois, USA.

Brunner, M., Dudkowski, D., Mingardi, C., and Nunzi, G. (2009). Probabilistic decentralized network management. In *IFIP/IEEE International Conference on Symposium on Integrated Network Management (IM)*, pages 25–32.

Bruno, R., Conti, M., and Gregori, E. (2005). Mesh networks: commodity multihop ad hoc networks. *IEEE Communications Magazine*, 43(3):123–131.

Campista, M., Passos, D., Esposito, P., Albuquerque, C., Saade, D., Rubinstein, M., Costa, L., and Duarte, O. (2008). Routing metrics and protocols for wireless mesh networks. *IEEE Network*, 22(1):6–12.

Carvalho, C. B. and Rezende, J. F. (2010). Roteamento em redes em malha sem fio IEEE 802.11 com adaptação de largura de canal. In *Simpósio Brasileiro de Redes de Computadores (SBRC)*, pages 161–174.

Dressler, F. (2008). A study of self-organization mechanisms in ad hoc and sensor networks. *Computer Communications*, 31(13):3018–3029.

Gillies, D., Thornley, D., and Bisdikian, C. (2009). Probabilistic approaches to estimating the quality of information in military sensor networks. *The Comp. Journal*, 52(3):1–10.

Glass, S., Portmann, M., and Muthukkumarasamy, V. (2008). Securing wireless mesh networks. *IEEE Internet Computing*, 12(4):30–36.

Heegaard, P. E. and Trivedi, K. S. (2009). Network survivability modeling. *Computer Networks*, 53(8):1215–1234.

Khan, S., Loo, K.-K., and Mast, N. (2010). SRPM: Secure routing protocol for IEEE 802.11 infrastructure based wireless mesh networks. *Journal of Network and Systems Management*, 18(2):109–209.

Kyasanur, P., So, J., Chereddi, C., and Vaidya, N. (2006). Multichannel mesh networks: challenges and protocols. *IEEE Wireless Communications*, 13(2):30–36.

Lima, M., Pujolle, G., Silva, E., Santos, A., and Albini, L. (2009). Survivable keying for wireless ad hoc networks. In *IFIP/IEEE International Conference on Symposium on Integrated Network Management (IM)*, pages 606–613.

Lima, M., Silva, H., Santos, A., and Pujolle, G. (2008). An architecture for survivable mesh networking. In *IEEE GLOBECOM*, pages 688–692.

Martignon, F., Paris, S., and Capone, A. (2009). Design and implementation of MobiSEC: a complete security architecture for wireless mesh networks. *Computer Networks*, 53(12):2192–2207.

Pirzada, A. A. and McDonald, C. (2006). Trust establishment in pure ad-hoc networks. *Wireless Personal Communications*, 37(1–2):139–163.

Pras, A., Schoenwaelder, J., Burgess, M., Festor, O., Perez, G. M., Stadler, R., and Stiller, B. (2007). Key research challenges in network management. *Communications Magazine*, 45(10):104–110.

Royer, E., Melliar-Smithy, P., and Moser, L. (2001). An analysis of the optimum node density for ad hoc mobile networks. In *IEEE International Conference on Communications (ICC)*, pages 857–861.

Seth, S. and Gankotiya, A. (2010). Denial of service attacks and detection methods in wireless mesh networks. *International Test Conference*, 0:238–240.

Shillingford, N. and Poellabauera, C. (2010). A framework for route configurability in power-constrained wireless mesh networks. *Ad Hoc Networks*, 8(8):857–871.

Wang, X., Wong, J., and Zhang, W. (2008). A heterogeneity-aware framework for group key management in wireless mesh networks. In *International Conference on Security and Privacy in Communication Networks (SecureComm)*, pages 1–6.

Yuan, Y., Wong, S., Lu, S., and Arbaugh, W. (2005). ROMER: resilient opportunistic mesh routing for wireless mesh networks. In *IEEE Workshop on Wireless Mesh Networks (WiMesh)*.