Controle de Acesso Auto-Organizável e Robusto Baseado em Nós Delegados para Redes Ad Hoc

Natalia Castro Fernandes e Otto Carlos Muniz Bandeira Duarte

[1]GTA/PEE/COPPE – Universidade Federal do Rio de Janeiro
Rio de Janeiro, RJ - Brasil

{natalia,otto}@gta.ufrj.br

Abstract. *This paper proposes a new mechanism to authenticate and monitor nodes in ad hoc networks (AMORA) that carries out access control without the need for a central administration entity. AMORA uses delegation chains to specify in a distributive way which users can access the network and it proposes the use of delegate nodes to issue certificates and to monitor nodes, avoiding malicious nodes from remaining on the network. Besides, AMORA treats efficiently network initialization and partitions. The results of the analysis shows that the mechanism is robust to Sybil and Collusion attacks and that it reduces the monitoring control load in each node in comparison with other mechanisms.*

Resumo. *Este artigo propõe um mecanismo para Autenticação e MOnitoração em Redes Ad hoc (AMORA) para realizar o controle de acesso sem a necessidade de uma entidade administradora centralizada. O AMORA utiliza cadeias de delegação para determinar, de forma distribuída, quais usuários podem acessar a rede e propõe o uso de nós delegados para emitir certificados e para monitorar os nós, impedindo a permanência de nós maliciosos na rede. Além disso, o AMORA trata a inicialização e as partições na rede. Os resultados da análise mostram que o mecanismo é robusto aos ataques conluio e Sybil, além de reduzir a carga de controle em cada nó, quando comparado a outros mecanismos.*

1. Introdução

As redes ad hoc móveis (*Mobile Ad hoc NETworks - MANETs*) são redes sem fio não infra-estruturadas que provêem comunicação entre os nós através de roteamento colaborativo [Campista et al., 2007]. Devido às características de meio de comunicação sem fio, ausência de infra-estrutura e roteamento colaborativo em múltiplos saltos, as redes ad hoc são alvos potenciais de diversos tipos de ataques. A utilização do ar como meio de transmissão torna a rede susceptível a ataques como a espionagem e a interferência. Além disso, o roteamento colaborativo traz graves vulnerabilidades à rede, pois o comportamento malicioso de um único nó pode prejudicar toda a rede [Fernandes et al., 2006]. Assim controlar a admissão e a exclusão dos nós por meio de autenticação e monitoramento é fundamental para prover segurança a esse tipo de rede.

Um dos principais mecanismos usados em redes infra-estruturadas para prover a autenticação são as autoridades certificadoras (AC) centralizadas, que assumem a premissa de existência de um administrador da rede. Essa premissa não se aplica às redes ad hoc, que requerem mecanismos totalmente distribuídos, auto-organizáveis e robustos a falhas, a segmentações da rede e a freqüentes entradas e saídas de nós. Uma abordagem simples para criar autoridades certificadoras em redes ad hoc é a criação de diversas

réplicas de servidores de autenticação. Esta técnica de redundância elimina o ponto único de falha e aumenta a disponibilidade do serviço, o que é importante para garantir o acesso de qualquer nó ao servidor em redes com freqüentes entradas e saídas de nós e partições. No entanto, a segurança continua comprometida, pois basta que um desses servidores seja invadido para que a rede fique vulnerável.

Uma abordagem distribuída e robusta a ataques é a que utiliza a técnica de criptografia de limiar [Zhou e Haas, 1999, Yi e Kravets, 2003, Pereira et al., 2007]. Nessa abordagem, a chave privada da autoridade certificadora (AC) é "dividida" em n sub-chaves e distribuída para um conjunto de n nós, de forma que apenas com a combinação de pelo menos $k \leq n$ assinaturas de sub-chaves é possível gerar uma assinatura idêntica a que seria gerada pela chave privada da AC. Assim, garante-se uma alta robustez do sistema, pois, para a rede ficar vulnerável, seria necessário invadir k dos n nós escolhidos para representar a autoridade certificadora. Portanto, esta técnica apresenta robustez ao ataque de conluio, que é um dos ataques mais difíceis de ser evitado. Por outro lado, para se obter uma assinatura com a chave privada da AC, k dentre os n nós precisam ser acessados. Assim, o serviço de autenticação torna-se indisponível para um nó qualquer da rede se este nó não conseguir acessar k dentre os n nós da AC. Portanto, a escolha dos valores n e k é um compromisso entre a disponibilidade e a confiabilidade do sistema. A principal desvantagem dessa proposta é a necessidade de um administrador que determina os usuários que podem acessar a rede, além de definir os valores de n e k, determinar quais os n nós escolhidos e distribuir as n sub-chaves da autoridade certificadora. Estas funções realizadas pelo administrador não são compatíveis com as características das redes ad hoc puras, que devem ser auto-organizáveis [Merwe et al., 2007]. É importante ressaltar que a escolha pelo administrador de k e n é rígida, pois se for necessário mudar estes valores por motivo de confiabilidade ou disponibilidade, é necessário que o administrador redistribua novas chaves parciais para os novos valores. A inicialização da rede também traz desafios para esta técnica, pois é necessário que exista pelo menos k nós da AC presentes na inicialização da rede para que o serviço de autenticação funcione e permita o ingresso de outros nós na rede. Portanto, embora as AC baseadas em criptografia de limiar sejam mais adequadas para redes ad hoc do que o uso de réplicas do servidor, elas ainda dependem de um administrador e de uma infra-estrutura fixa.

Uma abordagem distribuída e auto-organizável, não dependendo de administrador ou infra-estrutura, é a baseada em cadeias de certificados [Capkun et al., 2003, Hubaux et al., 2001]. Nesta abordagem, a rede é criada pelos usuários finais sem a necessidade de relações de segurança pré-estabelecidas entre os usuários, de forma que o funcionamento da rede depende apenas da cooperação e confiança entre os nós [Buttyan e Hubaux, 2003]. Nas propostas que utilizam cadeias de certificados, os nós se autenticam por meio da busca por cadeias de certificados em comum. Assim, se o nó A deseja se comunicar com o nó C, com o qual o nó A nunca teve contato, o nó A precisa autenticar o certificado de C. Supondo que o nó A conheça um terceiro nó, o nó B, no qual A confia. Se B já conhece C, pode informar a A que C é autêntico e, dessa forma, A passa também a confiar em C. Assim, para dois nós se comunicarem de forma segura, eles precisam percorrer uma cadeia de certificação até algum nó em que ambos confiam. Portanto, não existe uma autoridade certificadora central ou distribuída na qual todos os nós precisam confiar. A ausência de administrador e de infra-estrutura permite classificar a proposta como auto-organizável e distribuída. Além disso, não existem nós da rede com

funções especiais, como acontece com os n nós da criptografia de limiar. Por essas razões, a proposta atende a todas as características de uma rede ad hoc pura. Por outro lado, a abordagem de cadeia de certificado não controla o ingresso de nós na rede, o ingresso na rede se dá através da escolha de uma identidade e de um par de chaves. Portanto, não é possível excluir nós da rede mesmo que exista um sistema de monitoração, pois qualquer nó identificado como malicioso pode trocar de identidade e retornar a rede.

Neste artigo, é proposta uma nova abordagem distribuída, auto-organizável e sem entidade administradora centralizada, como a proposta de cadeia de certificados, mas que realiza o controle de ingresso e a monitoração de nós para exclusão de nós maliciosos da rede. O objetivo é obter uma robustez semelhante ao do mecanismo de criptografia de limiar sem as suas desvantagens. O mecanismo proposto, chamado de Autenticação e MOnitoração em Redes Ad hoc (AMORA), utiliza cadeias de delegação para autorização de ingresso e autenticação de nós na rede. Dessa forma, usuários autorizados a utilizar a rede podem delegar o acesso à rede a outros usuários, formando a cadeia de delegação. Assim, a entidade administradora que controla o acesso a rede deixa de ser centralizada e passa a ser distribuída. O AMORA também propõe os nós delegados, que são uma estrutura dinâmica fundamental para a certificação e a monitoração dos nós que provê robustez e alta disponibilidade. Os nós delegados são responsáveis pela verificação/revogação do direito de acesso e emissão de certificados para os nós que estiver monitorando. A utilização dos nós delegados permite uma maior flexibilidade, já que basta uma consulta aos delegados para saber se um determinado nó pode acessar a rede, mesmo que o nó que o autorizou não esteja presente. Portanto, o AMORA é adequado às características das redes ad hoc, pois é auto-organizável, distribuído, trata as partições e a inicialização da rede e é robusto contra ataques em conluio e ataques *Sybil*.

O artigo está organizado da seguinte forma. Na Seção 2, é apresentada uma descrição detalhada da proposta e, na Seção 3, é feita uma análise do mecanismo proposto. Por fim, na Seção 4, são apresentadas as conclusões.

2. O Sistema de Controle de Acesso Proposto

O AMORA controla o acesso à rede através dos mecanismos propostos de autorização de acesso, autenticação, monitoração e exclusão de nós maliciosos. Para tanto, duas estruturas principais são utilizadas: a cadeia de delegação e os nós delegados.

2.1. A Cadeia de Delegação para Autorização de Ingresso na Rede

O mecanismo proposto de autorização de ingresso na rede é distribuído e baseia-se em cadeias de delegação [Tamassia et al., 2004, Elien, 1998] para evitar a necessidade de um administrador centralizado que determine quais usuários podem ingressar na rede. A autorização de ingresso de usuários é feita por usuários já autorizados, através da emissão de mensagens de autorização para os novos usuários, formando uma cadeia de delegação, como mostrado na Figura 1a. Portanto, o AMORA confia nas relações sociais entre os usuários para permitir o ingresso na rede.

Na cadeia de delegação, a raiz é o usuário que dá inicio a distribuição de autorizações, embora a raiz não precise ter nenhuma atribuição especial. O usuário que autoriza outro usuário a ingressar na rede é chamado de “pai” e o usuário autorizado é chamado de “filho”. A relação entre pai e filho na cadeia de delegação do AMORA é

baseada na identidade do usuário, a qual está associada a um par de chaves assimétricas. Há uma distinção entre usuário e nó da rede. Um usuário é uma pessoa que pode usar a rede, enquanto que um nó é o usuário que ingressa na rede e passa a ser identificado pelo endereço IP. Esta diferenciação é necessária devido à característica de auto-organização das redes ad hoc, que requerem que um nó obtenha dinamicamente o seu endereço IP. Assim, um usuário pode ingressar e sair da rede diversas vezes e a cada ingresso pode receber um endereço IP diferente. Desta forma, cada nó da rede possui dois pares de chaves assimétricas, um para a identidade do usuário e um para a identidade do nó.

Para um usuário pai autorizar o ingresso de um usuário filho, ele deve transmitir ao filho uma autorização, ilustrada na Figura 1c. A autorização é a forma de estabelecer as relações de delegação no mecanismo de autorização de ingresso proposto, e, dessa forma, é o ponto chave da cadeia de delegação. O campo Filhos da mensagem Autorização determina a quantidade de filhos que o novo usuário poderá ter. Assim, o pai pode autorizar o filho a inserir quantos filhos quiser, um total de f filhos ou, ainda, nenhum filho. Isso permite dar diferentes níveis de delegação na rede. Assim, um usuário pode permitir que outro usuário pouco confiável acesse a rede, mas sem permitir que ele autorize outros usuários a entrar na rede, ou ainda permitir que ele autorize poucos usuários. Isso é importante para limitar a capacidade dos usuários maliciosos de criar filhos na rede. Essa limitação, além de evitar o ingresso de usuários maliciosos, também impede que filhos falsos sejam criados para realizar um ataque *Sybil*. Nesse ataque, o usuário malicioso autorizado cria e assume a identidade de filhos falsos que realizam ações maliciosas. Dessa forma, mesmo que os filhos sejam identificados como maliciosos por um sistema de confiança, o usuário não seria excluído da rede. A limitação do número de filhos, embora dificulte a realização do *Sybil*, não é suficiente para impedir o ataque.

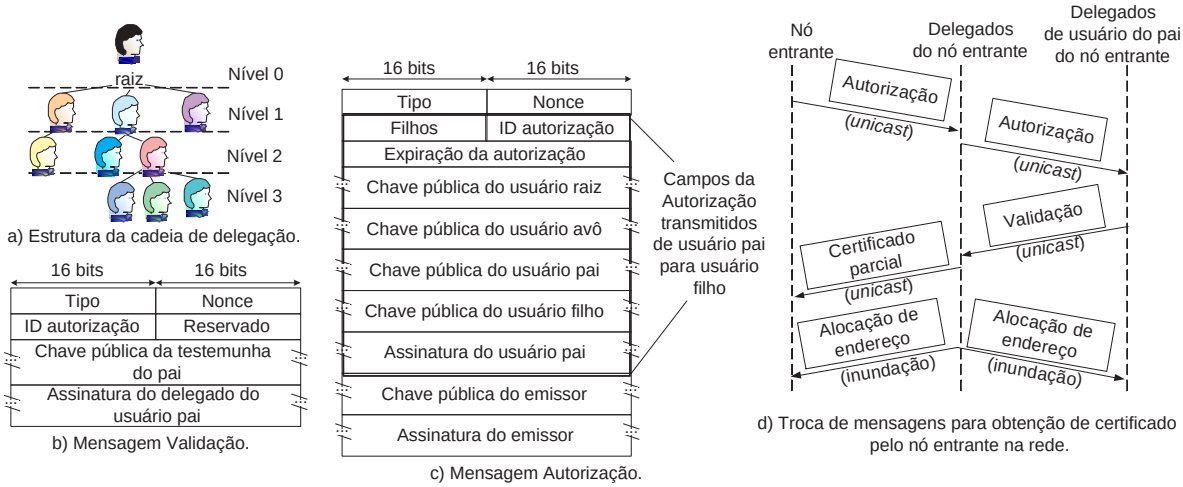


Figura 1. Formação da cadeia de delegação e ingresso na rede através do uso de autorizações.

2.2. Nós Delegados

A estrutura de cadeia de delegação sozinha não permite um controle de acesso seguro. Os nós precisam ser autenticados, ter suas ações monitoradas e os nós detectados como maliciosos devem ser excluídos da rede. A cadeia de delegação também não impede que um usuário autorizado ingresse na rede sob diferentes endereços IP simultaneamente. Além disso, o processo de autenticação para uma comunicação segura em uma cadeia de

delegação requer que os nós percorram a cadeia de certificação até a raiz para garantir que o certificado é válido. Assim, basta que um dos elos da cadeia esteja indisponível para que a autenticação falhe. Para prover segurança no controle de acesso e ao mesmo tempo flexibilizar a tarefa de autenticação, propõe-se o mecanismo de nós delegados. Os delegados são nós responsáveis pela autenticação de usuários, pela emissão de certificados, pelo monitoramento das ações maliciosas e pela entrada e saída dos nós na rede. Para garantir robustez, cada nó tem um conjunto formado por m delegados que deverão atestar se uma determinada ação deve ser tomada ou não com relação ao nó monitorado. Para prover maior disponibilidade, devido à saída de nós e à formação de partições, basta que apenas k delegados, onde $k \leq m < 2k$, se manifestem para que uma atitude seja tomada na rede. Desta forma, são necessários pelo menos k atestados de delegados para que um certificado se torne válido ou para expulsar um nó da rede. Com isso, a rede é robusta ao conluio mesmo que existam até $M < k$ nós maliciosos na rede.

Existem dois tipos de conjuntos de delegados: os de nó e os de usuário. Os delegados de nó são responsáveis por guardar e julgar os dados de monitoramento das atitudes do nó na rede. Assim, se um nó observa ações maliciosas de seu vizinho, ele deve contatar os delegados de nó do vizinho, notificando o que foi observado. Dessa forma, ao invés de cada nó guardar dados de monitoração de todos os nós, cada nó guarda informações apenas sobre os nós que está monitorando como delegado, evitando sobrecarga de armazenamento. Os delegados de usuário são responsáveis por monitorar o uso e as emissões de autorizações de ingresso. Esses delegados impedem que uma mesma autorização de ingresso seja usada simultaneamente diversas vezes para a criação de identidades falsas, além de controlar o número de filhos autorizados a ingressar na rede pelo nó monitorado.

Os delegados são distribuídos aleatoriamente entre os nós da rede através de uma função *hash*, para impedir que o nó manipule a escolha de seu conjunto de delegados, evitando o conluio na rede. Assim, cada nó obtém um conjunto de m_n delegados de nó de acordo com o seu IP e um conjunto de m_u delegados de usuário baseado na chave pública do usuário pai. O uso da chave pública do pai evita a utilização da mesma autorização para obter vários endereços IP simultaneamente. Se um nó tentar obter dois endereços IP usando a mesma autorização, os delegados de nó não detectarão a ação maliciosa, pois com IPs diferentes, o conjunto de delegados de nó é diferente. Por outro lado, os delegados de usuário serão os mesmos, pois eles são escolhidos de acordo com a chave pública do pai, que está na autorização. Esses delegados identificarão o uso malicioso da autorização e não permitirão a emissão do certificado para a segunda identidade. Com isso, impede-se que um nó utilize diversas identidades falsas com a mesma autorização, o que também caracteriza o ataque *Sybil*. O uso do endereço IP para selecionar os delegados de nó garante que qualquer nó na rede que queira acusar um comportamento malicioso saberá quais são os delegados de nó monitorando o nó acusado. Assim, os delegados de usuário são importantes para monitorar o uso da autorização e os delegados de nó, para monitorar o comportamento de cada nó.

A seleção do delegado i de nó, onde $1 \leq i \leq m_n$ é feita segundo a equação $T_i = hash^i(IP)$, e o delegado j de usuário, onde $1 \leq j \leq m_u$, pela equação $T_j = hash^j(C_p)$, onde $hash^k(X) = hash^{k-1}(X)$ e C_p é a chave pública do usuário pai. No entanto, deve-se verificar se os delegados escolhidos por essa função estão ausentes da rede, se o nó foi escolhido como seu próprio delegado e se algum delegado foi

selecionado mais do que uma vez. No AMORA, supõe-se a existência de uma estrutura capaz de armazenar os endereços utilizados na rede de forma compacta, chamada de filtro de endereços [Fernandes e Duarte, 2008]. Essa estrutura é atualizada de forma distribuída sempre que um nó entra ou sai da rede, permitindo que qualquer nó verifique se certo IP está sendo utilizado. O protocolo para atualizar o filtro de endereço permite que todos os nós estejam sempre com o mesmo estado no filtro, ou seja, com o mesmo conjunto de endereços ocupados. Caso o delegado selecionado não esteja presente na rede, seja o próprio nó ou tenha sido selecionado mais que uma vez como delegado do mesmo nó, deve ser escolhido um novo delegado no filtro de endereços como o nó que possui o menor IP maior que o IP do delegado selecionado. No caso de ausência, esse novo delegado deve ser mantido até que o delegado ausente retorne à rede, para manter a premissa de que, ao observar o filtro de endereços, é possível determinar os delegados de nó de qualquer nó.

A manutenção do conjunto de delegados é feita pelo próprio nó. Caso o nó não realize essa tarefa, o seu certificado será descartado, já que o nó que recebeu o certificado não conseguirá contatar os delegados para verificar a lista de revogação. Esta é uma lista existente em sistemas de certificação que contém os certificados dentro da validade, mas que foram revogados e não devem mais ser considerados como válidos. Dessa forma, sempre que um certificado é recebido, deve-se consultar à lista de revogação da entidade que emitiu aquele certificado. Assim, para que a consulta à lista de revogação seja bem sucedida, cada nó mantém seu conjunto de delegados através do envio periódico de pacotes de teste para seus delegados. Caso um delegado não responda ao pacote de teste, o nó anuncia à rede a ausência do delegado e, em seguida, o substitui. O conjunto de delegados de usuário, por outro lado, deve se manter ativo independente da interferência do usuário. Isso garante que qualquer usuário filho entre na rede mesmo que o pai não esteja presente. Assim, sempre que a ausência de um nó que é delegado de usuário é anunciada, esse delegado deve ser substituído. O controle de ausência e transmissão de dados para o novo delegado deve ser feito de forma automática pelos demais delegados de usuário.

2.3. Mecanismos do AMORA

2.3.1. Ingresso de Usuários/Nós na Rede

O mecanismo de ingresso de usuários/nós na rede permite que o usuário obtenha um par de chaves para ser associado ao IP escolhido, se autentique e receba um certificado. Após o ingresso, o usuário é visto como um nó pela rede e passa a ser monitorado por seus delegados e a monitorar outros nós.

Para entrar na rede, primeiramente, o novo usuário obtém uma autorização com o usuário pai. Essa autorização é obtida sem utilizar a rede com base nas relações sociais entre os usuários. Em seguida, o novo usuário escolhe um par de chaves assimétricas e fixa os primeiros p bits da chave pública como o sufixo do seu endereço IP, que será usado para identificá-lo como nó da rede. Esse procedimento associa a chave pública a um IP, o que dificulta ataques como a identidade falsa, pois o nó malicioso precisaria encontrar um par de chaves associada ao IP que deseja falsificar. Em seguida, o usuário verifica se o IP selecionado já está presente na rede. Caso esteja, um novo par de chaves é selecionado e o processo é repetido. Caso não esteja, o usuário contata os delegados correspondentes ao IP selecionado e à chave pública do usuário pai, enviando a autorização recebida do usuário pai a cada um. Os delegados do novo nó validam a autorização recebida com os delegados de usuário do usuário pai, como descrito na Figura 1d. Os delegados de usuário do usuário

pai, após receberem a mensagem dos delegados do novo nó, verificam se a autorização foi realmente gerada pelo pai e se ele ainda tem direito de emitir autorizações, conforme especificado na autorização do pai e de acordo com o número de filhos já inseridos na rede pelo pai. Caso os delegados de usuário do pai validem a autorização, através da mensagem ilustrada na Figura 1b, os delegados de nó do filho devem anunciar para toda rede que um novo endereço foi alocado. Cada nó da rede, após receber pelo menos k anúncios de novo endereço alocado assinados por delegados correspondentes ao IP anunciado, deve inserir o novo endereço no filtro de endereços.

Além de alocar o novo endereço, os delegados também devem enviar o certificado parcial (Figura 2b) para o novo nó. O certificado completo (Figura 2a) é composto por pelo menos k_n assinaturas de certificados parciais de delegados de nó e pelo menos k_u assinaturas de delegados de usuário, onde $k = k_n + k_u$. Isso garante que o nó está utilizando de forma correta a sua autorização e que não é um nó malicioso.

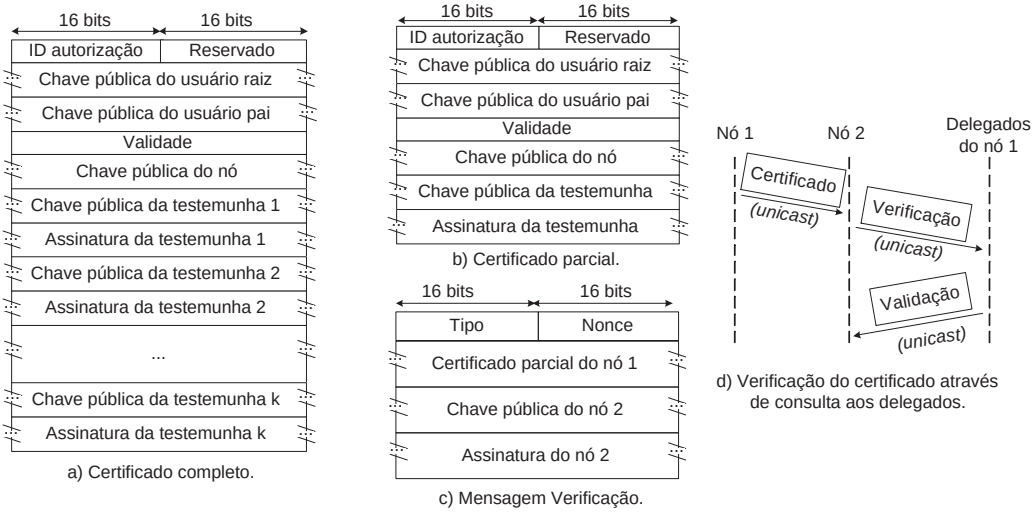


Figura 2. Certificação e verificação de listas de revogação no AMORA.

2.3.2. Monitoração e Exclusão de nós

A exclusão de um nó da rede se dá por mau comportamento ou por ausência. A exclusão por ausência pode ser indicada pelos delegados do nó ausente ou pelos nós que estavam sendo monitorados pelo nó ausente. A ausência é detectada porque cada nó e seus delegados devem trocar periodicamente pacotes de teste para que o conjunto de delegados ativos fique sempre atualizado. A exclusão por mau comportamento é indicada pelo atestado de pelo menos k_n delegados de nó e impede que nós identificados como maliciosos ou não-cooperativos permaneçam na rede.

No AMORA, quando um filho é excluído, o pai e todos os nós acima do pai na cadeia perdem pontos no parâmetro confiança, que permite avaliar se um nó é malicioso ou não. Isso impede que os nós criem filhos falsos para realizar as ações maliciosas sem serem identificados, pois, após a criação de certa quantidade de filhos maliciosos, o pai acabará sendo excluído. O sistema proposto também determina que se um nó é excluído, também devem ser excluídos todos os seus descendentes.

O sistema de monitoração do AMORA funciona com diferentes tipos de sistemas de detecção de intrusão e de confiança [Xu et al., 2007, Velloso et al., 2006]. Por

simplicidade, nessa descrição será utilizado um sistema de avaliação de comportamento simplificado. No sistema de monitoração proposto, sempre que um nó observa uma ação maliciosa, ele contata os delegados do nó, enviando a denúncia. Os delegados, ao receberem uma denúncia, verificam a assinatura e o certificado recebidos, e, caso sejam válidos, armazenam essa informação. No sistema de avaliação simplificado, cada delegado aceita apenas uma denúncia de cada nó durante um período t_d. Isso evita que os delegados sejam sobrecarregados com um excesso de mensagens de denúncia, além de evitar a sobrecarga no armazenamento das informações. Supondo que todas as denúncias tenham um peso igual, a reputação do nó i para o delegado d no momento j (${R_{i|d}}^j$) pode ser atualizada a cada denúncia por ${R_{i|d}}^j = {R_{i|d}}^{j-1} - 1$. Após um período t_a sem denúncias, a reputação é atualizada para ${R_{i|d}}^j = {R_{i|d}}^{j-1} + 1$, para evitar o impacto de falso-positivos na detecção de ações maliciosas e de denúncias falsas feitas por nós maliciosos. A variável ${R_{i|d}}^j$ é limitada por 0 e R_{max}, não devendo ultrapassar esses valores.

Cada delegado d do nó i envia para a rede um atestado de exclusão se a reputação ${R_{i|d}}^j$ do nó monitorado alcançar um limiar $L_{i|d}$. Se até k_n delegados enviarem esse atestado, o nó é excluído e o certificado deverá entrar para a lista de certificados revogados. O valor de $L_{i|d}$ indica a rigidez de avaliação do nó. Um $L_{i|d}$ grande evita que nós bem-comportados sejam excluídos injustamente, mas é menos eficiente na punição dos nós maliciosos. O valor de $L_{i|d}$ também é usado para punir nós que tenham filhos excluídos por mau comportamento. Sempre que um nó filho é excluído, $L_{i|d}$ é atualizado por $L_{i|d} = L_{i|d} + \frac{t_i}{nc_i \cdot N}$, onde t_i é o número de filhos que o nó pode inserir na rede, N é o número de nós na rede e nc_i é o número de níveis na cadeia de delegação entre o nó i e o descendente excluído. Se o número de filhos for ilimitado t_i vale N. Dessa forma, o nó que tem direito de autorizar mais filhos recebe uma punição maior por cada filho malicioso, para incentivar a responsabilidade na delegação da autorização de ingresso, o que torna a rede mais robusta. Esse mecanismo é mais uma forma de evitar o ataque *Sybil*, pois se o nó malicioso criar diversos filhos para realizar as ações maliciosas, o seu $L_{i|d}$ será reduzido até a sua exclusão da rede.

2.3.3. Emissão e Revogação de Certificados

Após o ingresso na rede, o nó possui um certificado que será utilizado para estabelecer comunicações seguras com outros nós. Eventualmente, um certificado pode ser revogado e transferido para a lista de revogação devido à exclusão de um nó. Nas autoridades certificadoras, a consulta à lista de revogação é feita pela consulta a um repositório central. No sistema proposto, o repositório é guardado de forma distribuída pelos delegados. Para validar um certificado recebido de um nó B, o nó A deve buscar em seu filtro de endereços os delegados do nó B. Caso os delegados indicados no certificado sejam referentes ao nó B e estejam todos presentes, o nó A deve fazer um pedido de verificação de certificado através da mensagem Verificação (Figura 2c), como ilustrado na Figura 2d. Os delegados deverão responder a esse pedido informando se o certificado é válido ou não, através da mensagem Validação (Figura 1b).

2.3.4. Inicialização da Rede e Formação de Partições

Além de tratar o ingresso, a saída e a revogação de certificados dos nós, o AMORA também trata a inicialização da rede e a formação de partições. A inicialização da rede é um problema para os sistemas de controle de acesso em redes ad hoc devido à inexistência

de uma garantia de um número mínimo de nós presentes na rede. Dessa forma, durante a inicialização da rede, não há como garantir que $n \geq (k+1)$, onde n é o número de nós na rede e $k = k_u + k_n$ é o número mínimo de delegados para emitir um certificado. Se $n < (k+1)$, não há como formar o conjunto de delegados. Assim, nesses casos, que podem ser detectados pelo filtro de endereços, o AMORA determina que todos os nós operem como delegados e que os certificados sejam validados com um número de assinaturas inferior a k. Esse tipo de problema também ocorre após a saída de vários nós ou durante a formação de partições, sendo tratado da mesma forma. Outra restrição relativa à inicialização é que o usuário raiz da cadeia de delegação ou os seus filhos imediatos precisam estar na rede durante a inicialização. Um usuário não pode entrar na rede enquanto o seu pai não tiver entrado, pois o ingresso exige a verificação dos delegados do pai, que só são criados após o primeiro contato do pai com a rede. Como todos os nós conhecem a chave pública da raiz, todos os nós no nível um da cadeia de delegação podem validar a autorização dada pela raiz com qualquer nó. As demais autorizações precisarão ser validadas gradativamente, com o ingresso dos nós filhos e seus descendentes.

Um problema da formação de partições é a separação dos delegados do nó monitorado. Os delegados que forem deslocados para outra partição considerarão o nó monitorado como ausente e apagarão todos os dados, exceto listas de revogação e autorizações referentes ao nó. Da mesma forma, o nó perceberá a ausência dos delegados, alocando novos nós para essa atividade. Após uma união de partições, os delegados de um mesmo nó que estavam em partições diferentes devem trocar informações observadas nas suas partições para que informações não sejam perdidas.

3. Análise do Sistema Proposto

3.1. Robustez contra conluio na votação

O AMORA é seguro mesmo que existam até $k-1$ nós maliciosos na rede, onde $k = k_n + k_u$, k_n é o número mínimo de delegados de nó e k_u é o número mínimo de delegados de usuário para tomar uma decisão na rede. Além disso, o AMORA é robusto contra conluios para prejudicar nós não-maliciosos durante as votações mesmo que existam mais do que k nós maliciosos na rede, como será mostrado a seguir.

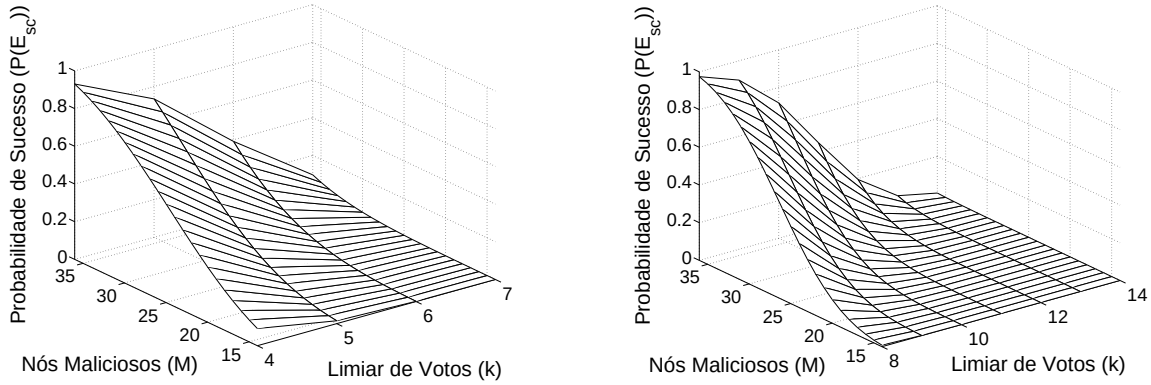
O AMORA emite/revoga certificados com base nos atestados dos delegados. Se em uma rede existem muitos nós maliciosos, o resultado de uma votação pode ser influenciado pelo envio de atestados falsos que comprometam um determinado nó. Assim, os parâmetros relativos aos delegados devem ser escolhidos de forma a minimizar a chance de sucesso em um conluio na votação. A utilização de um valor de k_i, onde $k_i \in \{k_u, k_n\}$, grande permite uma maior robustez ao conluio nas votações, pois é necessário pelo menos k_i nós comprometidos para modificar o resultado de uma votação. Por outro lado, esse parâmetro interfere na disponibilidade do serviço na rede. Se o k_i é muito grande, pode ser difícil manter o conjunto de delegados necessários para emitir um certificado. Além disso, o valor de k_i interfere no número de mensagens trocadas para se obter ou validar um certificado. Dessa forma, deve-se escolher k_i como o menor valor que garanta uma probabilidade de sucesso de conluio pequena durante as votações.

A probabilidade de sucesso de um conluio na votação com o objetivo de prejudicar um nó não-malicioso, $P(E_{sc})$, pode ser calculada com base no número de nós na rede, N, no número de nós comprometidos na rede, M, no número de delegados por nó, $m =$

$m_u + m_n$, e no valor de k. Supondo que o conluio seja feito para impedir a validação de um certificado legítimo e que $N > M > m$. Supondo ainda que $(N-1-M) \geq (m-k)$, o que significa que o número de nós não-maliciosos que podem ser delegados é pelo menos $m - k$. A probabilidade de sucesso de um conluio na votação corresponde à combinação de conjuntos de delegados com pelo menos k nós maliciosos e é dada por

$$P(E_{sc}) = \frac{C_k^M \cdot C_{m-k}^{N-1-M} + C_{k+1}^M \cdot C_{m-k-1}^{N-1-M} \cdots C_m^M \cdot C_{m-m}^{N-1-M}}{C_m^{N-1}}. \quad (1)$$

O gráfico correspondente à Equação 1 está representado na Figura 3(a), onde $N = 50$ e $m = 7$. Observa-se que para $k = 7$, mesmo que metade da rede seja composta por nós maliciosos dispostos a enviar atestados falsos nas votações para prejudicar nós não-maliciosos, a probabilidade de sucesso do conluio é de $0,005$. Assim, sistemas robustos são viáveis com um valor adequado de k. Por outro lado, o valor do número total de delegados para cada nó (m) também influencia esse resultado, pois, com o aumento de m, a probabilidade de sucesso de conluio aumenta, como pode se observar na Figura 3(b), onde $N = 50$ e $m = 14$. De fato, a probabilidade de existirem pelo menos k nós maliciosos em um conjunto de delegados aumenta se o conjunto de delegados também aumentar. Dessa forma, é preciso haver um equilíbrio entre m e k para que o AMORA permaneça robusto durante as votações mesmo com muitos nós maliciosos na rede.



(a) Para 7 delegados por nó (m=7).

(b) Para 14 delegados por nó (m=14).

Figura 3. Probabilidade de sucesso de um conluio na votação para prejudicar um nó não-malicioso em função do número de nós maliciosos M e do limiar de atestados k, para uma rede com N=50 nós.

3.2. Carga de Armazenamento para Autenticação e Monitoração dos Nós

Os parâmetros do AMORA devem ser escolhidos de forma a obter uma robustez ao conluio na votação e a não sobrecarregar os nós. Evita-se a sobrecarga de dados de autenticação e monitoramento, porque muitos dispositivos sem-fio possuem restrições de armazenamento. Nos sistemas baseados em cadeia de certificado, cada nó tem uma alta sobrecarga de dados por necessitar guardar repositórios de certificados para conseguir encontrar cadeias de certificado em comum. Nas autoridades certificadoras com criptografia de limiar, se o nó pertence a um dos n nós escolhidos para representar a autoridade certificadora, sua carga de armazenamento será dada por $C_l = N \cdot C_a$, onde N é o número

de nós na rede e C_a é o tamanho de cada registro contendo os dados para autenticação de cada nó. No AMORA, cada nó monitora aproximadamente $N_m = \frac{m \cdot N}{N} = m$ nós, onde m é o número de delegados por nó, o que significa que a carga de armazenamento de cada nó é de $C_d = m \cdot C_a$. Uma vez que $C_l >> C_d$, pode-se afirmar que no sistema proposto opta-se por distribuir a carga de armazenamento entre todos os nós, ao invés de concentrá-la em um pequeno grupo de nós, pois não são feitas premissas sobre a capacidade de armazenamento de nenhum nó da rede.

Na monitoração e na confiança, o AMORA apresenta uma grande vantagem com relação aos sistemas da literatura, nos quais cada nó é responsável por computar a confiança de todos os nós. Assim, nesses sistemas, cada nó guarda dados relativos a um total de N nós, enquanto no sistema proposto, cada nó guarda dados relativos apenas aos m nós monitorados. Essa redução de carga, já que $m << N$, se deve a distribuição da responsabilidade de monitoramento de forma aleatória entre os delegados, reduzindo a carga de armazenamento sem diminuir a segurança.

3.3. Formação de Partições

No AMORA, é interessante que nas partições sempre existam delegados de usuário de todos os usuários, pois, caso os delegados de usuário de certo usuário não estejam presentes, nenhum filho deste usuário poderá se unir àquela partição. O valor de m_u influencia na probabilidade de que, após uma partição, os nós permaneçam com delegados ativos nas duas partições. Supondo que o número de nós na partição formada seja P, o número total de nós na rede seja N e que $N \geq m_u + 1$, pode-se afirmar que a probabilidade da partição não possuir delegados de usuário de um determinado nó que não está na partição ($P(E_{p_u})$) é dada por

$$P(E_{p_u}) = \begin{cases} \frac{C_P^{(N-m_u-1)}}{C_P^N} = \frac{(N-m_u-1)!(N-P)!}{(N-m_u-P-1)!(N)!}, se\ N \geq (P+m_u+1) \\ 0, se\ N < (P+m_u+1) \end{cases} . \quad (2)$$

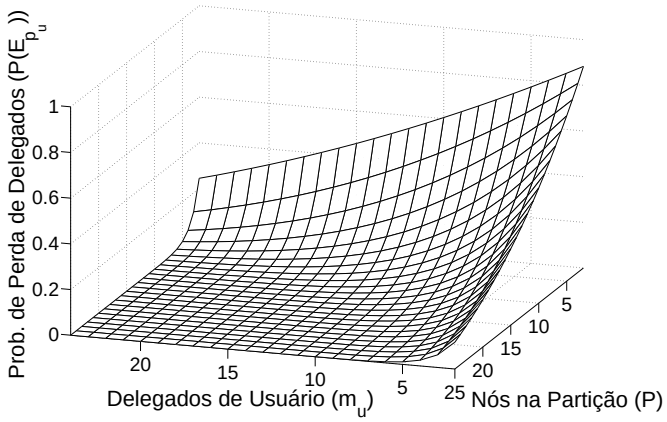


Figura 4. Probabilidade de perda de delegados de usuário após formação de partição em função do número de delegados de usuário e do número de nós na partição, para N=50.

A Figura 4 mostra a probabilidade de uma partição não possuir delegados de usuário de um determinado nó que não está na partição em função da relação entre o

número de nós na partição P e o número de delegados de usuário m_u, supondo que o número de nós na rede é $N = 50$. O que se observa, é que para valores maiores de m_u, essa probabilidade diminui. A partir desse resultado, pode-se concluir que, como é desejável que os delegados do usuário estejam presentes sempre para controlar o ingresso dos nós filhos, o m_u deve ser grande. Por outro lado, como os delegados de nó podem ser perdidos com a formação de partições sem grandes prejuízos para a rede, o m_n deve ser pequeno, evitando a sobrecarga de armazenamento e dificultando conluios.

3.4. Cadeia de Delegação

Nas propostas baseadas em cadeias de certificados para autenticação em redes ad hoc, um nó precisa verificar todos os saltos da cadeia para determinar se o nó é confiável. No AMORA, cada delegado verifica apenas a autorização enviada pelo usuário pai para emitir um certificado, pois se supõe que, se o usuário pai já possui um certificado válido, ele já conseguiu provar anteriormente que seu pai também é parte da cadeia. Esse tipo de relação é importante para que o ingresso de novos nós não seja impedido quando todos os antecessores na cadeia não estiverem presentes na rede. Uma vez que a verificação não é realizada até a raiz da cadeia de certificação, a probabilidade de falsificar um certificado é avaliada de acordo com a probabilidade de um nó forjar todos os seus delegados. Assim, falsificar um certificado corresponde a encontrar um par de chaves correspondente ao IP de cada delegado, gerar as assinaturas dos atestados dos delegados e garantir que, durante a consulta a lista de certificados revogados para validação do certificado falso, nenhum dos delegados reais utilizados irá responder.

Supondo que o atacante consegue gerar as chaves correspondentes aos delegados, ainda assim, ele não conseguiria validar um certificado. Para o ataque ser funcional, é preciso que todos os delegados estejam presentes no filtro de endereços, que mostra todos os nós ativos na rede, mas estando, de fato, ausentes da rede. Assim, a segurança da cadeia do AMORA depende não apenas a capacidade de gerar os pares de chaves assimétricas relativas aos k delegados, mas, também, de gerar uma identidade que tenha pelo menos k delegados ausentes com ausência não identificada no filtro de endereço. Portanto, calculou-se a probabilidade de uma ausência não ser detectada. A maior chance de ter todos os delegados ausentes com a ausência não-detectada é durante a formação de uma partição. Quando as partições se formam, o filtro de endereço deve ser atualizado e existe uma probabilidade de uma ausência não ser detectada ($P(E_a)$), que é dada por $P(E_a) = P(E_p) \cdot P(E_{t_u}) \cdot P(E_{t_n}) \cdot P(E_m)$, onde $P(E_p)$ é a probabilidade de o nó ficar na outra partição, $P(E_{t_u})$ corresponde à probabilidade de o nó não ter delegados de usuário após uma formação de partição, $P(E_{t_n})$ corresponde à probabilidade de o nó não ter delegados de nó após uma formação de partição e $P(E_m)$ representa a probabilidade de o nó não estar monitorando nenhum nó na partição. A probabilidade de o nó ficar na outra partição é dada por $P(E_p) = 1 - \left(\frac{P}{N}\right)$, onde P é o número de nós na partição e N é o número de nós na rede. As duas parcelas seguintes da equação são dadas por

$$P(E_{t_i}) = \begin{cases} \frac{C_P^{(N-m_i-1)}}{C_P^{N-1}} = \frac{\prod_{b=1+P}^{m_i+P}(N-b)}{\prod_{a=1}^{m_i}(N-a)}, se\ N \geq (P+m_i) \\ 0, se\ N < (P+m_i) \end{cases}, \quad (3)$$

onde $i \in \{u, n\}$ e m_i é o número de delegados do tipo i. Por fim, $P(E_m)$, que é a probabilidade de o nó não estar monitorando nenhum nó na partição, é composta por duas

parcelas, sendo elas a probabilidade de nenhum nó que estava sendo monitorado ficar na partição analisada ($P(E_{tp})$) e a probabilidade de que após a formação da partição o nó não seja selecionado por nenhum outro como delegado ($P(E_{ts})$). Se antes da formação da partição o nó monitorasse m nós, o que corresponde à média de nós monitorados na rede, dada por $\frac{m \cdot N}{N} = m$, pode-se afirmar que

$$P(E_{tp}) = \begin{cases} \frac{C_P^{(N-m_u-1)} \cdot C_P^{(N-m_n-1)}}{C_P^{N-1} \cdot C_P^{N-1}} = \frac{\prod_{b=1+P}^{m_u+P}(N-b) \cdot \prod_{b=1+P}^{m_n+P}(P-b)}{\prod_{a=1}^{m_u}(N-a) \cdot \prod_{a=1}^{m_n}(N-a)}, se\ (N-m) \geq P \\ 0, se\ (N-m) < P \end{cases}, \quad (4)$$

onde P é o número de nós na partição e N é o número de nós na rede. Supondo que $P(E_s)$ é a probabilidade do nó A ser selecionado pelo nó B como delegado, dado que A está no filtro de endereços, mas, de fato, está ausente da partição e B está presente na partição. A probabilidade de um nó ausente que está presente no filtro de endereços não ser escolhido como delegado do tipo i, $P(E_{ts_i})$, é dada por

$$P(E_{ts_i}) = \begin{cases} (1 - P(E_{s_i}))^P = (1 - \frac{C_{m_i-1}^{P-1}}{C_{m_i}^P})^P = \left(1 - \frac{m_i}{P}\right)^P, se\ P \geq (m_i + 1) \\ 0, se\ P < (m_i + 1) \end{cases}, \quad (5)$$

onde $i \in \{u, n\}$ e $P(E_{ts}) = P(E_{ts_u}) \cdot P(E_{ts_n})$. Supondo que $m_u = 5$, $m_n = 3$, $N = 50$ e $P = N/7 \approx 7$, a probabilidade de uma ausência não ser detectada é da ordem de 10^{-8}, o que é um valor que pode ser considerado desprezível. Dessa forma, um nó externo não consegue entrar na rede através da falsificação de um certificado.

4. Conclusões

As redes ad hoc seguras requerem um controle de acesso distribuído, com as funções de autorização de ingresso, autenticação, monitoração e exclusão de nós maliciosos. Os sistemas de autenticação baseados em criptografia de limiar não atendem a todas as características da rede, pois contam com a presença de um administrador que cadastra os usuários e configura o serviço na rede. Os sistemas baseados em cadeias de certificados mostram uma nova perspectiva de uma rede totalmente auto-organizável. Essa estratégia, no entanto, é pouco robusta por não ser capaz de impedir a entrada de usuários maliciosos na rede, já que não existe nenhum sistema que restrinja o ingresso de usuários com base em relações pré-estabelecidas de segurança.

O sistema de controle de acesso proposto introduz uma nova estratégia, permitindo que o administrador passe a ser uma entidade distribuída. Além disso, o sistema impede a entrada de usuários maliciosos por meio do uso de autorizações e do sistema de monitoração. A utilização de nós delegados cria um sistema de certificação robusto e flexível, que torna desnecessário percorrer toda a cadeia de delegação para emitir e validar certificados. Devido às características apresentadas e a análise realizada, é possível afirmar que o sistema proposto é robusto, apresenta alta disponibilidade e também é auto-organizável, dependendo apenas do estabelecimento da cadeia de delegação entre os usuários. Foi mostrado também que o AMORA apresenta baixa sobrecarga de armazenamento e é robusto mesmo quando a rede já possui mais do que k nós maliciosos. Portanto, o sistema proposto se adéqua às características das redes ad hoc e é uma alternativa viável para as aplicações que exigem segurança.

Referências

Buttyan, L. e Hubaux, J.-P. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications*, 8(5):579–592.

Campista, M. E. M., Moraes, I. M., Esposito, P., Amodei Jr., A., Costa, L. H. M. K. e Duarte, O. C. M. B. (2007). The ad hoc return channel: a low-cost solution for Brazilian interactive digital TV. *IEEE Communications Magazine*, 45(1):136–143.

Capkun, S., Buttyan, L. e Hubaux, J.-P. (2003). Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 2(1):25–64.

Elien, J.-E. (1998). Certificate discovery using SPKI/SDSI 2.0 certificates. Master's thesis, S. B. Massachusetts Institute of Technology.

Fernandes, N. C. e Duarte, O. C. M. B. (2008). Autoconfiguração de endereços baseada em filtros de bloom para redes ad hoc. Em *XXVI Simpósio Brasileiro de Redes de Computadores (SBRC'08)*, páginas 273–286.

Fernandes, N. C., Moreira, M. D. D., Velloso, P. B., Costa, L. H. M. K. e Duarte, O. C. M. B. (2006). Ataques e mecanismos de segurança em redes ad hoc. Em *Minicursos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'2006)*, páginas 49–102.

Hubaux, J.-P., Buttyán, L. e Capkun, S. (2001). The quest for security in mobile ad hoc networks. Em *2nd ACM international symposium on Mobile ad hoc networking & computing (MobiHoc '01)*, páginas 146–155. ACM.

Merwe, J. V. D., Dawoud, D. e McDonald, S. (2007). A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Computing Surveys*, 39(1).

Pereira, F. C., da Silva Fraga, J., Notoya, A. E. e Custódio, R. F. (2007). Autoridade certificadora dinâmica para redes ad hoc móveis. Em *Anais do 25o. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, páginas 191–204.

Tamassia, R., Yao, D. e Winsborough, W. H. (2004). Role-based cascaded delegation. Em *9th ACM symposium on Access control models and technologies (SACMAT'04)*, páginas 146–155. ACM.

Velloso, P. B., Laufer, R. P., Duarte, O. C. M. B. e Pujolle, G. (2006). HIT: A human-inspired trust model. *8th IFIP IEEE International Conference on Mobile and Wireless Communication Networks (MWCN'2006)*, páginas 35–46.

Xu, M., Zhang, H., Du, R. e Zhan, J. (2007). A trust chain build scheme for enhancing wireless network security. Em *International Conference on Wireless Communications, Networking and Mobile Computing (WiCom 2007)*, páginas 2314 – 2317. IEEE.

Yi, S. e Kravets, R. (2003). MOCA: mobile certificate authority for wireless ad hoc networks. Em *2nd Annual PKI Research Workshop (PKI 2003)*.

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