Um Mecanismo de Exclusão Acurado baseado em Confiança para Controle de Acesso em Redes Ad Hoc *

Lyno Henrique G. Ferraz[1], Natalia C. Fernandes[1], Pedro B. Velloso[2] e Otto Carlos M. B. Duarte[1]

[1] Grupo de Teleinformática e Automação
PEE/COPPE - DEL/POLI
Universidade Federal do Rio de Janeiro

[2]Instituto de Computação
Universidade Federal Fluminense

{lyno, natalia, otto}@gta.ufrj.br, velloso@ic.uff.br

Abstract. *Mobile ad hoc networks are based on the cooperation between nodes. These networks are prone to frequent network partitions due to the fading channels, mobile nodes, and frequent membership changes. Hence, to ensure security and fairness, ad hoc networks depend on distributed and robust access control mechanism. In this paper, we propose a distributed access control mechanism based on a trust model to exclude non-cooperative nodes. Thereby, all nodes participate in the network control and play multiple roles, monitoring the nodes, voting to punish non-cooperative nodes. Our mechanism accurately identifies non-cooperative nodes in different density scenarios and even in partition likely scenarios. The combination of voting and trust mechanisms guarantees good classification in spite of low and imprecise neighbor action detection. Simulation results show that mechanism excludes nodes up to 99.5% of efficiency and 1.4% of false positives.*

Resumo. *Redes ad hoc móveis são baseadas na cooperação de nós para seu funcionamento. Esse tipo de rede é sujeita a partições de rede frequentes devido ao canal não confiável, nós móveis e entrada e saída de nós na rede. Desse modo, para garantir segurança e justiça, redes ad hoc dependem de um mecanismo controle de acesso robusto e distribuído. Este artigo propõe um mecanismo de controle de acesso baseado em um modelo de confiança para excluir nós não cooperativos da rede. Assim, todos nós participam do controle da rede assumem papéis diferentes, ao monitorar os nós da vizinhança e votar para punir os nós não cooperativos. O mecanismo proposto identifica de maneira acurada os nós não cooperativos em cenários com diferentes densidades e até em cenários sujeitos a partições. A combinação de um modelo de confiança com um mecanismo de votação garante boa classificação apesar da detecção falha e imprecisa de ações. Resultados de simulações mostram que o mecanismo exclui nó com eficiência de até 99,5% com 1,4% de falsos positivos.*

*Este trabalho foi apoiado por recursos da FINEP, CAPES, CNPq, FAPERJ, FUJB e FUNTTEL.

1. Introdução

As redes ad hoc não possuem infraestrutura física ou qualquer controle centralizado. Nesse tipo de rede, os próprios nós que assumem os papéis de roteador, servidor e também cliente. Ademais, quanto mais nós participarem da rede, maior o número de rotas possíveis entre os nós, maior a banda disponível e menor a possibilidade de ocorrer partições na rede. Desta forma, para se conseguir esses atributos, os nós devem cooperar em prol da rede. No entanto, os nós podem falhar em cooperar por estarem sobrecarregados, com defeito, ou podem comportar-se mal e assumir um comportamento egoísta para economizar os próprios recursos, ou malicioso para atrapalhar a rede. Portanto, um sistema seguro que garanta a cooperação entre nós é indispensável para a operação correta da rede.

A segurança das redes ad hoc é normalmente realizada através do uso de um sistema de controle de acesso com autenticação. Assim, somente os nós autorizados podem participar e usufruir da rede. Entretanto, a utilização de um sistema de controle de acesso não garante que os nós na rede cooperem sempre. Mesmo se somente um grupo seleto de nós for autorizado a participar da rede, isso não os impede de depois mudarem seus comportamentos e atrapalhar a rede seja intencionalmente ou devido limitações de recursos. Assim, o sistema de controle de acesso deve ser capaz de identificar os nós não cooperativos e limitá-los o acesso aos recursos da rede.

Neste sentido, esse artigo propõe a construção de um mecanismo que identifique os nós não cooperativos e os puna para não perturbar o funcionamento da rede. O mecanismo realiza o controle de acesso distribuído, e ao identificar um nó não cooperativo, o expulsa da rede. O mecanismo proposto é baseado em tribunal de júri, no qual cada nó assume múltiplos papéis: tanto de testemunha e jurado, quanto de réu. A testemunha monitora seus vizinhos e avalia o nível de confiança neles. O jurado julga certos nós, se devem ser ou não punidos e em caso positivo, vota pela exclusão deles da rede. Finalmente, cada nó assume papel de réu, assim ele é sujeito ao tribunal do júri.

Ao se utilizar o modelo de tribunal de júri, o controle de acesso é realizado através da combinação das testemunhas e do júri. As testemunhas utilizam um modelo de confiança acurado e escalável baseado em interações locais para identificar a natureza dos seus vizinhos. Assim, as testemunhas avaliam o nível de confiança de cada um dos vizinhos e quando acharem que um não é confiável para permanecer na rede, informam ao júri acerca da confiabilidade do nó, que se torna réu. Quando o júri é informado sobre o mau comportamento do réu, ele realiza uma votação entre os jurados para decidir se o réu será excluído da rede. O júri é composto por um grupo dinâmico de nós escolhidos aleatoriamente na rede, que é reconfigurado quando ocorrem entradas e saídas de nós na rede. Além disso, a utilização de um júri distribuído na rede com um modelo de confiança escalável cria um senso global de confiabilidade com baixa sobrecarga de mensagens. Para analisar a proposta foram realizadas simulações que comparam a proposta com trabalhos relacionados. Os resultados mostram que o mecanismo atinge 99,5% de eficiência com 1,4% de falsos positivos, assim é altamente acurado.

O restante do artigo está organizado como se segue. A Seção 2 descreve os principais trabalhos relacionados sobre confiança e controle de acesso em redes ad hoc. Na Seção 3 é apresentada o modelo do sistema e o contexto do artigo. A Seção 4 apresenta a proposta. Na Seção 5 as simulações realizadas e resultados obtidos são descritos, e

finalmente a Seção 6 conclui o artigo.

2. Trabalhos Relacionados

As redes ad hoc, devido à falta de infraestrutura, só funcionam corretamente com a cooperação dos nós participantes. Então, é necessário um sistema seguro que controle a rede e permita a presença de somente nós cooperativos. Na literatura, existem diversos sistemas seguros em redes ad hoc que baseiam suas propostas em controle de acesso com autenticação. Esses sistemas utilizam-se de recursos para prover segurança à rede, como o uso de identidades com a emissão de certificados para identificar os nós, e também o uso de modelos de confiança ou mecanismos de identificação e punição de nós não cooperativos [Zhou e Haas, 1999, Fernandes et al., 2010, Adnane et al., 2008, Buchegger e Le Boudec, 2002, Yang et al., 2006].

Tradicionalmente, as entidades certificadoras (*Certification Authorities* - CA) são utilizadas para garantir a validade das identidade. Entretanto, o uso de CAs em redes ad hoc não é recomendado, pois requer infraestrutura especializada e uma entidade central de controle. Zhou e Haas [Zhou e Haas, 1999] propõem a distribuição da entidade certificadora para redes ad hoc com o uso de criptografia de limiar. A ideia é dividir a responsabilidade da CA em um grupo de nós especializados com um esquema de criptografia de limiar (k,m). Contudo, este esquema ainda necessita de m nós especializados, dos quais ao menos k devem estar disponíveis. Outros sistemas [Luo et al., 2005, Luo et al., 2004] também utilizam criptografia de limiar, mas todos necessitam de administradores para gerenciar participantes ou nomes, e para configurar um grupo de nós especiais.

Como a autenticação deve ser feita sem qualquer tipo de controle centralizado, entidades certificadoras distribuídas não são suficientes para garantir a segurança em redes ad hoc. Fernandes *et al.* [Fernandes et al., 2010] propõe ACACIA (*A Controller-node-based Access-Control mechanIsm for Ad hoc networks*), um sistema distribuído de controle de acesso e autenticação sem a necessidade de uma CA. O sistema é auto-organizado e gerencia as chaves público-privadas e as identidades, além de controlar a entrada de nós na rede e punir os nós não colaborativos. ACACIA evita o uso de um administrador central para controlar o acesso dos nós com o uso de cadeias de delegação que controlam a entrada de nós na rede. Além disso, o sistema autogerencia o grupo de controle na inicialização e partição da rede. Ademais, o sistema provê segurança a rede contra ataques em conluio e de *Sybil* por meio de escolha aleatória do grupo de controle (controladores) e exclusão de nós maliciosos. Entretanto, esse sistema apresenta um algoritmo de classificação de comportamento de nós sujeito à falhas de detecção e classificação de comportamento, cuja acurácia de exclusão de nós maliciosos depende do número de vizinhos.

A classificação acurada do comportamento de nós pode ser obtida através do uso de sistemas e modelos de confiança e reputação [Sun et al., 2008]. Existem diversos sistemas e modelos de confiança e reputação para redes ad hoc, que em sua maioria lidam com duas funcionalidades de rede: roteamento e encaminhamento de pacotes [Yu e Liu, 2005, Adnane et al., 2008, Buttyan e pierre Hubaux, 2003, Al-Karaki e Kamal, 2008, Zakhary e Radenkovic, 2010]. Velloso *et al.* [Velloso et al., 2010] apresentam um modelo de confiança para redes ad hoc baseado em interações humanas. Nesse modelo, cada nó constrói uma relação de

confiança com seus vizinhos. Uma das maiores vantagens desse modelo é permanência local das interações entre os nós, e assim evita a sobrecarga de mensagens na rede toda e mantém o consumo de recursos em um nível baixo. Além disso, outra vantagem desse modelo é o uso de recomendações de outros nós para o cálculo do nível de confiança.

Todos esses modelos e sistemas de confiança acima citados provêem boa classificação do comportamento dos nós, mas dependem da existência de sistemas seguros de controle de acesso e autenticação para a correta classificação dos nós. Sem o sistema de controle de acesso e autenticação, nós maliciosos poderiam falsificar identidades e atrapalhar o cálculo da confiança e reputação, e também poderiam utilizar as identidades falsas para entrar novamente na rede sempre que seus valores de confiança e reputação estiverem baixos.

Diversas propostas baseiam-se na identificação e punição de nós maliciosos e egoístas para estimular a cooperação entre os nós [Song e Zhang, 2010, Mahmoud e Shen, 2010]. Em [Marti et al., 2000], os nós utilizam os mecanismos de *watchdog* e *pathrater* para identificar os nós mal comportados e escolher caminhos que os evitem. Entretanto, essa proposta não pune os nós, que podem continuar usando a rede e possivelmente prejudicá-la. No protocolo CONFIDANT (*Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks*) [Buchegger e Le Boudec, 2002], os nós monitoram a vizinhança e os atribuem um valor de reputação. Todas as vezes que um nó detectar um vizinho que deixa de encaminhar pacotes ou falha em cooperar, ele atualiza o valor de reputação do vizinho. Quando o valor de reputação do vizinho fica menor que um limiar, o nó informa aos outros para evitar o vizinho no roteamento. A principal desvantagem desse protocolo é ser suscetível a mensagens falsas e pode punir nós cooperativos. SCAN [Yang et al., 2006] estende protocolos de roteamento para garantir o encaminhamento seguro de pacotes. No SCAN, os nós devem possuir uma ficha para participar da rede. As fichas são entregues por nós vizinhos legítimos, que já participam da rede. Todos nós monitoram independentemente seus vizinhos e quando detectam que um nó se comporta mal, trocam mensagens sobre o mal comportamento do nó. Se os vizinhos concordarem em condenar o nó mal comportado, eles revogam sua ficha e o impedem de participar da rede.

Esse artigo propõe a construção de um mecanismo de exclusão de nós para restringir o acesso de nós que não se comportam adequadamente. O mecanismo utiliza um sistema auto-organizado e autogerenciado de autenticação e controle de acesso baseado no sistema ACACIA, que identifica os usuários e gerencia as identidades. Além disso, o mecanismo utiliza um modelo de confiança baseado no proposto por Velloso *et al.* para avaliar a confiança dos nós. Assim, obtém-se um sistema seguro de controle de acesso que pune nós com acurácia.

3. Modelo do Sistema

A criação de uma rede ad hoc é motivada por um grupo com interesse ou relações comuns, como trabalhadores de uma mesma empresa, militares, amigos, etc. Eles utilizam suas relações sociais para criar uma cadeia de delegação como o do sistema ACACIA [Fernandes et al., 2010]. A cadeia de delegação realiza controle de acesso não centralizado baseado nas relações entre os usuários. Assim, qualquer um pode criar uma nova rede e se tornar o nó raiz da cadeia de delegação, ou pode se associar a uma rede já

existente ao obter um convite de outro usuário. Desta forma, cada usuário tem um número determinado de convites que ele pode distribuir para novos membros, que se tornam seus filhos na cadeia de delegação. O usuário envia um convite *offline* para o novo membro e transfere alguns de seus próprios convites (ou nenhum) para o novo membro de acordo com a confiança que tem nele. Esse procedimento limita o número de novos membros que um usuário e seus convidados podem chamar para rede, portanto reduz a possibilidade de um usuário não confiável convidar novos membros. Após obter o convite *offline*, o novo membro obtém uma lista com os endereços IPs (*Internet protocol*) alocados e escolhe um endereço IP livre, além de um par de chaves público-privada, e finalmente uni-se à rede. Os nós membros da rede enviam mensagens que informam sua presença periodicamente. Cada mensagem contêm os dados de um nó, seu endereço IP, chave pública e identificador (*hash* da chave pública). Assim, os nós sabem se outro faz parte da rede e podem verificar assinaturas de mensagens.

Cada nó executa um sistema detector de mau comportamento (BBDS - *Bad Behavior Detection System*) que monitora as ações dos vizinhos como encaminhamento de mensagens e envio em *broadcast*. Esquemas como [Marti et al., 2000] e [Dehnie e Tomasin, 2010] podem ser usados com esse propósito. Baseado nas ações avaliadas pelo BBDS e também as opiniões dos vizinhos comuns, o nó constrói um nível de confiança para cada vizinho. A utilização de recomendações de vizinhos é importante, pois a detecção das ações do BBDS pode ter falhas.

Para construir um senso global na classificação do comportamento de um nó, utiliza-se uma estrutura chamada de júri, similar à proposta por [Fernandes et al., 2010]. Essa estrutura consiste de um grupo de nós que é responsável pelo controle de um réu. Todas as decisões acerca do réu são realizadas por meio de votações do júri daquele réu. Então, se o júri concorda que o nó não é cooperativo e não pode mais participar da rede, ele divulga na rede que o nó e seus descendentes da cadeia de delegação foram excluídos e não podem mais participar da rede. Mais informações sobre como criar e manter tais grupos distribuídos podem ser encontradas em [Fernandes et al., 2010].

Modelo de Confiança

O mecanismo de exclusão proposto usa o modelo de confiança de Velloso *et al.*, que permite os nós avaliarem o nível de confiança de seus vizinhos, que representa uma previsão do comportamento futuro dos nós a partir do comportamento inferido pelo sistema detector de mau comportamento (BBDS) [Velloso et al., 2010]. Além disso, os nós trocam recomendações para compensar problemas de monitoramento devido à incapacidade ou restrição de recursos. Recomendações são opiniões dos nós sobre um vizinho comum, portanto não são encaminhadas. Nesse modelo, o nível de confiança é um valor contínuo de 0 a 1. O valor 1 representa o maior nível de confiança, e 0 o menor. A confiança, $T_{\mathbf{w}}(\mathbf{d})$, de uma testemunha, $\mathbf{w}$, em um réu, $\mathbf{d}$, é dada pela soma ponderada de sua própria avaliação do comportamento, $Q_{\mathbf{w}}(\mathbf{d})$, e as recomendações, $R_{\mathbf{w}}(\mathbf{d})$, dos vizinhos tanto de $\mathbf{w}$ e também de $\mathbf{d}$, como descrito pela equação

$$T_{\mathbf{w}}(\mathbf{d}) = (1 - \alpha)Q_{\mathbf{w}}(\mathbf{d}) + \alpha R_{\mathbf{w}}(\mathbf{d}). \quad (1)$$

onde α representa o peso das recomendações em relação à própria avaliação da testemunha em relação ao comportamento do réu. O valor de $R_{\mathbf{w}}(\mathbf{d})$ é calculado a partir das

recomendações recebidas, e leva em conta a confiança do recomendador. A avaliação de comportamento $Q_{\mathbf{w}}(\mathbf{d})$ feita pela testemunha é dada pela expressão

$$Q_{\mathbf{w}}(\mathbf{d}) = \beta E_{\mathbf{w}}(\mathbf{d}) + (1 - \beta) T_{\mathbf{w}}(\mathbf{d}). \quad (2)$$

onde $T_{\mathbf{w}}(\mathbf{d})$ representa o nível de confiança no momento anterior, $E_{\mathbf{w}}(\mathbf{d})$ representa o nível de confiança estimado pelo BBDS e β indica o peso da avaliação do BBDS em relação ao nível de confiança estimado anteriormente.

O objetivo desse mecanismo é classificar a confiança dos nós, baseado-se em ações passadas de maneira escalável. Uma importante característica desse modelo é o uso de recomendações, que no cálculo do valor de confiança, auxiliam nós que possuem baixa percepção às ações dos outros e sistema BBDS de baixa eficiência. Além disso, nós que mintam em suas recomendações podem ser detectados pelo BBDS e ter seu valor de confiança diminuído, e assim suas recomendações perdem peso. Desta forma, a utilização de um modelo de confiança com o sistema de gerenciamento de identidades permite a identificação e caracterização correta do comportamento dos nós.

4. Mecanismo Proposto

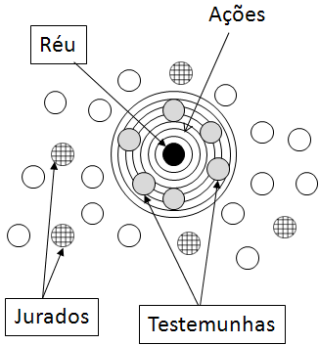
Nesta seção é apresentado o mecanismo proposto para a exclusão de nós da rede. O foco é a construção de um mecanismo distribuído robusto e acurado baseado em um tribunal de júri. O mecanismo identifica os nós não cooperativos e os expulsa da rede. Além disso, o mecanismo previne e resiste a ataques de *Sybil*, mentirosos e em conluio. A seguir a operação básica da proposta é descrita.

4.1. Ideia Básica do Mecanismo Proposto

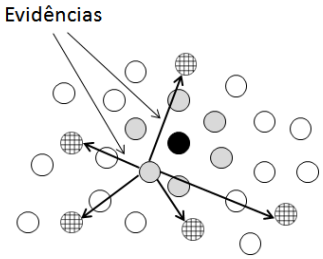
Após entrarem na rede, os novos membros, assim como os membros antigos, fazem sua parte no controle da rede, e assumem os papéis de réu, testemunha e jurado. Assim, todo nó é réu e para cada réu é associado um júri, que é um grupo de nós responsáveis pela avaliação da exclusão do réu. Assim, todo nó também é jurado e cada jurado constrói um valor de reputação para o réu, e quando a reputação fica menor que um limiar, o jurado vota pela exclusão do réu. A votação é sempre definida pela maioria, assim, se nós maliciosos quiserem forçar a exclusão de algum nó, eles precisam estar em maioria. Um jurado de um réu é escolhido dinamicamente e aleatoriamente de acordo com a lista de nós participantes da rede. Aplica-se a função *hash* ao identificador de um réu, para se achar um identificador de um nó da rede, que se torna um jurado do réu. O próximo jurado do réu é obtido reaplicando-se a função *hash* ao resultado obtido no passo anterior. Esse procedimento repete-se até achar todos os jurados do réu. Dessa maneira, como todos nós conhecem a lista de participantes da rede, eles podem descobrir os jurados de qualquer réu. Além disso, o júri é atualizado todas as vezes que a lista de participantes é modificada por causa de entrada ou saída de nós, ou por partições na rede. Assim, nós maliciosos em conluio que tentem se organizar para excluir um nó, têm pouca probabilidade de fazer parte do júri de um mesmo réu.

As testemunhas são responsáveis pelo monitoramento de seus vizinhos. Através de um sistema detector de mau comportamento (BBDS), as testemunhas detectam as ações dos vizinhos e inferem um valor de confiança com o modelo apresentado na

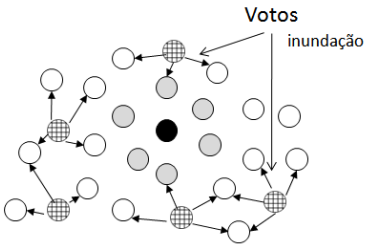
Seção 3. Ao detectar um comportamento não cooperativo, seja malicioso, egoísta ou prejudicial devido à escassez de recursos, as testemunhas transformam o nó em réu do tribunal do júri ao enviar mensagens de evidência para o júri, denunciando as ações do réu. Esse procedimento é representado pela Figura 1. Primeiro, na Figura 1(a), as testemunhas percebem ações do nó réu, e classificam seu comportamento como prejudicial. Em seguida, as testemunhas enviam mensagens de evidência para o júri periodicamente enquanto o comportamento do réu continuar classificado como prejudicial, como mostrado na Figura 1(b). Finalmente, ao receberem as mensagens de evidência, os jurados realizam uma votação para julgar se o nó réu deve ser expulso da rede.



(a) O nó réu realiza ações que são percebidas pelo sistema detector de mau comportamento (BBDS) das testemunhas. A partir da avaliação do BBDS, as testemunhas inferem um nível de confiança no nó réu.



(b) As testemunhas, ao julgarem que o nó réu não é confiável, seja por sua natureza ser maliciosa, egoísta, ou por estar com limitações de recursos, enviam mensagens de evidência ao júri.



(c) Um jurado, baseado nas mensagens de evidência recebidas julga se o réu deve ser excluído da rede. Caso decida pela exclusão, ele inunda a rede com seu voto. Se mais da metade dos jurados votarem pela exclusão, o réu é excluído da rede, e passa a ser ignorado por todos os outros nós.

Figura 1. O processo de exclusão de nós

Nas próximas seções, o réu será referido por $\mathbf{d}$, que tem seu comportamento monitorado por um grupo de testemunhas $\mathbf{W_d}$. Então, $\mathbf{w} \in \mathbf{W_d}$ é uma testemunha de $\mathbf{d}$. O grupo de testemunhas $\mathbf{W_d}$ envia mensagens de evidência para o júri $\mathbf{J_d}$. O tamanho do júri, $|\mathbf{J_d}| = S_\mathbf{J}$, é defindo pelo nó raiz no momento de criação da rede ad hoc. As decisões de exclusão de nós são realizadas por meio de votação da maioria, ou seja, somente se $\mathbf{k_J} = \lfloor S_\mathbf{J}/2 \rfloor + 1$ nós do júri votarem a favor da decisão.

4.2. Mecanismo de Envio de Evidências

O mecanismo de envio de evidências dita a relação entre testemunhas e o júri. Evidências são mensagens enviadas por testemunhas que informam ao júri sobre com-

portamentos não cooperativos de um réu. As testemunhas monitoram as ações do réu, e quando avaliam que o comportamento do réu não é como o esperado, possivelmente prejudicando a rede, elas enviam mensagens de evidência. Portanto, os nós devem ser capazes de detectar e avaliar as ações dos nós vizinhos. As testemunhas usam um sistema detector de mau comportamento (BBDS) para realizar essa tarefa.

Em uma primeira abordagem, evidências são simples notificações que um nó realizou uma ação prejudicial à rede detectada pelo BBDS. Por conseguinte, uma ação prejudicial de um nó $\mathbf{d}$ faz com que cada vizinho $\mathbf{w} \in \mathbf{W_d}$ envie uma mensagem de evidência para o júri $\mathbf{J_d}$. ACACIA utiliza essa abordagem, na qual os nós enviam mensagens para um grupo de nós de controle (*controllers*) todas as vezes que um nó perceber uma ação não cooperativa de outro nó (detectada pelo BBDS).

O mecanismo de exclusão proposto utiliza o modelo de confiança descrito na Seção 3 que constrói um valor para caracterizar a confiança dos vizinhos baseado em avaliações do BBDS e recomendações de vizinhos. Somente quando o valor de confiança de um nó testemunha em seu nó réu vizinho for baixo, o nó envia mensagens de evidência para o júri do réu periodicamente, enquanto o valor de confiança permanecer baixo. Esse procedimento evita que ações realizadas por um réu sejam mal avaliadas ou mal interpretadas e façam que a testemunha envie mensagens de evidências quando não deveria. Ademais, uma testemunha pode não perceber uma ação, mas os vizinhos comuns ao réu podem perceber a ação e enviar recomendações com suas opiniões acerca do comportamento do réu. Então, se as testemunhas adquirirem um grupo mais consistente de informações e avaliam o réu e acordo com um modelo de confiança, então a informação enviada ao júri será mais precisa e evitará expulsão errônea de nós da rede. O modelo de confiança utilizado é o descrito na Seção 3.

A utilização desse modelo de confiança permite que as evidências sejam enviadas somente quando o valor de confiança for menor que um limiar de confiança mínima para permanecer na rede. Por esta razão o mecanismo evita o envio de mensagens de evidência antes da certeza da baixa confiabilidade do nó, diminuindo assim a sobrecarga das mensagens de controle.

4.3. Mecanismo de Exclusão de Nós

O mecanismo de exclusão de nós utilizado é baseado em um sistema de reputação, que é construído através das evidências enviadas pelas testemunhas. Portanto, a proposta baseia-se em um sistema de confiança de dois níveis. O primeiro nível é executado entre as testemunhas localmente na vizinhança do réu, e o segundo nível do sistema de confiança é realizado pelas interações das testemunhas com o júri. Ao se utilizar a abordagem de dois níveis de confiança, é possível obter uma detecção e exclusão acurada de nós não cooperativos. Assim, um jurado possui um valor de reputação para seu réu e através das mensagens de evidências, ele atualiza o valor de reputação do réu. Quando a reputação do réu atingir um valor mais baixo que um limiar, o jurado vota pela exclusão do réu.

O sistema de confiança de segundo nível é executado dentro do júri, que trata as evidências das testemunhas e avalia um valor de reputação para o réu. Esse sistema tem como objetivos a baixa sobrecarga de mensagens de controle e baixo impacto no sistema por causa de mentirosos e falhas do BBDS. O mecanismo funciona da seguinte

maneira: um nó jurado mantém a reputação de seu réu, e todas as vezes que ele receber uma mensagem de evidência, ele decrementa o valor da reputação. O valor da reputação é incrementado automaticamente a cada período determinado de tempo se o jurado não receber nenhuma mensagem de evidência.

A definição do funcionamento do sistema se segue: um nó jurado de $\mathbf{d}$ ($\mathbf{j} \in \mathbf{J_d}$), mantém a reputação de $\mathbf{d}$ no momento i, denotada por $R^i_{\mathbf{d|j}}$. Se o jurado receber uma evidência da testemunha $\mathbf{w}$ ele atualiza o valor da reputação para

$$R^i_{\mathbf{d|j}} = \max\left(R^{i-1}_{\mathbf{d|j}} - u, 0\right) \tag{3}$$

onde u é a unidade de decremento/incremento da reputação. Para evitar a sobrecarga de evidências, o jurado só aceita uma evidência de uma testemunha dentro de um período T_E. Ademais, o valor de reputação é incrementado periodicamente para reduzir o impacto de evidências falsas. Após um período T_R sem evidências a reputação é atualizada para

$$R^i_{\mathbf{d|j}} = \min\left(R^{i-1}_{\mathbf{d|j}} + u, R_{max}\right) \tag{4}$$

onde R_{max} é a reputação máxima permitida. Caso a reputação atinja o limiar $T_{\mathbf{d|j}}$, o jurado $\mathbf{j}$ vota pela exclusão do nó $\mathbf{d}$. O voto é difundido na rede, e quando o réu possuir $\mathbf{k_J}$ ele é excluído da rede, e os nós da rede não consideram mais suas mensagens.

O limiar $T_{\mathbf{d|j}}$ é utilizado como forma de proteção contra ataques *Sybil*. Nesse tipo de ataque, o nó malicioso cria diversas identidades para dividir ou levar a culpa de suas ações maliciosas. Assim, a forma de proteção contra esse tipo de ataque é dificultar a obtenção de identidades. Neste sentido, o valor do limiar $T_{\mathbf{d|j}}$ é modificado todas as vezes que um descendente na cadeia de delegação for expulso da rede para

$$T_{\mathbf{d|j}} = \max\left(T_{\mathbf{d|j}} + \frac{F_{\mathbf{d}}}{N \cdot h} \cdot c, 1\right) \tag{5}$$

onde $F_{\mathbf{d}} = \min(F_{\mathbf{d}_{max}}, N)$, $F_{\mathbf{d}_{max}}$ é o número máximo de descendentes de d, N o número de nós na rede e h o número de saltos na cadeia de delegação entre o nó réu $\mathbf{d}$ e seu descendente expulso da rede. O parâmetro c é usado para ajustar a importância do incremento do limiar. A atualização do limiar desencoraja ataques *Sybil*, pois aumenta a responsabilidade ao convidar novos nós e distribuir convites para seus descendentes.

Nessa abordagem, o voto pela exclusão do réu é diretamente relacionado pela taxa de evidências recebidas pelo jurado. Se as evidências forem enviadas a cada ação não cooperativa detectada pelo BBDS como o sistema ACACIA, ao se variar número de vizinhos de um réu, a taxa de evidências também varia, e altera o taxa de decremento da reputação. Como consequência, a acurácia do sistema de reputação e, portanto do mecanismo de exclusão depende do número de vizinhos. Entretanto, o uso do sistema de confiança de dois níveis reduz esse efeito. Testemunhas enviam as mensagens de evidência somente quando o valor de confiança converge para um valor abaixo do limiar, e devido à troca de recomendações, as testemunhas provavelmente possuem valor de confiança semelhante no réu, e consequentemente enviam as mensagens de evidência ao mesmo tempo.

5. Simulações

Para avaliar a proposta foram realizadas simulações utilizando o *Network Simulator 3* (NS-3) [ns3, 2006] comparando a proposta que utiliza o sistema de confiança em dois níveis com o sistema ACACIA. A comparação com o sistema ACACIA permite avaliar o impacto do uso do mecanismo de confiança proposto. As simulações avaliam a acurácia do mecanismo de exclusão quando ocorrem erros de classificação de comportamento do sistema detector de mau comportamento (BBDS) e quando a testemunhas não são capazes de perceber todas ações. Além disso, verificamos a sobrecarga de mensagens do mecanismo de exclusão e tempo desde a entrada de um nó mal comportado até sua exclusão. A seguir o modelo é descrito e em seguida as simulações e resultados.

5.1. Modelo de Comportamento dos Nós

Neste artigo foi utilizado um modelo de comportamento no qual um nó realiza dois tipos de ações, boas ou más. Nesse contexto, é definida a natureza de um nó como um valor entre 0 e 1 que define a frequência das ações boas e más. Assim, se um nó possui natureza igual a $0,6$, isso significa que 6 ações de cada 10 são boas e 4 são más. Todos nós realizam ações com intervalo exponencialmente distribuído de valor médio de 1 unidade de tempo ($\lambda = 1$). O sistema detector de comportamento (BBDS) foi modelado para estimar a natureza dos nós baseado em ações passadas. Ademais, o limiar de natureza mínima permitida para que um nó permaneça na rede foi definido como $0,3$. Esse valor pode ser modificado de acordo com os requisitos da rede para garantir uma confiabilidade mais alta ou permitir uma confiabilidade mais baixa. As testemunhas ao detectarem que o réu possui menor valor de confiança que o limiar mínimo de natureza, enviam evidências ao júri. Assim toda exclusão de nós com natureza abaixo deste limiar é considerada como verdadeiro positivo e acima como falso positivo, e da mesma maneira, uma não exclusão de nós com natureza acima deste limiar é considerada como verdadeiro negativo e abaixo como falso negativo[1].

É considerado que a detecção de ações não é perfeita. Um nó percebe somente parte das ações dos vizinhos. Para modelar falhas de detecção de comportamento, foi definida a percepção, um valor que indica a probabilidade de um nó detectar ações de outros. As simulações utilizaram um valor de 50% de percepção a não ser quando explicitamente dito diferente. Todos os resultados são apresentados com 95% de intervalo de confiança.

5.2. Resultados

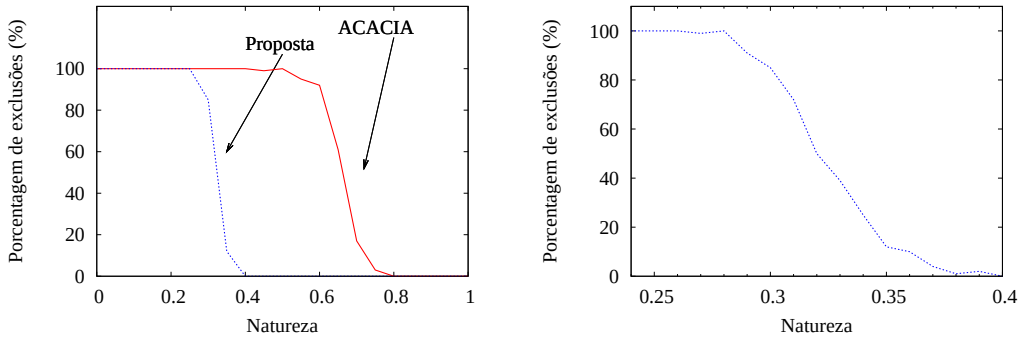
Primeiramente foram realizados testes com topologia em grade 3x3, no qual cada nó só tem vizinhança com os nós adjacentes. Somente o nó central possui adjacência com todos outros, e nessa simulação, o nó central tem sua natureza variada enquanto os outros nós possuem natureza 1, ou seja, não realizam ações maliciosas.

Para verificar a eficiência da exclusão, a natureza do nó central é variada de 0 até 1. O nó central deve ser excluído da rede quando sua natureza for menor que $0,3$. A Figura 2(a) mostra a porcentagem das rodadas nas quais o nó central foi excluído da rede[2]. A utilização do sistema de confiança em dois níveis aumenta a acurácia das exclusões em comparação ao sistema ACACIA. A Figura 2(b) mostra que os falsos positivos

[1]Os modelos dos ataques correspondem a descarte de pacote de dados, então não têm efeito no controle da rede.

[2]Essas simulações tiveram 100 rodadas.

concentram-se perto do limiar de natureza estabelecido em uma faixa até 0,9 de natureza acima da estabelecida, o que representa um ganho de acurácia de até 50 vezes comparado com a outra proposta.



(a) Porcentagem de rodadas que houve exclusão de nós.

(b) Eficiência de exclusão de nós com modelo de confiança.

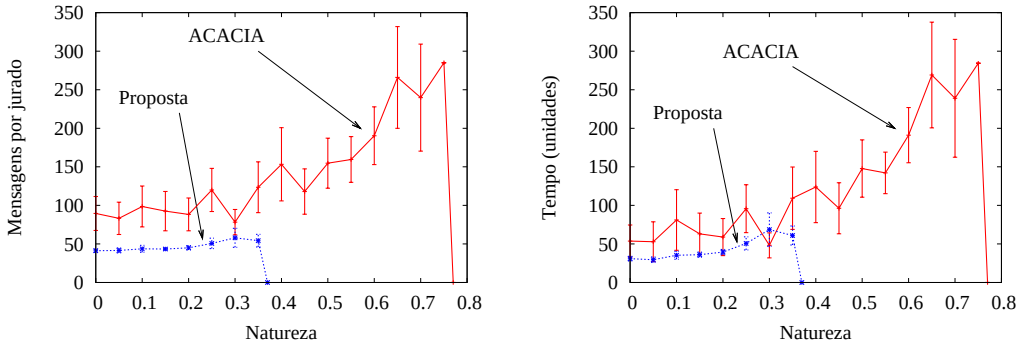
Figura 2. Eficiência de exclusão.

A Figura 3(a) mostra o número de evidências que cruzam a rede por jurado, e uma vez que os jurados estão distribuídos na rede, essas mensagens causam grande impacto em toda rede. O valor zero de evidências indica que não houve expulsões, apesar de possíveis evidências terem sido enviadas. O mecanismo proposto não envia mensagens de evidência enquanto a confiança do no é maior que o limiar de natureza da rede, devido à utilização do modelo de confiança do primeiro nível. Logo, a sobrecarga d mensagens de controle do mecanismo proposto é bem menor que no sistema ACACIA, que por sua vez envia mensagens todas as vezes que uma ação maliciosa é detectada.

A Figura 3(b) mostra o tempo até a exclusão do nó central. No modelo de confiança do primeiro nível, antes das testemunhas começarem a enviar evidências, o valor de confiança no vizinho deve convergir para um valor abaixo do limiar de natureza. Apesar disso, o tempo até a exclusão do nó do mecanismo proposto é equivalente ao sistema ACACIA. Além disso, o tempo de exclusão e não ultrapassa 70 unidades de tempo, ou seja, considerando que a taxa de ações é uma por unidade de tempo, o mecanismo demora até 70 ações para excluir um nó.

Posteriormente foram realizadas simulações em redes com 64 nós com topologia em grade. A natureza dos nós é definido por uma variável aleatória uniformemente distribuída entre 0 e 1. Portanto, isso significa que aproximadamente 30% dos nós têm natureza abaixo do limiar e são considerados não confiáveis para a rede.

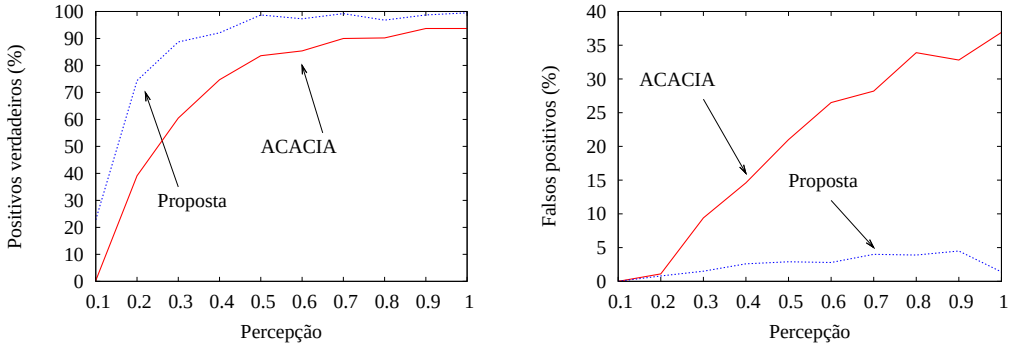
Para simular falhas de detecção de ações e classificação errada de comportamento do BBDS, dois tipos de simulação forma realizadas. No primeiro tipo, a taxa das ações percebidas pelos nós é variada, ao se varia o parâmetro percepção dos nós. A Figura 4(a) mostra a eficiência de exclusão ao se variar a percepção. Apesar dos nós possuírem percepção baixa, o mecanismo com confiança possibilita alta eficácia de exclusão de nós e, além disso, como mostrado no gráfico 4(b), o mecanismo de confiança mantém a taxa de falsos positivos abaixo de 5%. Com 100% de percepção, a eficiência de exclusão obtida é de 99,5% com uma taxa de 1,4% de falsos positivos.



(a) Número de evidências trafegadas na rede até a exclusão do nó.

(b) Tempo até a exclusão dos nós.

Figura 3. Número de evidências e tempo de exclusão.



(a) Taxa de positivo verdadeiro.

(b) Taxa de falso positivo.

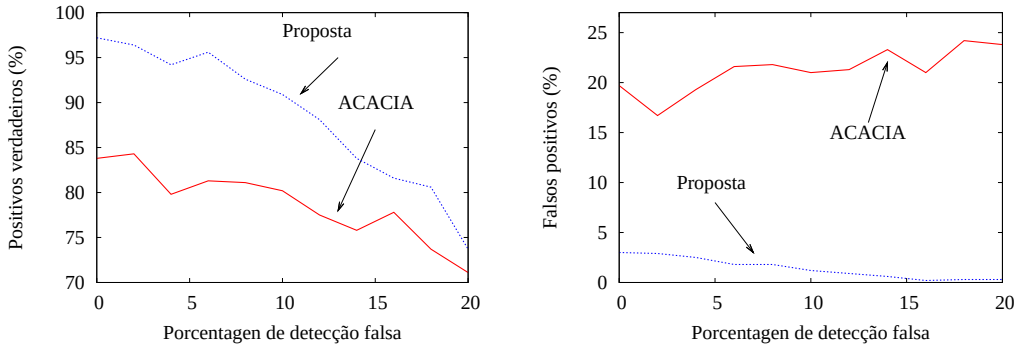
Figura 4. Eficiência de exclusão de nós com diferentes valores de percepção.

Os testes anteriores consideram que o sistema detector de comportamento (BBDS) é perfeito, quando detecta ações, as classifica corretamente entre boas ou más. No segundo tipo de simulação de falhas do BBDS, varia-se a probabilidade de classificação correta do BBDS, que pode classificar uma ação boa em má e vice-versa. Assim, um cenário mais próximo do real é simulado, no qual uma ação boa de encaminhamento pode ser confundida por uma ação maliciosa devido a colisões de pacotes. A Figura 5(a) e 5(b) mostra que o BBDS pode cometer até 18% de falhas na classificação das ações e o mecanismo proposto ainda exclui corretamente 80% do nós não cooperativos com a taxa de falsos positivos abaixo de 3%.

Então como mostrado, o mecanismo proposto ao utilizar o sistema de confiança de dois níveis, realiza a exclusão robusta de nós não cooperativos. Além disso, o mecanismo aprimora a eficiência e a acurácia das exclusões, pois o mecanismo proposto é capaz de detectar nós com naturezas diferentes, enquanto a outra proposta não distingue nós que realizam ações não cooperativas esporádicas.

6. Conclusão

Esse artigo aborda a questão do controle de acesso em redes ad hoc, especificamente a exclusão de nós não cooperativos. A exclusão de nós é importante para garantir



(a) Taxa de positivo verdadeiro. (b) Taxa de falso positivo.

Figura 5. Eficiência de exclusão de nós com erros de classificação de ações.

o funcionamento da rede, mantendo na rede apenas nós cooperativos.

O artigo propõe um mecanismo distribuído de exclusão de nós não cooperativos. O mecanismo foi inspirado em um tribunal de júri, de maneira que todos nós possuem múltiplos papéis. Deste modo, os nós são responsáveis pelo monitoramento da vizinhança (papel de testemunha), exclusão de nós (papel de jurado), e também estão sujeitos ao tribunal de júri (papel de réu). Ademais, o mecanismo usa um modelo de confiança para identificar os nós que prejudicam o funcionamento da rede. O modelo de confiança garante a exclusão acurada de nós, baixa sobrecarga de mensagens devido ao funcionamento local do modelo, e robustez do mecanismo de exclusão em relação a falhas do sistema detector de mau comportamento.

O uso de um sistema de autenticação e gerenciamento de identidades, e de um modelo de confiança que utiliza a troca de experiência entre vizinhos, faz o mecanismo de exclusão ser resistente a diferentes ataques e realizar a exclusão baseado em um consenso global de confiança. Além disso, O mecanismo obteve uma eficiência máxima de 99,5% com uma taxa de 1.4% de falsos positivos em resultados de simulações.

Referências

[Adnane et al., 2008] Adnane, A., de Sousa, Jr., R. T., Bidan, C. e Mé, L. (2008). Autonomic trust reasoning enables misbehavior detection in olsr. Em *Proceedings of the 2008 ACM symposium on Applied computing*, SAC '08, p. 2006–2013, New York, NY, USA. ACM.

[Al-Karaki e Kamal, 2008] Al-Karaki, J. N. e Kamal, A. E. (2008). Stimulating node cooperation in mobile ad hoc networks. *Wirel. Pers. Commun.*, 44:219–239.

[Buchegger e Le Boudec, 2002] Buchegger, S. e Le Boudec, J.-Y. (2002). Performance analysis of the confidant protocol. Em *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '02, p. 226–236, New York, NY, USA. ACM.

[Buttyan e pierre Hubaux, 2003] Buttyan, L. e pierre Hubaux, J. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. *ACM/Kluwer Mobile Networks and Applications (MONET*, 8:579–592.

[Dehnie e Tomasin, 2010] Dehnie, S. e Tomasin, S. (2010). Detection of selfish nodes in networks using coopmac protocol with arq. *Wireless Communications, IEEE Transactions on*, 9(7):2328 –2337.

[Fernandes et al., 2010] Fernandes, N., Moreira, M. e Duarte, O. (2010). A self-organized mechanism for thwarting malicious access in ad hoc networks. Em *INFOCOM, 2010 Proceedings IEEE*, p. 1 –5.

[Luo et al., 2004] Luo, H., Kong, J., Zerfos, P., Lu, S. e Zhang, L. (2004). Ursa: ubiquitous and robust access control for mobile ad hoc networks. *Networking, IEEE/ACM Transactions on*, 12(6):1049 – 1063.

[Luo et al., 2005] Luo, J., Hubaux, J.-P. e Eugster, P. T. (2005). Dictate: Distributed certification authority with probabilistic freshness for ad hoc networks. *IEEE Trans. Dependable Secur. Comput.*, 2:311–323.

[Mahmoud e Shen, 2010] Mahmoud, M. E. e Shen, X. (2010). Stimulating cooperation in multi-hop wireless networks using cheating detection system. Em *Proceedings of the 29th conference on Information communications*, INFOCOM'10, p. 776–784, Piscataway, NJ, USA. IEEE Press.

[Marti et al., 2000] Marti, S., Giuli, T. J., Lai, K. e Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. Em *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, p. 255–265, New York, NY, USA. ACM.

[ns3, 2006] ns3 (2006). The ns3 network simulator. Acessado em http://www.nsnam.org/. `http://www.nsnam.org/`.

[Song e Zhang, 2010] Song, C. e Zhang, Q. (2010). Protocols for stimulating packet forwarding in wireless ad hoc networks [security and privacy in emerging wireless networks]. *Wireless Communications, IEEE*, 17(5):50 –55.

[Sun et al., 2008] Sun, Y., Han, Z. e Liu, K. (2008). Defense of trust management vulnerabilities in distributed networks. *Communications Magazine, IEEE*, 46(2):112 –119.

[Velloso et al., 2010] Velloso, P., Laufer, R., de O Cunha, D., Duarte, O. e Pujolle, G. (2010). Trust management in mobile ad hoc networks using a scalable maturity-based model. *Network and Service Management, IEEE Transactions on*, 7(3):172 –185.

[Yang et al., 2006] Yang, H., Shu, J., Meng, X. e Lu, S. (2006). Scan: self-organized network-layer security in mobile ad hoc networks. *Selected Areas in Communications, IEEE Journal on*, 24(2):261 – 273.

[Yu e Liu, 2005] Yu, W. e Liu, K. (2005). Attack-resistant cooperation stimulation in autonomous ad hoc networks. *Selected Areas in Communications, IEEE Journal on*, 23(12):2260 – 2271.

[Zakhary e Radenkovic, 2010] Zakhary, S. e Radenkovic, M. (2010). Reputation-based security protocol for manets in highly mobile disconnection-prone environments. Em *Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on*, p. 161 –167.

[Zhou e Haas, 1999] Zhou, L. e Haas, Z. (1999). Securing ad hoc networks. *Network, IEEE*, 13(6):24 –30.