Mitigação de Ataques de Inundação para Redes em Malha sem Fio usando Reputação e *Filtering*

Flávio Arieta, Larissa Barabasz, Michele Nogueira

[1]Núcleo de Redes sem Fio e Redes Avançadas (NR2)
Universidade Federal do Paraná (UFPR)

{fan10,ltb08,michele}@inf.ufpr.br

Abstract. *Wireless mesh networks (WMNs) have being applied in different social contexts, such as health care, transportation and entertainment. These networks support tecnological convergence and resilience, required for the effective operation of those aplications. However, WMNs are prone to attacks that compromise mobility management and network access. This work proposes MIRF, a security scheme based on reputation and filtering to mitigate flooding attacks on mobility management of wireless mesh networks. The efficiency of the MIRF scheme has been evaluated by simulations considering scenarios with and without attacks. Analyses show that it significantly improves the packet delivery ratio in scenarios with attacks, mitigating their intentional negative effects, as the reduction of malicious ARP requests. Furthermore, improvements have been observed in the number of handoffs on scenarios under attacks, being faster than scenarios without the scheme.*

Resumo. *As redes em malha sem fio vêm sendo aplicadas em diferentes contextos sociais, tais como saúde, transporte e entretenimento. Essas redes possuem características natas suportando a convergência tecnológica e a resiliência, necessárias para o funcionamento efetivo dessas aplicações. Entretanto, as redes em malha sem fio são alvos de ataques que comprometem o gerenciamento da mobilidade e o acesso à rede. Desta forma, este trabalho propõe MIRF, um esquema de segurança para* **M***itigação de ataques de* **I***nundação em redes em malha sem fio com base em* **R***eputação e* **F***iltering. O esquema MIRF foi avaliado através de simulações considerando cenários com e sem ataques. Os estudos realizados mostram que o esquema melhora significativamente a taxa de entrega de pacotes diante de ataques, mitigando seus efeitos negativos, como a redução nas requisições ARP maliciosas. Por fim, melhorias foram observadas nas operações de handoffs em cenários sob ataques, sendo mais rápidos do que nos cenários sem a adoção do esquema.*

1. Introdução

As redes em malha sem fio são uma importante alternativa para a comunicação de dados. Essas redes são compostas por roteadores e clientes *mesh* (nós), apoiadas por uma comunicação multissalto de topologia dinâmica e com suporte à mobilidade [Akyildiz et al. 2005]. O *backbone* dessas redes é formado por roteadores *mesh* (*mesh routers – MRs*), sendo a comunicação entre estes nós realizada unicamente via interface sem fio. Estes nós são constituídos de interfaces de diferentes tecnologias de comunicação

e dotados de mobilidade mínima, atendendo às requisições dos usuários (os clientes *mesh* ou *mesh clients – MCs*). Os roteadores possuem funcionalidades de *gateways* e pontes, permitindo a interligação com outras redes, tais como as redes locais sem fio e a Internet.

Essas redes são autoconfiguráveis, provendo resiliência, tolerância a falhas e capacidade de adaptação às alterações em sua topologia. Essas vantagens tornam as redes em malhas uma interessante solução para a comunicação de dados, suportando o uso crescente dos mais diversos dispositivos móveis, a convergência tecnológica e a mobilidade. Com o avanço das tecnologias sem fio e o fácil acesso a dispositivos portáteis, a mobilidade em redes sem fio exerce uma grande importância. Para que a mobilidade seja possível, são necessários mecanismos que garantam a disponibilidade dos serviços aos usuários requerendo acesso à Internet a partir de seus respectivos dispositivos móveis, de forma contínua sem restringir sua movimentação. O desafio em questão é garantir a transparência, ou seja, que todo o processo de mobilidade seja imperceptível às aplicações e, consequentemente, aos usuários. Para tal, se faz necessária a existência de um gerenciamento de mobilidade efetivo e seguro.

Nas redes em malha sem fio, a segurança na gerência de mobilidade é um campo ainda pouco tratado. A privacidade, a disponibilidade, a justiça, o não-repúdio e o controle de acesso são requisitos de segurança que dizem respeito às redes em malha [Egners and Meyer 2010]. Estes estão estritamente associados ao cenário de utilização e às características dessas redes, tais como o dinamismo e a heterogeneidade de seus componentes. A mobilidade dos nós na rede é suscetível a ameaças de segurança que visam comprometer a disponibilidade, prejudicando o ingresso e a manutenção de clientes *mesh* na rede. A disponibilidade pode ser afetada por ações que objetivem sobrecarregar a rede ou indisponibilizar as atividades dos roteadores *mesh*.

Como as soluções de gerenciamento de mobilidade existentes para as redes locais sem fio não atendem por completo aos requisitos de segurança das redes em malha, se faz necessário o projeto de soluções específicas que considerem as diferenças entre estas redes. Desta forma, este artigo apresenta o esquema MIRF (**M**itigação de ataques de **I**nundação em redes em malha sem fio com base em sistemas de **R**eputação e **F**iltering) cujo objetivo consiste em prover serviços essenciais relacionados ao gerenciamento de mobilidade mesmo na presença de ataques contra ARP (*Address Resolution Protocol*), um dos ataques mais comprometedores para o gerenciamento de mobilidade nessas redes [Barabasz and Nogueira 2011]. Além disso, busca-se garantir os serviços relacionados à gerência da mobilidade durante o máximo de tempo possível diante de ataques e também promover a capacidade de recuperação dos serviços afetados em tempo hábil. Para tal, MIRF baseia-se no gerenciamento de confiança entre os nós, particularmente na técnica de reputação, e em *filtering*, o mecanismo de autorreação adotado.

O artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados ao gerenciamento de mobilidade e às arquiteturas de segurança nas redes em malha sem fio. A Seção 3 detalha o funcionamento do esquema proposto, descrevendo os seus pressupostos e a visão geral do esquema. A Seção 4 detalha a avaliação do esquema. Por fim, a Seção 5 apresenta as conclusões e direções futuras.

2. Trabalhos Relacionados

O gerenciamento de endereços, uma das questões de projeto do gerenciamento de localização, tem por finalidade permitir a identificação de um nó móvel na rede durante a sua movimentação. Nas redes em malha sem fio, essa identificação deve ocorrer tanto interna quanto externamente, ou seja, no *backbone mesh* e no domínio da Internet. A inalteração do endereço IP de um cliente *mesh*, permite que, após a ocorrência de *handoffs*, as comunicações UDP e TCP deste nó sejam mantidas. Os protocolos como Mobile IP e iMesh [Xie and Wang 2008], por sua vez, são soluções que permitem ao cliente a manutenção do seu endereço IP sem restrições de mobilidade.

A mobilidade e o roteamento são tratados independentemente nos mecanismos de gerenciamento de mobilidade [Xie and Wang 2008]. Essa abordagem clássica pode levar a tarefas de processamento desnecessárias e a redundâncias de funções. Essas questões poderiam ser evitadas caso a mobilidade e o roteamento se complementassem, ou seja, caso existisse uma abordagem conjunta entre ambos. Uma abordagem nesta direção foi desenvolvida no protocolo Mobile Party [Mehdi et al. 2007], cuja solução faz uso de uma estrutura de árvore de endereços para lidar com a mobilidade e o roteamento.

Soluções de gerenciamento de mobilidade que tratam de questões de segurança não são conhecidas. Em geral, para suprir as necessidades de segurança em protocolos de gerência de mobilidade, uma arquitetura de segurança deve ser adotada. Entretanto, as arquiteturas de segurança propostas não são direcionadas particularmente a protocolos de gerenciamento de mobilidade. Assim sendo, essas soluções desconsideram as especificidades dos protocolos com os quais estão trabalhando. MobiSEC [Martignon et al. 2008] é uma dentre as arquiteturas de segurança propostas. Essa arquitetura provê um arcabouço completo para lidar com as questões de segurança relativas ao *backbone* e ao acesso à redes em malha. Esta arquitetura, por sua vez, se enquadra como uma solução de segurança genérica.

A questão mobilidade versus segurança nos protocolos de gerenciamento de mobilidade ainda tem muito a ser explorada. Neste artigo, um esquema de segurança para o gerenciamento de mobilidade é proposto. Ele visa a mitigar ataques de inundação de pacotes ARP maliciosos gerados para comprometer *handoffs* (transferência de um nó móvel associado a um roteador mesh a outro).

3. MIRF - Esquema para Mitigação de Ataques de Inundação

Esta seção apresenta MIRF, um esquema para **M**itigação de ataques de **I**nundação em redes em malha sem fio com base em **R**eputação e ***F**iltering*. O esquema MIRF tem como principal objetivo prover segurança a gerência de mobilidade em redes em malha sem fio. O esquema visa garantir a disponibilidade dos mecanismos destinados ao suporte à mobilidade diante de ataques de Negação de Serviço via ARP, por serem os mais comprometedores no gerenciamento de mobilidade dessas redes [Barabasz and Nogueira 2011]. O esquema MIRF concilia duas técnicas de segurança: *filtering* e *grau de confiança*.

3.1. Premissas

O funcionamento do MIRF requer a existência de um protocolo eficiente para autenticação dos nós participantes na rede e a cooperação entre os roteadores mesh (*mesh*

routers – MRs). O esqueme MIRF necessita de garantias sobre a legitimação dos pacotes processados pelos nós MRs para que as informações referentes ao monitoramento e ao gerenciamento de confiança sejam mantidas e atualizadas corretamente. Para isso, deve-se garantir que os endereços IPs contidos nos cabeçalhos dos pacotes sejam válidos, impossibilitando assim ataques baseados em IP *spoofing* na rede. Portanto, supõe-se a existência de mecanismos de prevenção de acesso não-autorizado de nós clientes e nós roteadores na rede, sendo o primeiro passo a adoção de técnicas que visem à autenticação e à autorização [Sen 2012] de nós na rede. Além disso, com a adoção de técnicas para garantir a autenticação tanto dos nós clientes quanto dos nós roteadores na rede, parte-se do princípio de que todos os nós MRs, autenticados, são também cooperativos entre si.

3.2. Visão geral do esquema

O MIRF possui duas fases denominadas de **fase subjetiva** e **fase objetiva**. Na fase subjetiva, os roteadores mesh calculam o grau de confiança dos clientes mesh anexados a eles com base no histórico local das transações com cada um desses nós. Desta forma, é considerada a opinião direta do roteador que provê o acesso à rede ao cliente. Na fase objetiva, esse mesmo cálculo é realizado considerando não apenas a opinião direta, mas também as opiniões indiretas, ou seja, as opiniões que outros nós roteadores vizinhos possuem sobre o nó cliente. Entretanto, essa última fase será executada apenas quando o grau de confiança atribuído pelo roteador ao nó cliente esteja abaixo de um limiar mínimo.

As opiniões indiretas recebidas na fase objetiva são agregadas aos dados previamente coletados pelo nó MR sobre o nó MC.Essa agregação é realizada através de uma função de agregação/mapeamento que obtém o grau de confiança final referente ao nó MC. A partir dessa informação, é possível combinar todos os dados que o nó MR possui a respeito do nó MC, analisado ao fim do processo. Por fim, a confiança resultante desse processo é utilizada pelo nó MR para definir se um mecanismo de defesa deve ou não ser acionado. As subseções seguintes detalham as duas fases envolvidas no MIRF. Os diferentes símbolos utilizados são apresentados nas Tabelas 1 e 2.

Variável	Significado
μ_{ij}	Frequência de requisições ARP observadas no nó MR i sobre o nó MC j
α_{ij}	Grau de confiança do tráfego ARP atribuído pelo nó MR i ao nó MC j
β_{ij}	# vezes que um nó MC i foi classificado como malicioso pelo nó MR j
λ_{ij}	Instante da última mensagem ARP processada no nó MR i do nó MC j
γ_{ij}	Situação atual do nó: confiável, não-confiável ou em análise

Tabela 1. Variáveis utilizadas na descrição do esquema MIRF

3.3. Fase Subjetiva

Nesta fase, todos os clientes são monitorados pelos nós MRs responsáveis por prover seu acesso. Um nó MR, ao ter um cliente conectado, além de lhe garantir o acesso aos recursos da rede, também é responsável pela atribuição do grau de confiança baseando-se, estritamente, nas informações coletadas a partir do monitoramento individual do tráfego ARP do cliente em questão. Essas tarefas têm início no ato da associação de um nó MC à um no MR e se estendem pelo tempo em que esse roteador servir como ponto de acesso do nó MC à rede. No caso de *handoffs*, as tarefas referentes ao monitoramento e ao acesso

Constante	Significado
Υ_{MAX}	Valor máximo aceitável para a frequência de requisições ARP por ciclo
$\mathrm{M}_{\mathrm{MIN}}$	Tempo mínimo de duração de um ciclo ARP
$\mathrm{L}_{\mathrm{MAX}}$	Tempo mínimo de espera para o recebimento de respostas ao chamar o método de requisição de opiniões
$\mathrm{K}_{\mathrm{MIN}}$	Grau de confiança mínimo para um nó MC ser considerado confiável
Γ_{ARP}	Peso dos pacotes ARP no incremento ou decremento do grau de confiança de um nó MC
$\mathrm{N}_{\mathrm{DEF}}$	Tempo de punição padrão para um nó MC classificado como malicioso com relação ao seu tráfego ARP

Tabela 2. Constantes utilizadas na descrição do esquema MIRF

à rede são transferidas ao novo nó MR que servir como ponto de acesso do nó MC. As tarefas referentes ao monitoramento e, posteriormente, à atribuição do grau de confiança a partir das informações locais a respeito do cliente, caracterizam a fase subjetiva do MIRF. Esta fase é dividida nas etapas: inicialização, monitoramento, avaliação da reputação e análise parcial. Tais etapas são apresentadas a seguir.

3.3.1. Inicialização

Após a associação bem-sucedida do cliente à um nó MR, tem-se início etapa de inicialização, onde o nó MR é responsável por atribuir valores padrões iniciais aos dados referentes ao grau de confiança e aos dados necessários ao monitoramento do nó MC. Para fins de simplificação, no MIRF, um nó MR sempre será referido pela variável i, enquanto que um nó MC será referido pela variável j. Assim, as informações pertinentes ao grau de confiança do nó MC j atribuídas pelo nó MR i consistem no grau de confiança, α_{ij}, na situação do nó MC na rede, γ_{ij}, e na quantidade de vezes que o nó MC foi classificado como malicioso, β_{ij}.

O grau de confiança do nó MR i sobre o nó MC j é definido como α_{ij}, em que $\alpha_{\mathrm{ij}} \in \mathbb{Q} \ / \ 0 \leq \alpha_{\mathrm{ij}} \leq 1$, sendo 1 o valor de confiança máximo que um nó MC pode assumir, e 0 é o valor mínimo. A fim de garantir que todos os clientes tenham oportunidade igual na rede no início da comunicação com um roteador, o valor inicial atribuído à α_{ij} é 0,5. Para os valores referentes à γ_{ij} e à β_{ij}, são atribuídos, respectivamente, o estado GREEN_STATE, que é o estado atribuído a um nó MC considerado confiável, e o valor 0. Os dados referentes ao monitoramento do nó MC j pelo nó MR i consistem na frequência de requisições ARP recebidas, μ_{ij}, no instante da última mensagem ARP processada, λ_{ij}, e na quantidade de pacotes recebidos por ciclo, ω_{ij}. As variáveis μ_{ij} e ω_{ij} são inicializadas com o valor 0, e à λ_{ij} é atribuído o instante de tempo atual, $\mathrm{I}_{\mathrm{ATUAL}}$, em que a associação foi estabelecida. Após a inicialização das variáveis, a etapa de monitoramento é iniciada.

3.3.2. Monitoramento

O nó MR, responsável por garantir o acesso à rede a um nó MC, o monitora com relação ao seu tráfego de requisições ARP. Tais requisições são utilizadas na associação aos MRs na iminência de sua mobilidade. Esses pacotes são referentes ao fluxo *upstream*, assim

sendo, serão analisados na chegada ao nó MR. Com o intuito de poupar processamentos desnecessários, tomou-se a decisão de analisar o tráfego e calcular o grau de confiança aos clientes apenas quando, e se, houver atividade relacionada ao tráfego ARP.

O processo realizado no recebimento de uma mensagem do tipo requisição ARP começa quando o roteador acusa o recebimento de uma dessas mensagens provenientes de um nó MC, e este está conectado a ele. A primeira ação tomada é a atualização da quantidade de requisições ARP recebidas, ω_{ij}. Já com relação ao cálculo da frequência de requisições ARP, μ_{ij}, esta é orientada a ciclos. Seja λ_{ij} o instante em que a última mensagem do tipo requisição ARP foi recebida pelo nó MR i, proveniente do nó MC j, e seja $\mathrm{I}_{\mathrm{ATUAL}}$ o instante de recebimento de uma requisição ARP. Se a próxima mensagem for recebida no instante $\mathrm{I}_{\mathrm{ATUAL}}$, e se $\mathrm{I}_{\mathrm{ATUAL}} - \lambda_{\mathrm{ij}} \geq \mathrm{M}_{\mathrm{MIN}}$, ou seja, se o tempo de duração do ciclo exceder o tempo mínimo de duração definido para um ciclo ARP, então se tem o término de um ciclo. Assim, obtêm-se uma amostra a ser analisada. A cada término de ciclo, é realizado o cálculo da frequência de requisições ARP, μ_{ij}. Dessa forma, μ_{ij} será relativa ao tráfego de requisições ARP no intervalo de tempo $\Delta \mathrm{c}_{\mathrm{ij}}$.

No término de um ciclo, a frequência de requisições ARP desse ciclo é finalmente calculada. O valor final obtido μ_{ij} representa quantas mensagens do tipo requisição ARP foram enviadas a cada segundo durante o ciclo em questão. Logo após o cálculo da frequência de requisições ARP no ciclo, o valor obtido serve então de base para o cálculo da confiança. A etapa seguinte exemplifica como o cálculo é efetuado.

3.3.3. Avaliação da Reputação

Seja um ciclo definido como o intervalo de tempo em que foram coletadas as informações a respeito do comportamento de um nó MC por parte de um nó MR. Assim como o cálculo da frequência de requisições ARP, μ_{ij}, o cálculo do grau de confiança é realizado no término de um ciclo. Ao tomar como base μ_{ij}, previamente calculado na etapa anterior, é realizada a atualização do grau de confiança do nó MC em questão. A partir desse valor, duas ações podem ser realizadas: se a frequência de requisições ARP se apresentar acima do valor considerado aceitável, ou seja, $\mu_{\mathrm{ij}} \geq \Upsilon_{\mathrm{MAX}}$, então o grau de confiança desse nó MC é decrementado; caso contrário, é incrementado. As equações 1a e 1b foram utilizadas para a atualização do grau de confiança do nó MC.

A Equação 1a representa a fórmula utilizada para o incremento, ao passo que a Equação 1b representa a fórmula para o decremento. O valor a ser incrementado ou decrementado do grau de confiança é definido por uma constante, Γ_{ARP}, sendo este diretamente proporcional ao tempo total de duração do ciclo em questão, $\Delta \mathrm{c}_{\mathrm{ij}}$. Dessa forma, ao considerar ambos os valores Γ_{ARP} e $\Delta \mathrm{c}_{\mathrm{ij}}$ nas fórmulas, quanto mais duradouro for o ciclo em questão, maior será a influência exercida no resultado obtido.

$$\alpha_{\mathrm{ij}} = \alpha_{\mathrm{ij}} + \Delta \mathrm{c}_{\mathrm{ij}} * \Gamma_{\mathrm{ARP}} \tag{1a}$$

$$\alpha_{\mathrm{ij}} = \alpha_{\mathrm{ij}} - \Delta \mathrm{c}_{\mathrm{ij}} * \Gamma_{\mathrm{ARP}} \tag{1b}$$

A partir do novo grau de confiança obtido, pode-se atribuir dois possíveis estados para γ_{ij}: GREEN_STATE ou YELLOW_STATE. Ainda há outro possível estado, o

RED_STATE, porém, na fase subjetiva, ainda não cabe ao nó MR definir esse estado ao nó MC. Cada um dos estados que um nó MC pode assumir é definido como:

- GREEN_STATE — Se $\alpha_{ij} \geq K_{MIN}$, então $\gamma_{ij} = GREEN\_STATE$;
- YELLOW_STATE — Se $\alpha_{ij} < K_{MIN}$, então $\gamma_{ij} = YELLOW\_STATE$;
- RED_STATE — Se, na fase objetiva, $\alpha_{ij_{FINAL}} < K_{MIN}$, então $\gamma_{ij_{FINAL}} = RED\_STATE$. O tempo total de punição na rede, por sua vez, é definido como $\beta_{ij} * N_{DEF}$.

3.3.4. Análise Parcial

Nessa etapa, é possível atribuir ao nó MC dois estados: GREEN_STATE ou YELLOW_STATE. Um nó MR i classifica um nó MC j como GREEN_STATE quando o tráfego de requisições ARP está dentro do aceitável. O nó MC j, então definido como confiável, pode usufruir integralmente dos recursos da rede. O monitoramento do tráfego de um nó MC perdura até que este se desligue da rede ou realize *handoff*, transferindo assim a tarefa de monitoramento ao novo nó MR que lhe servirá como ponto de acesso.

Caso o nó MR classifique o nó MC como YELLOW_STATE, o processo de requisição de opiniões deve ser inicializado, definindo então o início da fase objetiva. Até que essa segunda fase determine se o nó MC analisado é ou não malicioso, esse ainda possui acesso total à rede durante o período em que essa fase estiver em vigor.

Quanto ao terceiro possível estado a ser atribuído a um nó MC, o estado RED_STATE, por agora limita-se a defini-lo como o estado atribuído a um nó MC classificado como malicioso. Esse estado é exemplificado na última etapa da fase objetiva.

3.4. Fase Objetiva

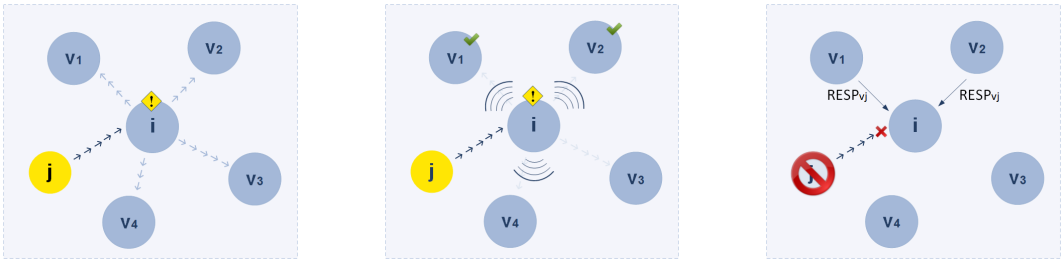
A fase subjetiva, ao detectar que um nó MC foi classificado como YELLOW_STATE, invoca a fase objetiva. Nessa fase, um conjunto de evidências é coletado contando não apenas com a opinião individual dos nós MRs a respeito do cliente em análise, mas também com a opinião de seus nós MRs vizinhos sobre esse cliente. Dessa forma, a agregação de informações internas e externas sobre o nó MC em questão contribui para a tomada de uma decisão final mais justa, uma vez que essa decisão pode invocar o mecanismo de segurança para conter um nó MC considerado malicioso.

A fase objetiva é caracterizada pelas etapas de coleta de opiniões, de agregação de opiniões seguida da sua avaliação e, por fim, pela etapa de decisão. A esta última, cabe o veredicto final se um mecanismo de segurança deve ou não ser invocado.

3.4.1. Coleta de Opiniões

A Figura 1 ilustra o processo pelo qual um nó MC é submetido ao ser definido pela fase subjetiva com o estado YELLOW_STATE. No exemplo, considera-se que o nó MC em questão será classificado como malicioso pela fase objetiva. Os processos representados na Figura 1 são: início da fase objetiva (Figura 1(a)), requisição de opiniões (Figura 1(b)) e respostas da requisição e mecanismo de defesa da rede (Figura 1(c)).

Na Figura 1(a), os nós MR e MC são definidos, respectivamente, como i e j, onde o nó MC j mantém-se conectado à rede através de nó MR i. As setas escuras representam



(a) (b) (c)

Figura 1. MIRF - fase objetiva

as requisições ARP sendo enviadas, em primeira instância, ao nó MR i, enquanto que as setas claras representam essas mesmas requisições sendo retransmitidas à rede por intermédio desse roteador. A atribuição do estado YELLOW_STATE indica que o grau de confiança do nó MC j, com relação ao seu tráfego de requisições ARP, está abaixo do esperado. Com isso, tem-se início a fase objetiva com a coleta de opiniões.

Na fase de coleta de opiniões, Figuras 1(b) e em 1(c), o nó MR i tem como função o envio de requisições de opiniões aos seus nós MRs vizinhos a respeito do nó MC j. Tais requisições são transmitidas em *broadcast* e se destinam a quaisquer nós MRs próximos que possuam informações sobre o nó MC em questão na requisição. Os vizinhos são definidos como v_1, v_2, v_3 e v_4. Após o envio da requisição, o nó MR i irá aguardar $\mathrm{L_{MAX}}$ instantes, tempo este destinado à coleta de respostas referentes à requisição enviada. Durante o período de espera de opiniões $\mathrm{L_{MAX}}$, o nó MC j ainda possui completo acesso a todos os recursos da rede, conforme representado na Figura 1(b).

Os nós MRs vizinhos, ao receberem tal requisição, verificam se possuem informações referentes ao cliente solicitado por MR j. Essa tarefa é realizada consultando a estrutura onde são armazenadas as opiniões recentes que os nós MRs mantém sobre os nós MCs. São duas as informações mantidas a respeito do nó MC: o grau de confiança no momento da desassociação e o instante em que a informação é armazenada. Tais informações são armazenadas nessa estrutura no ato da desassociação de um nó MC com seu respectivo nó MR.

As respostas à requisição são representadas na Figura 1(c). Os vizinhos que receberem a requisição e possuírem informações a respeito do cliente, no caso os nós MRs v_1 e v_2, enviam suas respostas a fim de compartilhar tais informações. Tais respostas são representadas como $RESP_{vj}$, onde v representa o nó MR vizinho e j o nó MC referente à informação que o vizinho está enviando. Se estas chegarem ao nó MR i dentro do período $\mathrm{L_{MAX}}$, estas opiniões irão contribuir com o espaço de evidências do nó MR i referente ao nó MC j. O fim desse período determina a fase da agregação de todas as informações que o nó MR possui a respeito do cliente analisado até então.

3.4.2. Agregação de Opiniões e Avaliação da Reputação

Ao atingir esse estágio no MIRF, o campo de evidências é composto por opiniões de nós MRs vizinhos recebidas sobre o nó MC j em análise, bem como pela opinião que o próprio MR i possui. No MIRF, ao assumir que os nós MRs são cooperativos entre si,

todas as opiniões recebidas, desde que procedam de um nó MR autenticado e autorizado na rede, serão consideradas válidas. Para a agregação das informações internas e externas coletadas e para a definição do grau de confiança final de um cliente, considera-se:

$$\alpha_{\mathrm{ij}\,FINAL} = \frac{\alpha_{\mathrm{ij}} + \sum_{v}^{T_{op}} \mathrm{k_{vj}}}{1 + T_{op}} \tag{2}$$

onde T_{op} representa a quantidade de opiniões recebidas e $\mathrm{k_{vj}}$ representa a opinião do nó MR vizinho v a respeito do nó MC j. Esse valor é considerado na fase seguinte para a tomada de decisão.

A abordagem para a agregação adotada é uma abordagem determinística: o grau de confiança final tem como base a média das opiniões coletadas, além da sua própria opinião [Selvaraj and Anand 2012]. Além disso, essa abordagem define o caráter individual do MIRF; uma vez que a opinião final é calculada, esta será considerada apenas internamente, ou seja, pelo nó MR que realizou a análise do nó MC. Portanto, o grau de confiança final atribuído ao cliente em questão não representa um grau de confiança global, assim como não será compartilhado com todos os nós MRs da rede, exceto nos casos em que seja requisitado, pela etapa de coleta de opiniões da fase objetiva do MIRF.

3.4.3. Decisão

Nesta fase ocorre, finalmente, a tomada de decisão com base em $\alpha_{\mathrm{ij}\,FINAL}$, valor este previamente calculado pela etapa anterior. Aqui, a decisão tomada define se o nó é classificado como malicioso ou não. Se $\alpha_{\mathrm{ij}\,FINAL} > \mathrm{K_{MIN}}$, ou seja, se o grau de confiança final está acima do limite mínimo, nenhuma ação é realizada pelo nó MR e o nó MC permanece com acesso total à rede. Caso contrário, se definido como malicioso, o nó MC recebe a classificação RED_STATE. A atribuição desse estado, por sua vez, precede a invocação do mecanismo de segurança, o esquema de *filtering*.

Na adoção do esquema de *filtering*, este se aplica a todos os tipos de tráfego da rede e não somente ao tráfego referente às requisições ARP. Portanto, um nó MC classificado como RED_STATE, ou seja, um nó malicioso, não possui acesso a nenhum recurso da rede o qual dependa do repasse de mensagens, através do nó MR com o qual está conectado, para a rede. O único recurso disponível a esse nó MC são as atividades que dizem respeito à sua mobilidade, que, por sua vez, não necessitam que quaisquer mensagens sejam repassadas para a rede.

O tempo de bloqueio definido pelo esquema de *filtering* é definido como $\beta_{\mathrm{ij}} * \mathrm{N_{DEF}}$. Ou seja, nos próximos $\beta_{\mathrm{ij}} * \mathrm{N_{DEF}}$ instantes que se seguem, o nó MR, o qual classificou o nó MC como malicioso, irá impedir qualquer repasse de mensagens à rede provenientes do nó MC bloqueado. No entanto, esse bloqueio não é definitivo. O nó MC, após $\beta_{\mathrm{ij}} * \mathrm{N_{DEF}}$ instantes contando a partir do instante em que a punição lhe foi aplicada, recebe uma nova oportunidade e é reincorporado à rede.

O total de vezes que o nó MC j é bloqueado pelo nó MR i, β_{ij}, tem por objetivo conferir maior severidade no tempo de bloqueio do cliente na rede. A quantidade de vezes que o nó MC é classificado como malicioso influencia diretamente no aumento do tempo

de exclusão do mesmo na rede. Mesmo que um nó MC possa ser reincorporado à rede, tal ação depende do seu bom histórico registrado pelo nó MR.

4. Avaliação

Para avaliar o desempenho do MIRF, foi utilizado o simulador NS-2 na versão 2.34 [NS2]. O esquema foi implementado no protocolo PGMID (Protocolo de Gerenciamento de Mobilidade Intra-Domínio) [Boukerche and Zhang 2008]. Como protocolo de roteamento, adotou-se o HWMP [Bahr 2006] em modo reativo, e o protocolo IEEE 802.11 [the Standards for Wireless LAN] na camada de enlace.

A topologia dos roteadores mesh na rede seguem uma disposição em grade. A rede em malha consiste em vinte roteadores *mesh* cujos raios de alcance equivalem à 250m. Tais roteadores representam o *backbone* da rede, os quais são dotados de mobilidade mínima, e estão distribuídos uniformemente de acordo com a topologia *grid* ao longo de uma área de 1300 x 1100m. O modelo de mobilidade *Random Waypoint* foi o adotado para promover a movimentação dos clientes *mesh*, os quais se movimentam com velocidade de até 5m/s. O tráfego na rede é definido com o auxílio do gerador de tráfego *cbrgen*, e consiste em fluxos de pacotes CBR de 521 *bytes* enviados a cada 20ms, sendo o número máximo de conexões correspondente ao número de clientes na simulação. Para todas as simulações foram garantidas pelo menos uma comunicação entre um cliente atacante e um não-atacante, e para cada comunicação dessas, uma comunicação entre clientes não-atacantes é estabelecida. Para as simulações com ataque, a quantidade de atacantes definida corresponde a 10% do total de clientes da simulação, e suas ações maliciosas são desencadeadas a cada 10ms. Grupos de 4, 6 e 12 clientes foram considerados na avaliação. Foram realizadas simulações de 400s, totalizando 33 simulações para cada grupo.

Para a implementação do protocolo PGMID é definido que as mensagens de sondagem são enviadas a cada 2s e que o número máximo de saltos das mensagens ARP é equivalente a 7. Para o atraso máximo de resposta, são realizadas simulações adotando diferentes valores para esse atraso. Dessa forma, procura-se verificar se é possível potencializar o desempenho do PGMID apenas com a alteração desse valor, sobretudo nas simulações envolvendo 12 clientes, simulações essas em que foram verificados os piores índices de desempenho do PGMID, mesmo nos ambientes livres de ataques. Para um ciclo ARP, representado por $\mathrm{M_{MIN}}$, sua duração mínima é definida em 0,5s e o valor máximo definido para a frequência de requisições ARP, representada por Υ_{MAX}, é estipulada em 5 requisições ARP por ciclo. Com relação ao grau de confiança mínimo para que um nó MC seja considerado confiável na rede, este valor é estipulado em 0,5, sendo representado por $\mathrm{K_{MIN}}$. O grau de confiança 0,5 também é o valor atribuído aos nós MCs que adentram a rede. Tal valor inicial é justificado por garantir igual oportunidade para todos os nós MC na rede. No que diz respeito à ativação do mecanismo de requisição de opiniões da etapa de coleta de opiniões, o tempo máximo para o recebimento de opiniões de outros nós MRs é de 20ms, sendo representado por $\mathrm{L_{MAX}}$. Para a atualização do grau de confiança de um nó MC, o peso das mensagens ARP na rede corresponde a 0,01, sendo este valor representado por Γ_{ARP}. Por fim, nos casos em que o nó MC é classificado como malicioso, o tempo de punição inicial corresponde a 10s, este sendo representado por $\mathrm{N_{DEF}}$.

Dois cenários distintos foram considerados nas simulações para 4, 6 e 12 clientes: os cenários com **ataques contra ARP** e os cenários **sem ataques**. Para cada um desses

cenários, as simulações foram realizadas considerando o protocolo PGMID em sua forma original e também considerando o protocolo PGMID adotando o esquema MIRF como solução para lidar com os **ataques contra ARP** na rede. Para os ataques contra ARP, o nó malicioso tem como estratégia a constante restauração de sua tabela ARP ao seu estado inicial. Dessa forma, as requisições ARP serão geradas frequentemente com o intuito de sobrecarregar a rede. As seguintes métricas foram adotadas para comparar entre o desempenho do PGMID em sua forma original e seu desempenho com o esquema MIRF:

Taxa de entrega dos pacotes UDP (TE): Percentual de pacotes UDP proveniente do nó MC origem que são recebidos com sucesso pelo nó MC destino;

Latência de entrega dos pacotes UDP (LE): Tempo total desde que um pacote UDP é enviado de um nó MC origem até que o mesmo seja recebido pelo nó MC destino.

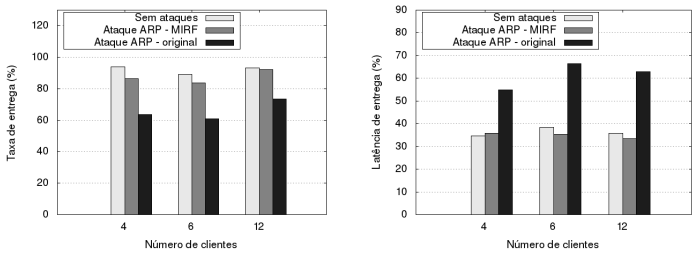
Total de *handoffs* (TH): Total de vezes em que os nós MCs trocaram seu ponto de acesso à rede, ou seja, se associaram a outro nó MR.

Latência de *handoffs* (LH): Intervalo de tempo entre o momento de decisão da troca do ponto de acesso à rede por parte de um nó MC até o momento em que é estabelecida uma nova conexão com um nó MR considerado mais adequado.

A forma como a solução MIRF se comporta diante de constantes ataques é avaliada considerando as seguintes métricas: a latência da fase objetiva - cujo marco inicial é a chamada do método de requisição de opiniões e marco final é o instante em que a decisão final é tomada - e o total de vezes em que esta é requisitada na rede. Ambas essas métricas buscam quantificar a escalabilidade do MIRF, ou seja, sua habilidade de lidar com uma gama crescente de trabalho, este consequência dos ataques contra ARP na rede.

4.1. Resultados e Análises

Os gráficos nas Figuras 2(a) e 2(b) ilustram a taxa de entrega (TE) e a latência de entrega (LE) dos pacotes UDP. Tais figuras apresentam a comparação entre os três diferentes tipos de simulação realizadas: as simulações sem ataques, as com ataque contra ARP sem a adoção de mecanismos de segurança e as com ataque contra ARP adotando o MIRF.



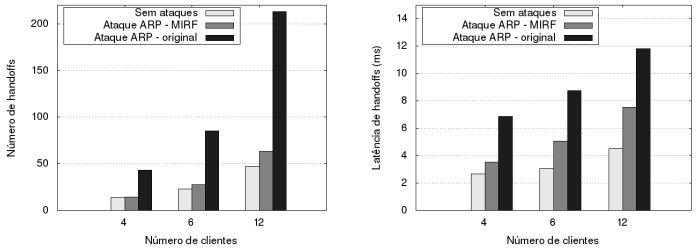
(a) (b)

Figura 2. Taxa de entrega (TE) e latência de entrega (LE) de pacotes UDP

Na Figura 2(a), a TE em cenários com ataques contra ARP adotando o PGMID original decai em 32%, em 31,50% e em 21,47% para 4, 6, e 12 clientes, respectivamente. Porém, ao incorporar o MIRF ao PGMID, as quedas na TE são de apenas 8,05%, de 6,17% e de 1,38%. A adoção do MIRF representou um aumento de 27,08% na TE nas simulações envolvendo 6 clientes. Para as simulações envolvendo 12 clientes, a TE obtida em ambientes sem ataques e em ambiente com ataques contra ARP apresenta uma diferença de apenas 1,28%. Dessa forma, as TEs obtidas em ambientes com ataque adotando o MIRF se equiparam às TEs obtidas em ambientes sem ataques. A melhora da TE

também reflete numa menor LE desses pacotes. Como pode ser observado na Figura 2(b), com a adoção do MIRF essa latência é reduzida em 34,76%, em 46,83% e em 47,02% para 4, 6 e 12 clientes, respectivamente. As latências obtidas também se equiparam às obtidas nas simulações em ambientes sem ataques. Dessa forma, com relação às métricas referentes ao tráfego de dados, o MIRF se mostrou eficiente.

As Figuras 3(a) e 3(b) apresentam o total de *handoffs* (TH) e a latência dos *handoffs* (LH) realizados. Assim como ocorre com relação ao tráfego UDP, o total de *handoffs* e sua latência também apresentam melhorias nas simulações onde o MIRF é incorporado ao PGMID. A TH tem a maior diferença entre os valores obtidos para as simulações com ataque sem o MIRF e as com o MIRF. A diminuição do TH chega a ser de 70,42% considerando um ambiente com 12 clientes. É importante notar que a diminuição do número de *handoffs* não implica em enlaces de pior qualidade mantidos entre os clientes e os roteadores. Isso pode ser observado pela melhora obtida para todas as outras métricas. Por fim, assim como ocorre com relação à TE e à LH, os resultados obtidos são muito similares para as simulações sem ataques e as com ataque adotando o MIRF, provando mais uma vez sua eficiência. A LH também acompanha a diminuição do TH. Para 4, 6 e 12 clientes a diminuição dessa latência é de 48,62%, de 42% e de 36,36%, respectivamente. Originalmente, em um ambiente sem a adoção do MIRF a latência de um *handoff* podia atingir cerca de 11ms ao passo de que com o MIRF esta atinge no máximo 7,52ms.

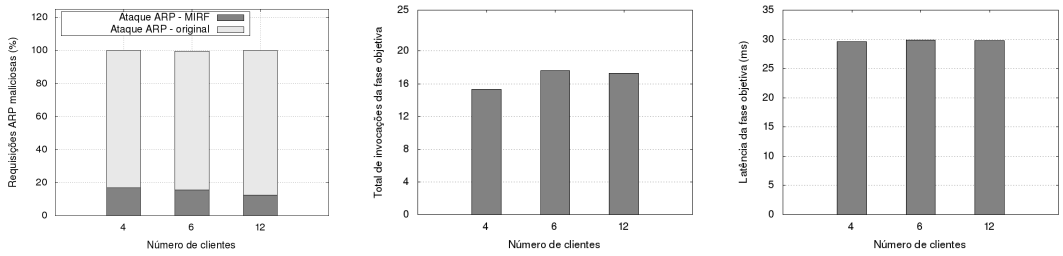


(a) (b)

Figura 3. Total e latência de *handoffs*

A Figura 4(a) representa o percentual de mensagens ARP maliciosas presentes na rede num ambiente com o ataque contra ARP adotando o MIRF e sem a adoção de mecanismos de segurança. Com a incorporação do MIRF ao PGMID, observou-se que o máximo de requisições maliciosas que permaneceram na rede foram para as simulações envolvendo 4 clientes, onde 16,08% dessas mensagens se mantiveram. O melhor resultado foi obtido para as simulações envolvendo 12 clientes, onde 87,70% do total de mensagens ARP maliciosas foram contidas com o MIRF. Já para com 6 clientes, essa contenção foi de 84,20%. Com relação ao comportamento do MIRF no PGMID, duas métricas são consideradas para sua avaliação: o total de vezes em que a fase objetiva é invocada e sua respectiva latência. Tais métricas são representadas nas Figuras 4(b) e 4(c).

A quantidade de vezes em que a fase objetiva do MIRF é invocada é semelhante para todas as simulações realizadas. Este valor é de aproximadamente 17 ao longo das simulações. Com relação à latência da fase objetiva, nela estão incluídos o tempo necessário para o processamento do cálculo referente ao grau de confiança e também o tempo reservado para a fase de requisição de opiniões, o qual é fixado em 20ms. A média obtida para as simulações envolvendo 4, 6 e 12 clientes é de aproximadamente 30ms para cada. Dessa forma, como 20ms são reservados para o método de requisição de opiniões,

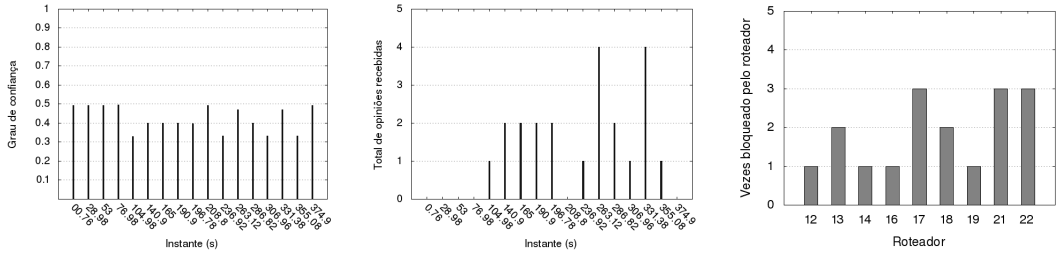


(a) (b) (c)

Figura 4. Latência e total de invocações da fase objetiva do MIRF

todas as outras atividades inclusas na fase objetiva ocupam 10ms dessa latência. Assim, a latência dessa fase é considerada aceitável.

Para ilustrar o comportamento de um nó malicioso diante da solução de segurança MIRF são apresentados os dados obtidos referentes à uma simulação envolvendo 4 clientes. Para tal, são considerados o grau de confiança ao longo da simulação, o total de opiniões recebidas no método de requisição de opiniões e, por fim, o total vezes em que o nó malicioso foi bloqueado, assim como qual roteador o bloqueou. Essas métricas são apresentadas nas Figuras 5(a), 5(b) e em 5(c).



(a) (b) (c)

Figura 5. Comportamento de um nó malicioso na rede

O grau de confiança ao longo da simulação, como pode ser observado em 5(a), diz respeito ao grau de confiança atribuído ao nó malicioso em questão logo após a fase objetiva ser finalizada. Para todas as invocações da fase objetiva o nó em análise foi definido com um grau de confiança inferior a 0,5, ou seja, um grau de confiança o qual classifica-o como um cliente malicioso. Com relação às opiniões recebidas pelo método de requisição de opiniões da fase objetiva, até os 104s o grau de confiança é calculado apenas com base na opinião do roteador o qual está realizando a análise, uma vez que nenhuma opinião foi recebida, como pode ser observado na Figura 5(b). A partir desse instante, em 81,81% das vezes em que esse método foi requisitado ao menos uma opinião externa foi considerada para o cálculo do grau de confiança final na fase objetiva. Isso comprova que o tempo destinado à coleta de opiniões da fase objetiva, valor este fixado em 20ms, é suficiente para que diferentes opiniões sejam coletadas na maioria dos casos.

A Figura 5(c) apresenta todos os roteadores pelo qual o cliente malicioso se associou e que também o definiu como malicioso, lhe atribuindo o estado RED_STATE. O cliente em questão, por sua vez, se associou a nove roteadores distintos ao longo da simulação. A vantagem de um nó ser muito móvel na rede, como é o caso, é que este se associa a diferentes roteadores, possibilitando que os mesmos mantenham o grau de confiança que atribuíram ao cliente armazenado em seu histórico de opiniões recentes

para quando este realizar *handoff*. Isso torna esses roteadores capazes de responder às requisições de opiniões da fase objetiva quando solicitado por seus vizinhos, contribuindo assim ao espaço de confiança utilizado no cálculo do grau de confiança final do cliente.

5. Conclusão

O gerenciamento da mobilidade é uma das questões mais relevantes nas redes em malha sem fio, sendo que um de seus maiores atrativos é a livre movimentação com a garantia de acesso à rede. Porém, ações maliciosas por parte dos nós podem influenciar negativamente na mobilidade da rede. A fim de conter o impacto que ações maliciosas podem causar a uma rede em malha, este artigo apresentou o esquema MIRF, cujo objetivo é mitigar ataques de inundação na mobilidade em redes em malha sem fio. O esquema foi avaliado por simulações e os resultados demonstram melhorias com o seu uso.

Referências

The Network Simulator NS-2. http://www.isi.edu/nsnam/ns/. [Online; Julho 2013].

Akyildiz, I., Wang, X., and Wang, W. (2005). Wireless mesh networks: a survey. *Computer Networks*, 47:445–487.

Bahr, M. (2006). Proposed Routing for IEEE 802.11s WLAN Mesh Networks. In *Proceedings of the ACM Annual International Wireless Internet Conference*, pages 6–1. ACM.

Barabasz, L. and Nogueira, M. (2011). Uma Avaliação de SeguranÃ§a no Gerenciamento de Mobilidade nas Redes em Malha sem Fio. *Anais do XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 329–338.

Boukerche, A. and Zhang, Z. (2008). A hybrid-routing based intra-domain mobility management scheme for wireless mesh networks. In *Proceedings of the 11th international symposium on Modeling analysis and simulation of wireless and mobile systems*, MSWiM '08, pages 268–275. ACM.

Egners, A. and Meyer, U. (2010). Wireless mesh network security: State of affairs. *IEEE 35th Conference on Local Computer Networks (LCN)*, pages 997–1004.

Martignon, F., Paris, S., and Capone, A. (2008). Mobisec: a novel security architecture for wireless mesh networks. *Proceedings of the 4th ACM symposium on QoS and security for wireless and mobile networks*, pages 35–42.

Mehdi, S., Ghazi, A., Badii, J., Djamal, Z., and Hossam, A. (2007). Mobile party: A mobility management solution for wireless mesh network. *IEEE International Conference on Wireless and Mobile Computing, Networking and Communication*, page 45.

Selvaraj, C. and Anand, S. (2012). A survey on Security Issues of Reputation Management Systems for Peer-to-Peer Networks. *Computer Science Review*, 6(4):145–160.

Sen, J. (2012). Secure and Privacy-Preserving Authentication Protocols for Wireless Mesh Networks. *Clinical Orthopaedics and Related Research (CORR)*.

the Standards for Wireless LAN, T. W. G. S. IEEE 802.11. http://www.ieee802.org/11/. [Online; Março 2013].

Xie, J. and Wang, X. (2008). A survey of mobility management in hybrid wireless mesh networks. *IEEE Network*, 22:34–40.

