Um Novo Modelo para Confiança em Redes Ad Hoc *

Pedro B. Velloso[1] , Rafael P. Laufer[2] , Otto Carlos M. B. Duarte[3] , Guy Pujolle[1]

[1]Laboratoire d'Informatique de Paris 6 (LIP6)
Université Pierre et Marie Curie - Paris VI, Paris, France

[2]Computer Science Department
University of California, Los Angeles

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

Resumo. *Este trabalho propõe um novo modelo para a atribuição de confiança em redes ad hoc, inspirada no conceito humano de confiança. Cada nó da rede atribui um grau de confiança para os seus vizinhos. Para esta atribuição, o nó considera tanto a recomendação de outros vizinhos como a sua própria experiência. A recomendação de cada nó vizinho é calculada considerando não apenas o seu grau de confiança, mas também a sua precisão e a maturidade da relação. Um protocolo de troca de recomendação, denominado REP (Recommendation Exchange Protocol) é proposto com objetivo de viabilizar a troca de recomendações entre os nós vizinhos. O modelo proposto é analisado, através de simulações, mostrando sua eficácia e sobretudo como os principais parâmetros podem ser ajustados de acordo com as características da rede.*

Abstract. *This paper proposes a new approach to assign trust in ad hoc networks. Our system is inspired on the human concept of trust. The trust level considers the recommendation of trustworthy neighbors and their own experience. For the recommendation computation, we take into account not only the trust level, but also its accuracy and the relationship maturity. We also propose the Recommendation Exchange Protocol (REP), which aims at minimizing the number of exchanged messages. We analyze through simulations the main characteristics of the proposed model. The results show its eficacy and how parameters can be tuned to different network conditions.*

1. Introdução

Dentro da perspectiva das redes autônomas [1], um nó deve ter a capacidade de aprender a escolher o melhor comportamento a ser adotado de acordo com os seus objetivos e as condições da rede. Para isso, é necessário que o nó inicialmente aprenda sobre a sua rede e posteriormente seja capaz de tomar as suas próprias decisões . O processo de aprendizado presume a coleta de informações provindas de experiências passadas ou de nós vizinhos. Sempre que a informação coletada vier de um nó vizinho, um sistema de confiança se torna indispensável para diferenciar informações valiosas de informações errôneas. Assim, pode-se dizer que o primeiro passo em direção a uma rede colaborativa

*Este trabalho foi realizado com recursos do CNPq.

de nós autodidatas passa pela construção de um sistema de atribuição e gerenciamento de confiança. A necessidade de confiança cresce com o aumento da complexidade dos sistemas, devido ao seu maior grau de interdependência. Além disso, a informação de confiança sobre os nós vizinhos pode permitir a identificação e o isolamento de nós maliciosos.

A confiança é um conceito abrangente que engloba diversas definições. McKnight e Chervany [2] apresentam uma classificação conceitual da confiança. Eles argumentam que existem diferentes tipos de confiança e, por isso, todos os trabalhos deveriam especificar qual tipo está sendo abordado. Neste trabalho, serão abordados dois tipos de confiança. O primeiro está relacionado com o encaminhamento de pacotes, que permitirá aos nós decidir qual vizinho tem maior probabilidade de entregar um pacote corretamente, dado um determinado nó destino. O segundo é relacionado com a veracidade das informações recebidas de terceiros, que irá viabilizar a existência de um sistema de aprendizado eficiente e consistente.

As redes ad hoc dependem da colaboração dos nós para o seu bom funcionamento. No entanto, o comportamento de cada nó é dinâmico e depende da sua intenção, dos seus objetivos e das suas limitações. Desta forma, cada nó deve decidir o que é melhor para si mesmo, mas dentro de uma colaboração mínima, como em uma sociedade. Assim, os nós podem apresentar diferentes comportamentos, e uma determinada decisão pode não ser necessariamente a melhor para todos os nós. Por isso, uma ingênua dependência pode provocar baixa eficiência, alto consumo de energia e até mesmo ataques de nós maliciosos.

Existem alguns trabalhos que visam incentivar a colaboração dos nós em redes ad hoc através de sistemas de crédito [3–5]. Apesar do estímulo à cooperação ser um ponto importante, não é suficiente para proporcionar um ambiente de auto-aprendizagem, autoconfiguração e auto-adaptação.

O objetivo deste trabalho é propor um novo modelo de confiança para redes sem fio ad hoc. O modelo proposto visa simular as relações humanas de confiança e será baseado no aprendizado dos nós. As redes sem fio ad hoc se caracterizam pela ausência de uma infraestrutura de rede. Deste modo, os nós se comunicam diretamente sem a existência de um ponto de acesso centralizador que possa atribuir e gerenciar o grau de confiança dos demais nós da rede. A abordagem deste trabalho é diferente daquela proposta em outros trabalhos preocupados apenas com aspectos convencionais de segurança da rede, como a detecção de nós maliciosos, entre outros. O foco deste trabalho é proporcionar aos nós de uma rede ad hoc uma maneira de manter uma opinião sobre seus vizinhos, que servirá de base para a interação e a tomada de decisões entre eles. O sistema proposto é completamente distribuído e baseia-se na confiança que diferentes nós da rede possuem sobre um determinado nó sendo avaliado. O processo de avaliação do grau de confiança, na abordagem adotada, considera não somente o grau de confiança entre dois nós adjacentes, mas a precisão e a maturidade do seu relacionamento. A fim de viabilizar a troca de recomendações, também foi proposto o protocolo REP (*Recommendation Exchange Protocol*), que simplifica a troca de informações de confiança na rede.

Este trabalho está organizado da seguinte forma. Os principais trabalhos relacionados são apresentados na Seção 2. A Seção 3 apresentada o sistema de confiança proposto. Detalhes referentes às simulações e à análise dos resultados são apresentados na Seção 4. Por fim, na Seção 5 são apresentadas as conclusões e os trabalhos futuros.

2. Trabalhos relacionados

Existem diversos trabalhos [6–13] que tratam da questão da confiança em redes ad hoc. No entanto, a maioria deles está focada apenas nos problemas de roteamento e de identificação de nós maliciosos.

Liu *et al.* [6] propõem um modelo de confiança para redes ad hoc baseado na distribuição, aos nós interessados, de relatórios sobre ameaças . O objetivo é construir um roteamento no qual o grau de confiança é utilizado como uma métrica adicional. Eles apresentam uma abordagem diferente para o cálculo do grau de confiança. No entanto, é assumida uma cooperação entre os nós que nem sempre pode ser considerada como válida. Outro problema é considerar que todos os nós são capazes de detectar comportamentos maliciosos a partir de sistemas de detecção de intrusão. Esta premissa se baseia na escuta promíscua do meio, o que provoca um significativo aumento no consumo de energia que pode ser inaceitável para uma rede ad hoc.

Yan *et al.* [7] propõem uma solução para a insegurança em redes ad hoc, baseada em um modelo de confiança. É sugerida a utilização de uma função linear para o cálculo do grau de confiança de acordo com uma determinada ação. A função proposta para o cálculo da confiança considera uma lista negra de invasores, estatísticas de experiências passadas, a recomendação de outros nós, dentre outros fatores. No entanto, como estes fatores influenciaram no cálculo não é especificado. Além disso, também é apresentado um protocolo de roteamento que utiliza o esquema de confiança proposto, e como este novo protocolo pode minimizar diversos tipos de ataques a que um protocolo de roteamento está sujeito [14]. Novamente, o foco principal são os ataques ao protocolo de roteamento.

Pirzada e McDonald [8] propõem um modelo de confiança a fim de estimar a confiabilidade das rotas. Assim, esta pode ser uma métrica adicional no cálculo das rotas. Embora não garanta 100% de segurança, o modelo proposto permite aos nós optar pela rota mais confiável. Uma extensão ao protocolo DSR ()é proposta para avaliar a eficácia do esquema de confiança proposto. No entanto, o modelo se restringe ao protocolo DSR, e depende integralmente do uso do modo promíscuo, ignorando as limitações de energia dos nós móveis. Outro problema é a grande quantidade de informação que deve ser armazenada, em cada nó da rede.

Buchegger e Le Boudec [11] investigaram o compromisso entre robustez e eficiência na utilização de sistemas de reputação em redes móveis ad hoc. Também é proposto um mecanismo baseado em estatística Bayesiana para filtrar nós difamadores. São considerados para computar a reputação de um determinado nó, tanto os dados obtidos através de observações como dados enviados por outros nós. Eles mostram que levar em consideração as recomendações de outros nós pode acelerar o processo de descoberta de nós maliciosos.

Theodorakopoulos e Baras [12] analisaram a questão da inferência de grau de confiança como uma generalização do problema de menor caminho em um grafo orientado, onde as arestas correspondem a opinião que um vértice possui sobre o outro. Eles consideram que os nós formam sua opinião baseada estritamente em observações locais. A opinião de cada nó inclui o grau de confiança mais um valor que representa a precisão do grau de confiança. O objetivo é capacitar os nós a construir indiretamente relações de confiança baseada apenas em interações locais.

Virendra *et al.* [13] apresentam uma arquitetura baseada na confiança que permite aos nós da rede tomarem decisões referentes ao estabelecimento de chaves e a formação de grupos com outros nós. O esquema de confiança proposto também se baseia numa avaliação feita pelo próprio nó e na recomendação de outros nós. Entretanto, o procedi-

mento utilizado na avaliação do nó é baseado na monitoração dos nós e em um mecanismo de pergunta e resposta. Assim, o nó avaliador envia uma pergunta ao nó avaliado e depois compara a resposta com as informações obtidas durante a fase de monitoração.

3. Modelo de confiança proposto

A idéia básica consiste em construir um sistema de confiança que permita aos nós de uma rede aprender com as informações trocadas com seus vizinhos. Desta maneira, o principal objetivo é obter nós autoconfiguráveis, auto adaptáveis e auto-otimizáveis. Assim, as estações serão capazes de tomar suas próprias decisões. O principal objetivo não é proporcionar um ambiente confiável, mas sim capacitar os nós a reconhecer o ambiente ao qual pertencem. Isto é alcançado através da avaliação da confiabilidade de seus vizinhos. A informação de confiança será utilizada não apenas para o aprendizado e tomada de decisões, mas também poderá ser utilizada para a detecção e o isolamento de nós maliciosos.

O modelo proposto pode ser divido em duas camadas distintas, como mostra a Figura 1. A camada de Aprendizado é responsável por coletar e converter informações em conhecimento. A camada de Confiança define como avaliar a confiança de um nó vizinho de acordo com o conhecimento adquirido pela camada de aprendizado. Ambas as camadas podem interagir com todas as outras camadas e, por isso, podem ser consideradas como uma otimização intercamadas (*cross-layer optimization*). Isto significa que o processo de aprendizado pode utilizar informações de todas as camadas e as informações de confiança estão disponíveis para todas as camadas. A camada de Aprendizado considera o contexto do nó, que inclui o estado atual, as condições da rede, o lugar, a mobilidade e as ações de nós vizinhos para ajustar os parâmetros do modelo de confiança. Este artigo descreve a camada de Confiança. A camada de Aprendizado será alvo de estudo mais detalhado futuramente.

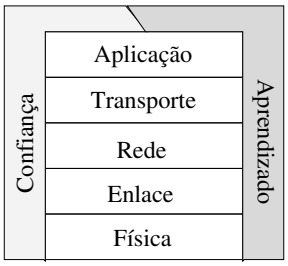


Figura 1: O modelo de confiança.

Primeiramente, é definido o grau de satisfação de um determinado nó como o quão perto ele está do seu objetivo. O modelo parte do princípio que a ação de um nó é baseada apenas no seu comportamento e tem sempre como objetivo maximizar o seu grau de satisfação. Porém, cada ação terá um efeito sobre os nós vizinhos.

O grau de confiança é baseado nas experiências anteriores e nas recomendações de nós vizinhos. As experiências anteriores resultam do julgamento das ações dos outros nós, realizado pela camada de Aprendizado. As ações podem produzir três tipos de veredictos. Uma ação pode produzir um impacto positivo, negativo, ou nenhum impacto nos nós adjacentes. Os dois primeiros tipos geram uma reação que poderá disparar uma atualização do grau de confiança e eventualmente provocar uma mudança de comportamento. A capacidade de percepção das ações dos nós está diretamente relacionada com a eficiência da camada de aprendizado. Por exemplo, nós com sérias restrições de con-

sumo de energia podem apresentar uma baixa eficiência por não poderem operar em modo promíscuo.

A recomendação dos nós vizinhos pode ser considerada no cálculo do grau de confiança. Para isto, foi introduzido o conceito de maturidade de relacionamento que reflete a duração do relacionamento de confiança entre dois nós. Este conceito permite aos nós atribuir maior importância a recomendações baseadas em relacionamentos de mais longa duração. Assim, para considerar as recomendações de outros nós para manter a tabela de confiança atualizada, os nós devem utilizar o protocolo de troca de recomendações (*Recomendation Exchange Protocol* - REP).

Cada nó deve manter uma tabela de confiança principal que conterá o grau de confiança de todos seus vizinhos. São considerados vizinhos apenas os nós que podem se comunicar diretamente. Além disso, um nó pode armazenar a opinião dos seus vizinhos sobre um determinado nó, sempre que possível. Assim a tabela principal é uma matriz de ordem d^2, com possíveis otimizações, onde d representa o número de nós. Cada entrada na tabela de confiança é associada a uma data de validade. Quando a data de validade de uma dada entrada expira, o nó deve removê-la juntamente com todas as recomendações associadas a esta entrada. No modelo proposto, os nós podem manter uma tabela de confiança auxiliar, que não é obrigatória, onde serão armazenadas a precisão do grau de confiança e a maturidade do relacionamento. O objetivo da tabela auxiliar é fornecer aos nós informações que viabilizem o aprimoramento do processo de avaliação do grau de confiança. No entanto, estações com restrições de armazenamento ou de energia podem decidir por não implementar o sistema de confiança na sua integralidade. Desta maneira, são definidos três modos de operação. Nós com baixa capacidade de armazenamento/energia operam no modo simples, no qual apenas a tabela de confiança principal é implementada e o protocolo REP é opcional. Nós com capacidade média operam no modo intermediário que mantém a recomendação dos nós vizinhos. No modo avançado, as estações implementam todos os componentes do sistema avaliação de confiança, ou seja, a tabela de confiança principal, auxiliar e o protocolo REP.

Cada nó irá computar um grau de confiança para cada vizinho, o qual será atualizado sempre que necessário. Os nós são inteiramente responsáveis pelos próprios processos de avaliação do grau de confiança. Assim, o processo de avaliação de confiança é dividido em duas fases distintas. Primeiramente, uma fase inicial, que ocorre quando dois vizinhos se conhecem e irão atribuir um grau de confiança pela primeira vez. A segunda fase assume que os nós já se conhecem e compreende a manutenção do grau de confiança sempre atualizado. O grau de confiança é uma variável continua limitada no intervalo $[0, 1]$, onde o valor 1 representa o grau mais confiável.

3.1. Fase inicial

Sempre que um nó encontra um novo vizinho, um grau de confiança lhe deve ser atribuído. O primeiro grau atribuído dependerá das condições da rede, da mobilidade, do lugar e do estado atual do nó que irá atribuir. Pode-se classificar a estratégia de atribuição do primeiro grau de confiança como prudente ou amigável/ingênua. Na estratégia prudente o nó não confia em estranhos, considerando todo novo vizinho como uma ameaça para a rede. Assim, um baixo grau de confiança será atribuído. Adotar a estratégia amigável/ingênua significa que, *a priori*, todo nó é confiável até que se prove o contrário. Neste caso, será atribuído um alto grau de confiança aos novos vizinhos. Quando um nó adota esta estratégia amigável/ingênua e se baseia no conhecimento adquirido anteriormente, é considerada como amigável, caso contrário, é considerada ingênua, pois a estratégia foi escolhida por falta de opção. Entre duas principais estratégias anteriores, existe ainda uma terceira, a estratégia moderada, na qual os nós atribuem um grau de

confiança intermediário aos novos vizinhos.

Diferentes situações exigem estratégias distintas. Por exemplo, caso um determinado nó já possua um considerável número de vizinhos confiáveis, uma alternativa viável seria tornar-se mais seletivo adotando uma estratégia prudente. Neste caso, o nó em questão não estará precisando desesperadamente de um nó confiável, pois a adição de um nó confiável talvez não represente um aumento significativo no seu grau de satisfação. Por outro lado, em uma rede onde a topologia muda constantemente e vizinhos são efêmeros, um nó pode adotar uma estratégia ingênua. Em um ambiente hostil um nó pode seguir uma estratégia prudente, enquanto que em um ambiente cordial e conhecido, um nó pode adotar uma estratégia amigável.

A fase inicial pode também considerar a recomendação de outros nós ponderada pelos seus respectivos graus de confiança. Para calcular o valor do primeiro grau de confiança do nó a sobre o nó b é proposta a seguinte expressão.

$$T_a(b) = (\alpha - 1) \cdot F_a + \alpha \cdot C_a(b), \tag{1}$$

onde F_a (*First Trust Value*) representa o valor obtido por a segundo a estratégia adotada, $C_a(b)$ é a contribuição de todos os nós $n \in K_a$ sobre o nó b. K_n define o grupo de nós do qual as recomendações serão consideradas no cálculo da contribuição de outros nós. Assim, K_n é um subgrupo dos vizinhos de n (N_a) que inclui todos os nós que satisfaçam um determinada condição. Dentre as possíveis condições para seleção de K_n, duas são consideradas neste trabalho:

$$K_n = \{\forall i \in N_a | T_a(i) \geq T_{th}\}. \tag{2}$$

onde T_{th} representa o valor de confiança limiar a partir do qual um vizinho será considerado nas contribuições. Uma outra opção seria selecionar os r primeiros nós pertencentes à N_a de acordo com o grau de confiança. A seleção de K_n é uma decisão importante para o processo de avaliação da confiança, que depende de muitos parâmetros. Algumas aspectos importantes na seleção de K_n bem como o conceito de "melhor amigo" são apresentados na Seção 3.4.

Escolher a melhor estratégia para obter o F_a não é uma tarefa simples. O valor do F_a deve levar em consideração principalmente o nível de mobilidade, o grau de satisfação atual e o número de vizinhos confiáveis. Sendo que conhecer o número de vizinhos confiáveis implica definir previamente um limiar de confiabilidade (R_{th}) a partir do qual um determinado nó pode ser considerado confiável. Como a escolha da melhor estratégia envolve vários parâmetros, preferiu-se atribuir esta tarefa à camada de Aprendizado.

3.2. O Cálculo da contribuição

O processo de avaliação do grau de confiança dos nós vizinhos pode levar em conta a recomendação de outros nós. A contribuição dos vizinhos é o conjunto das recomendações de todos os nós vizinhos. $C_a(b)$ representa a contribuição de todos o nós $i \in K_a$ sobre o nó b ponderada pelo grau de de confiança do nó a ($T_a(i)$) sobre o nó i, como mostra a Equação 3.

$$C_a(b) = \frac{\sum_{i \in K_a} T_a(i) M_i(b) X_i(b)}{\sum_{j \in K_a} T_a(j) M_j(b)}. \tag{3}$$

A relevância da recomendação de cada nó ($T_i(b)$) é fortemente relacionada à seleção de K_a. Quanto mais confiável for K_a mais útil será a recomendação dos nós vizinhos. A contribuição inclui não somente o grau de confiança ($T_a(b)$), como também a precisão

desta medida e a maturidade da relação, que representa há quanto tempo os nós se conhecem. A maturidade do relacionamento ($M_i(b)$) é representada em segundos por uma variável contínua e X é uma variável aleatória de distribuição normal que pode ser expressa por

$$X_i(b) = N(T_i(b), \sigma_i(b)) \tag{4}$$

onde σ representa a precisão e é definida como o desvião padrão, similar ao trabalho de Theodorakopoulos e Baras [12].

Cada valor na tabela de grau de confiança do nó i ($T_i(b)$) está associado a um valor de desvio padrão ($\sigma_i(b)$), que se refere à variação do valor do grau de confiança que o nó i observou. Assim, após uma atualização do grau de confiança do nó i sobre o nó b, o nó i deve atualizar o valor de $\sigma_i(b)$, que é definido como:

$$\sigma_i(b) = \sqrt{\frac{\sum_{j=1}^{k} (\overline{S}_k - S_j)^2}{k-1}}, \tag{5}$$

onde S_k representa o conjunto dos k últimas amostras de grau de confiança sobre o nó b, dado $k \in N \mid 2 \leq k \leq 10$. $\overline{S}_k$ é o valor médio. O parâmetro σ expressa a confiabilidade da medida do grau de confiança. Um valor grande de σ pode demonstrar a dificuldade do nó de avaliar o grau de confiança ou a instabilidade do comportamento do nó que está sendo avaliado.

A recomendação do nó i sobre o nó b é ponderada pela maturidade $M_i(b)$. Isto significa que quanto maior for o tempo que os nós se conhecem, maior será a relevância da sua opinião para o valor da contribuição final de todos os nós vizinhos. Nós maliciosos podem tentar falsificar graus de confiança por diversas razões. Por exemplo, um nó pode querer difamar um outro vizinho, ou pode querer convencer os outros vizinhos que um determinado nó malicioso é, na verdade, um nó de boa índole, ou ainda apenas querer confundir os outros nós. Assim, bastaria colocar um valor alto para a maturidade do relacionamento de um grau de confiança forjado, para que esta recomendação tivesse um grande peso no processo de atualização dos nós vizinhos. Para minimizar este efeito, cada nó deve definir um limiar para o valor de maturidade da relação (M_{max}) de tal forma que a maturidade pode ser expressa por:

$$M_i(b) = \begin{cases} M_i(b), & \text{if } M_i(b) < M_{max} \\ M_{max}, & \text{if } M_i(b) \geq M_{max}. \end{cases} \tag{6}$$

O valor de (M_{max}) deve ser baseado na média dos valores de maturidade de relacionamento de todos seus vizinhos.

3.3. Atualização do grau de confiança

A atualização do grau de confiança é um processo que pode ser desencadeado a qualquer momento, desde que o primeiro grau de confiança já tenha sido atribuído previamente. Este processo compreende dois passos diferentes. Primeiro, o nó deve saber quando o grau de confiança deve ser atualizado. Depois, é necessário saber como realizar o cálculo do novo grau de confiança.

O modelo proposto considera que uma atualização é sempre desencadeada por um evento, no entanto, a ocorrência de um evento não implica necessariamente a atualização do grau de confiança. A definição de um evento consiste na recepção de uma mensagem de recomendação ou na percepção de uma ação realizada por um dos vizinhos. A mensagem de recomendação contém uma ou mais recomendações de um determinado vizinho. O segundo tipo de evento, relacionado com as ações dos nós vizinhos, é mais complexo de ser avaliado e será tratado na Seção 3.5.

Desta maneira, a atualização do grau de confiança ($T_a(b)$) é definido como a soma da sua própria confiança com a contribuição dos nós vizinhos, parecido com o proposto em [13], como mostra a Equação 7.

$$T_a(b) = (1 - \alpha)Q_a(b) + \alpha C_a(b), \tag{7}$$

onde α permite escolher o fator mais relevante. $Q_a(b)$ representa a capacidade de um nó de avaliar o grau de confiança baseado nas suas próprias informações. A Equação 8 mostra como obter $Q_a(b)$, no modelo proposto.

$$Q_a(b) = \beta E_T + (1 - \beta)T_a(b), \tag{8}$$

onde E_T representa um valor de grau de confiança obtido através das ações de terceiros. O parâmetro β permite escolher o termo mais relevante. Isto significa que o parâmetro β depende de qual evento desencadeou a atualização do grau de confiança. Por exemplo, supondo que o nó a começou uma atualização sobre o nó b, desencadeada por uma recomendação do nó vizinho c, mas o nó a não notou nada de estranho no comportamento do nó b. Neste caso, o nó a pode ignorar o primeiro termo da Equação 8. Por outro lado, caso a atualização tenha sido desencadeada por uma reação, o nó a pode escolher $\alpha = \beta = 1$, ignorando a contribuição dos nós vizinhos (Equation 7) e o valor antigo para o grau de confiança sobre o nó b (Equação 8).

3.4. O Protocolo de troca de recomendações

Na seção anterior foi mostrado como os nós devem proceder para avaliar o grau de confiança de um nó vizinho, baseado nas próprias experiências e nas recomendações de outros nós. Nesta seção, é proposto um protocolo para troca de recomendações (REP - *Recommendation Exchange Protocol*).

O protocolo REP inclui três tipos de mensagens e sua implementação não é obrigatória para todos os nós, porém é fortemente recomendada. Cada nó pode escolher se usará ou não o protocolo de acordo com seus objetivos e restrições. Quando dois nós se encontram pela primeira vez, isto é, quando nós não vizinhos tornam-se vizinhos, uma mensagem de pedido de grau de confiança (*Trust Request - TREQ*) deve ser enviada em difusão. A mensagem TREQ contém apenas um identificador de nó. Antes de enviar uma TREQ, o nó deve esperar por uma determinada quantidade de tempo (*backoff*), a fim de evitar colisões e para possibilitar a agregação de vários pedidos de grau de confiança em apenas uma TREQ, caso neste período de espera surjam novos vizinhos. Por exemplo, quando o nó a e o nó b se encontram pela primeira vez, o nó a enviará uma TREQ com o identificador de nó igual a b ($TREQ_a^b$). O nó b, por sua vez, enviará uma $TREQ_b^a$. Os nós que recebem uma TREQ e possuem grau de confiança sobre o nó requisitado devem responder com uma mensagem de resposta de confiança (Trust Reply - TREP). Da mesma maneira e com os mesmos objetivos, antes de enviar um TREP o nó deve esperar por uma determinada quantidade de tempo. Uma mensagem TREP possui a recomendação do nó remetente sobre o nó cujo grau de confiança foi requisitado. Caso durante o (*backoff*) o nó receba mais de uma TREQ de nós diferentes, é possível escolher entre enviar duas mensagens em diretamente para os nós requerentes ou enviar uma mensagem em difusão. Um nó pode ainda definir um limiar para o envio da TREP baseado no grau de confiança do nó requerente a baixo do qual a mensagem não será respondida.

Após o envio de uma TREQ, o nó requerente deve esperar as respostas (TREP) de seus vizinhos por uma determinada quantidade de tempo (*timeout*). Caso o nó requerente não receba nenhuma TREP de seus vizinhos, a parcela da Equação 7 relativa à contribuição dos vizinhos deve ser ignorada, igualando o parâmetro α a 1.

Por último, a mensagem de anúncio de grau de confiança (*Trust Advertisement* - TA) é uma recomendação não solicitada. Uma mensagem TA inclui uma recomendação do nó que está anunciando sobre um de seus vizinhos. O envio de uma TA acontece sempre que uma atualização de grau de confiança gera um novo grau cuja diferença para a última TA enviada for maior que um determinado limiar ($TA_{threshold}$). Antes do envio de uma TA deve-se esperar por uma determinada quantidade de tempo, durante o qual é possível agregar TAs em uma mesma mensagem. A recepção de uma TA não implica necessariamente uma atualização do grau de confiança, mas apenas a atualização da recomendação recebida, para o caso em que o nó em questão seja também seu vizinho. Todos os tempos de espera (*backoff*) são aleatórios entre zero e um valor máximo de *backoff* previamente estabelecido.

Uma recomendação inclui o grau de confiança, sua precisão e a maturidade da relação. Para os nós que não implementam a tabela de confiança auxiliar, a recomendação inclui apenas o grau de confiança.

Uma outra possibilidade seria a eleição de b melhores amigos (*Best Friends* - BF) onde $b \leq |K_n|$. Assim, os nós poderiam enviar TREQs diretamente para seus BFs. A definição de BF é um nó que possui um grau de confiança acima de um certo limiar de BF, mas que também pode ainda considerar a maturidade da relação. O número de TREQs pode ser limitado por um limiar de TREQ a partir do qual os pedidos seriam enviados em um único TREQ em difusão. Este esquema permite aprimorar a contribuição dos vizinhos e ao mesmo tempo, diminuir o número de TREP, eliminando os TREP inúteis, ou seja, que não seriam considerados. Obviamente, o esquema depende em encontrar pelo menos um certo número m de BFs. Em algumas situações, quando as condições não são propícias, pode não ser uma tarefa fácil encontrar BFs, como por exemplo em ambientes hostis. Nestes casos, os nós não devem implementar as facilidades dos BFs.

3.5. Reações

No modelo proposto, os nós devem avaliar o efeito das ações de seus vizinhos no seu grau de satisfação. O efeito pode ser positivo, caso o grau de satisfação aumente. Se o grau de satisfação diminui, diz-se que a ação teve um efeito negativo. Por fim, caso não ocorram mudanças no grau de satisfação, a ação não fez efeito, ou fez efeito nulo. Quando a ação de um vizinho tem um efeito positivo ou negativo, o processo de atualização do grau de confiança é automaticamente iniciado. Assim o grau de confiança deste vizinho será recalculado. Existem dois problemas básicos, porém complexos, associados à avaliação das ações de terceiros. A primeira é o fato de que os objetivos de um nó devem estar muito bem definidos para se obter o grau de satisfação. Em seguida, tem-se o problema de perceber a verdadeira causa das variações do grau de satisfação, pois depende não só das ações dos nós vizinhos, mas também das condições da rede em geral. O uso de informações locais pode tornar esta tarefa ainda mais complexa. Por isso, a tarefa de reconhecer e reagir às ações dos nós é de responsabilidade da camada de Aprendizado (Figura 1).

4. Resultados

De forma a analisar o modelo de confiança proposto, foi implementado um simulador em C++. Nesta seção são apresentados os resultados obtidos a partir de simulações realizadas com este simulador. No simulador, cada nó possui um parâmetro denominado índole que varia de 0 a 1. Os nós mais confiáveis possuem índole igual a 1 enquanto que nós não-confiáveis possuem índole 0.

Os nós realizam determinadas ações durante o período de simulação. Os nós serão julgados pelos seus vizinhos a partir das ações que realiza. Estas ações simulam um pedido de rota não respondido, um pacote corretamente encaminhado, uma informação útil recebida, entre outras possibilidades. Uma ação pode ser interpretada como benéfica ou maléfica, de acordo com o evento representado. As ações são geradas segundo uma distribuição exponencial, podendo assumir o valor 1, que caracteriza uma ação benéfica, e o valor -1, que representa uma ação maléfica. O tipo de cada ação executada está diretamente relacionado com a índole do nó que a gerou. Assim, a índole de um nó representa a fração de ações benéficas realizadas por aquele nó. Isto significa que um nó com índole 0,8 realiza 8 ações benéficas em cada 10 ações realizadas.

No simulador, foi também introduzido o conceito de percepção a fim de simular a interface com a camada de Aprendizado. A percepção de um nó está diretamente relacionada com a capacidade de perceber as ações de terceiros, podendo variar de 0 a 1. Este valor representa a fração de ações que um determinado nó consegue perceber ao seu redor. Assim, um nó de percepção 0,4 consegue perceber apenas 4 ações em cada 10 realizadas por seus vizinhos.

A parcela da experiência de cada nó (Equação 8), que considera as ações dos nós vizinhos, é sempre calculada a partir das i últimas ações de cada vizinho. Por isso, para que esta parcela comece a ter efeito no grau de confiabilidade, um nó deve ter percebido no mínimo i ações de cada vizinho. Isto significa que durante o período de contato inicial em que o número de ações percebidas é menor que o valor de i, o nó utiliza apenas o valor das contribuições dos vizinhos e o valor do grau de confiança mais recente para calcular o grau de confiabilidade.

O protocolo REP foi implementado ainda sem as funcionalidades proporcionadas pelo conceito de "melhor amigo". Os parâmetros do protocolo REP foram definidos como mostra a Tabela 1.

Tabela 1: Parâmetros do protocolo REP.

parâmetro	valor
backoff	1 s
TREQ_timeout	2 s
$TA_{threshold}$	0,05

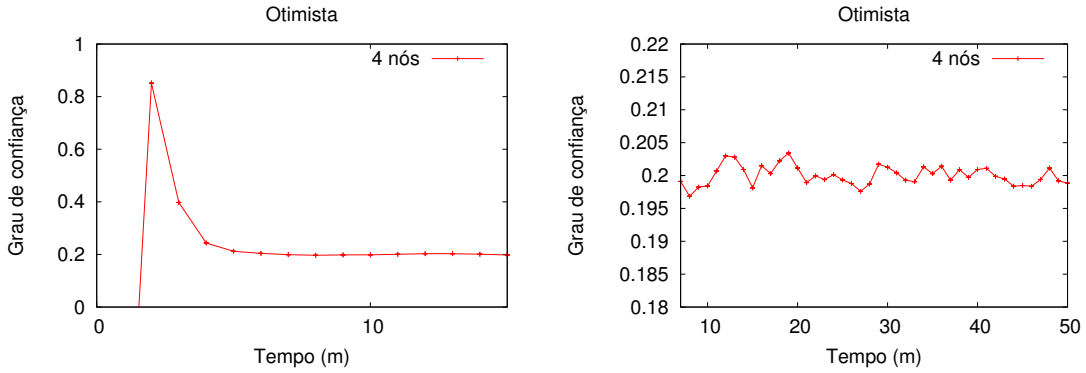
Um determinado vizinho pode possuir três estados. Um vizinho pode ser "desconhecido" quando ainda não foi identificada a sua presença. Os nós tomam conhecimento da existência de seus vizinhos apenas após a percepção de uma ação ou após o recebimento de uma mensagem. Assim que um nó identifica a presença de um novo vizinho, este passa para o estado "conhecido" no qual lhe é atribuído um grau de confiança igual a -1. Este valor foi definido apenas para diferenciar os nós que ainda não possuem um grau de confiança definido. Após a atribuição do primeiro grau de confiança, o vizinho passa para o estado "amigo".

Neste primeiro momento, foram avaliadas a influência do número de vizinhos, da estratégia adotada para a primeira atribuição de grau de confiança e da variação do parâmetro α da Equação 7 na avaliação do grau de confiança. Todos os resultados possuem um intervalo de confiança de 95% representado pelas barras de erro.

O ambiente de simulação consiste de nós com 250 m de raio de cobertura de comunicação, aleatoriamente distribuídos em uma área de 150 m $\times$ 150 m. Isto significa que se trata de uma rede ad hoc de comunicação direta, isto é, todos os nós da rede

conseguem se comunicar diretamente uns com os outros e, portanto, são todos vizinhos. Este cenário foi escolhido para melhor avaliar o efeito do número de vizinhos. Todos os nós operam no modo avançado, ou seja, implementam todo o sistema de confiança proposto neste trabalho. O tempo de simulação é de 1500 segundos. Foram definidos os valores 0,1, 0,5 e 0,9 para o FTV (*First Trust Value* da Equação 1) das estratégias de primeira atribuição de grau de confiança prudente, moderada e amigável/ingênua, respectivamente. Para efeito de simplificação, a estratégia amigável/ingênua foi chamada de estratégia otimista. Todos os nós adotam a mesma estratégia. Os valores de α e β são iguais a 0,5. O valor da percepção é de 0,5. Estes foram os valores padrões atribuídos para as simulações. Em cada configuração de simulação serão mencionados os parâmetros que foram modificados em relação ao valor padrão. Neste conjunto de simulações, o grau de confiança é igual para todos os nós.

A Figura 2 apresenta a resposta no tempo da média do grau de confiança dos vizinhos de um determinado nó sobre o próprio nó. Neste cenário especificamente, o tempo de simulação é de 3.000 segundos. Nota-se (Figura 2(a))que o grau de confiança em um determinado nó irá começar em um patamar e depois tenderá a se aproximar cada vez mais do valor correto. O valor correto, ou esperado, é a índole do nó avaliado. Após um certo tempo $t_1 \approx 5$min o valor do grau de confiança irá variar em torno do valor correto. Assim, pode-se dizer que existe um período transiente e um período estacionário. No período transiente, visto na Figura 2(a), o nó está tentando se aproximar do valor esperado. No período estacionário (Figura 2(b)), o grau de confiança permanece estável e varia muito pouco ao longo do tempo. O período estacionário pode ser aproximado por uma função senoidal com a amplitude amortecida por uma função exponencial.



(a) Período transiente (b) Período estacionário

Figura 2: Variação do grau de confiança no tempo.

Nos outros resultados, ao invés de mostrar a média do grau de confiança de um determinado nó no eixo das coordenadas, é mostrada a média do erro do grau de confiança, ou seja, a diferença entre o grau de confiança avaliado e o valor esperado (índole do nó avaliado). Esta nova informação irá mostrar quão distante o grau calculado está do grau de confiança esperado. Os gráficos começam com o valor em -1, pois neste momento não existe nenhum nó com vizinhos no estado amigo, ou seja, ainda não foi atribuído o grau de confiança a nenhum vizinho.

Na configuração utilizada na Figura 3 foi adotada uma estratégia otimista e foi variado o número de vizinhos. A índole dos nós é igual a 0,2. Este valor foi escolhido, pois permite visualizar melhor o período transiente. Pode-se perceber que à medida que o número de vizinhos aumenta, os nós conseguem chegar mais próximo do valor do grau de confiança esperado. Isto ocorre porque o aumento do número de vizinhos significa também um aumento no número de recomendações recebidas, o que implica uma maior

probabilidade de receber recomendações mais próximas da índole esperada. Além disso, é interessante observar que com menos vizinhos a variação do erro é maior após o tempo de "estabilização", pois com mais recomendações a precisão dos graus de confiança decai mais rapidamente e as variações derivadas da falta de percepção são também amenizadas. É importante ressaltar que mesmo para poucos vizinhos o erro entre o grau de confiança atingido e o grau de confiança esperado é muito pequena, sendo menor que 0,04.

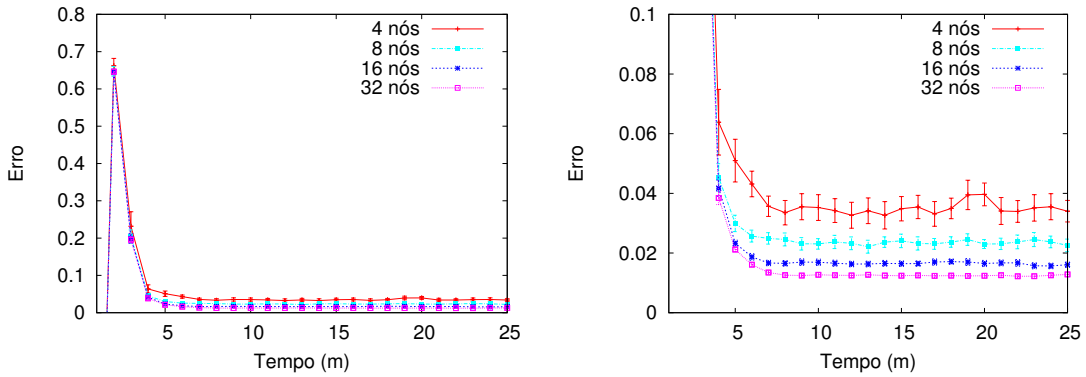


Figura 3: Influência do número de vizinhos.

A Figura 4 apresenta a influência da variação do parâmetro α na avaliação da confiança. A quantidade de nós foi mantida em 16. Diminuir o valor de α significa que a contribuição dos nós vizinhos tem um peso menor no cálculo do grau de avaliação. O primeiro detalhe importante a ser observado na Figura 4(a) é o fato de que quanto maior o valor de α, mais lenta é a convergência, ou seja, o transiente é mais longo. Tal comportamento ocorre porque a opinião global sobre um determinado nó demora a mudar. Desta forma, à medida que aumentamos a influência dos outros nós na atribuição do grau de confiança, a convergência fica mais lenta. Entretanto, todos os nós convergem para um valor mais próximo do real. A Figura 4(b) apresenta um detalhe da figura anterior para mostrar o período estacionário. Pode-se perceber que com um alpha superior a 0,5, apesar de ter uma convergência mais lenta, o grau de confiança chega mais próximo do valor esperado. Além disso, a variação do erro é menor. Isto comprova o resultado de que considerar as recomendações permite obter um grau de confiança mais acurado e mais preciso, enquanto que priorizar as experiências anteriores possibilita reduzir o transiente.

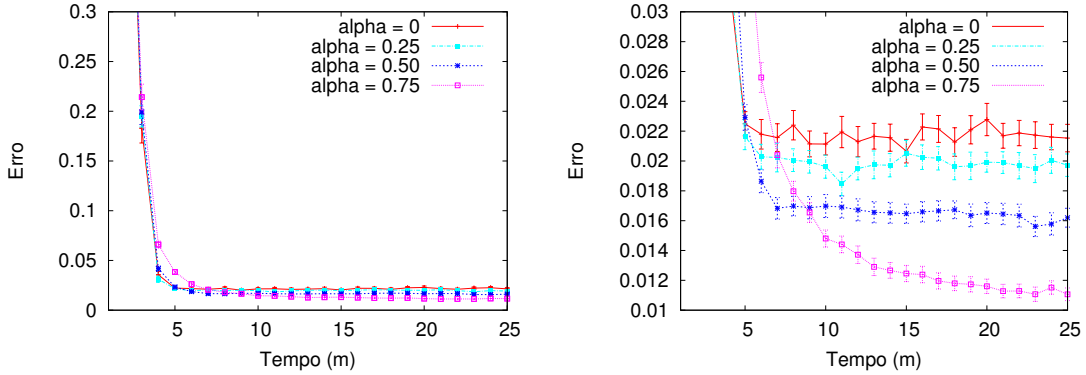


Figura 4: Variação do parâmetro $alpha$.

A Figura 5 ilustra o comportamento da avaliação do grau de confiança com a variação do grau de percepção. O grau de percepção mede a fração de ações de terceiros

que um determinado nó consegue perceber. Percebe-se que o grau de percepção está diretamente relacionado com a duração do período transiente. O aumento grau de percepção implica um decréscimo na duração do período transiente. Este resultado deve-se ao fato de existir um valor mínimo de ações que um nó deve perceber para que seja capaz de julgar o resultado das ações de um determinado vizinho. Quanto maior for este número mínimo, maior será a precisão do julgamento. No entanto, a duração do transiente será mais longa. É interessante notar que caso o grau de percepção de todos os nós chegue a zero, o valor do grau de confiança convergirá para a média dos valores atribuídos pela primeira vez e não necessariamente para o valor esperado.

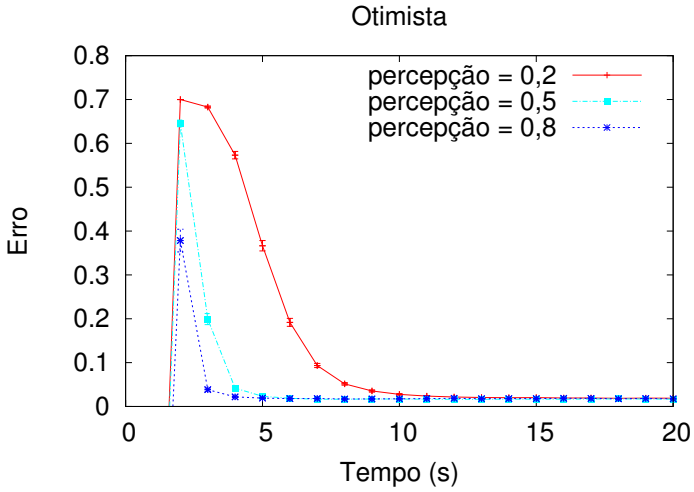


Figura 5: Variação do grau de percepção.

Em seguida, foi modificado o valor da percepção para 0,2 e variado o número de nós. A Figura 6 mostra que com um menor grau de percepção a importância de um número maior de vizinhos para alcançar um valor mais próximo do esperado é mais evidente. Isto significa que quanto menor o grau de percepção, menor é a probabilidade de um nó perceber, através das ações, a verdadeira índole de seus vizinhos. Por exemplo, supondo um a nó com índole igual a 0,8, que realizará 8 ações benéficas (valor 1) a cada 10 ações realizadas. Este nó possui apenas um vizinho v, com uma percepção de 0,5. Existe uma probabilidade, embora pequena, que as últimas i ações percebidas pelo vizinho v sejam maléficas (valor -1), apesar de o nó a gerar apenas duas a cada dez. Neste caso, o vizinho v obterá uma falsa má impressão sobre o nó a. No entanto, quando se tem muitos vizinhos, a probabilidade de que pelo menos um vizinho consiga perceber a verdadeira índole de um outro nó aumenta. Assim, ao receber recomendações de vários vizinhos, com o número de vizinhos tendendo ao infinito, a média destas recomendações tende ao valor esperado.

A Figura 7 apresenta a variação da avaliação do grau de confiança em relação à índole dos nós avaliados. Para isto, foi atribuída aos nós uma estratégia otimista (Figura 7(a)) e moderada (Figura 7(b)) e a índole dos nós foi variada entre 0,2 e 0,8. A diferença de estratégia é apenas para evidenciar o período de transiente no primeiro caso. Na Figura 7(a) observa-se que a índole não afeta significativamente a duração do período de transiente, provocando apenas um pico maior neste período, de acordo com a distância da estratégia inicial para a índole. A partir da Figura 7(b) percebe-se que durante o período estacionário, os nós têm mais dificuldade de identificar um nó com uma índole mediana que uma índole que esteja mais nos extremos. Isto acontece, pois os nós não percebem todas as ações de um determinado vizinho, assim, quanto maior for a razão entre as ações benéficas e as maléficas maior é a probabilidade de um nó se enganar.

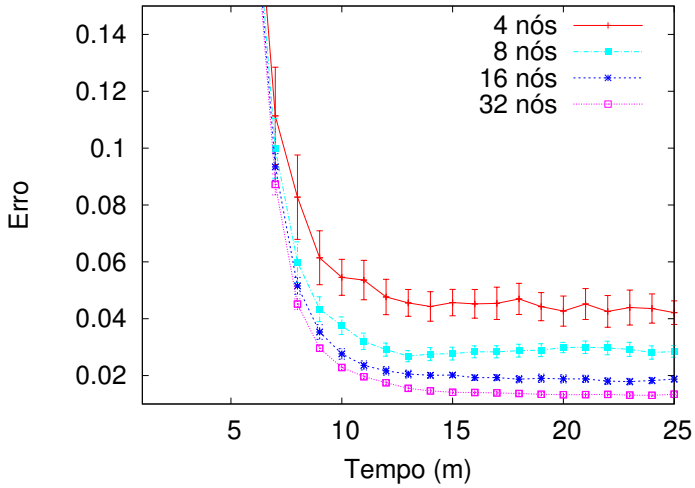
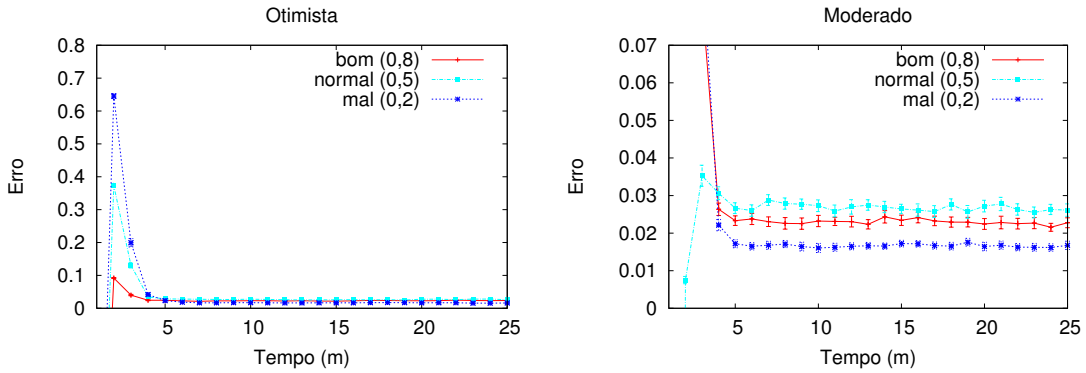


Figura 6: Número de vizinhos em relação a uma baixa percepção.



(a) Análise do transiente (b) Análise do estacionário

Figura 7: Influência da índole.

5. Conclusões

Neste artigo foi proposto um novo modelo de confiança para redes ad hoc. O principal objetivo é a construção de uma relação de confiança entre os nós, baseada no conceito humano de confiança. A abordagem deste artigo é diferente das propostas de outros trabalhos que se limitam a aspectos convencionais de segurança da rede, como a detecção de nós mal intencionados, entre outros. O foco do trabalho é prover aos nós de uma rede ad hoc uma maneira de manter uma opinião sobre seus vizinhos, que serve de base para a interação entre eles. O sistema proposto é completamente distribuído e a relação de confiança entre um nó e seus vizinhos baseia-se na recomendação de terceiros e nas suas próprias experiências. No processo de avaliação do grau de confiança, na abordagem adotada, considera não somente o grau, mas a precisão e a maturidade do relacionamento. A fim de viabilizar a troca de recomendações, foi proposto o protocolo REP (*Recommendation Exchange Protocol*).

O modelo proposto foi analisado através de simulações. Os resultados revelam a eficácia do sistema, mostrando o quão perto da índole de um nó seus vizinhos podem chegar. A influência dos principais parâmetros também foi analisada. Os parâmetros analisados foram a percepção, o número de vizinhos e o parâmetro alpha, que permite ponderar a própria experiência e a contribuição dos vizinhos no cálculo do grau de confiança. Foi possível identificar dois períodos distintos no processo de avaliação de confiança. Um período transiente que está diretamente relacionado com a percepção de cada nó e com

a estratégia inicial escolhida. Um período estacionário que depende principalmente da recomendação dos nós vizinhos e do valor do parâmetro $alpha$. Oe resultados mostram ainda que um número significativo de vizinhos pode compensar uma baixa percepção. Além disso, percebeu-se que o parâmetro $alpha$ é muito importante na escolha dos pesos do cálculo do grau de confiança, podendo influenciar tanto no período transiente como no estacionário.

Os trabalhos futuros incluem a análise do sistema proposto nas redes de múltiplos saltos na presença de mobilidade, avaliando a influência da maturidade da relação na avaliação do grau de confiança. Posteriormente, pretende-se desenvolver e acoplar ao sistema já implementado a camada de Aprendizado.

Referências

[1] J. O. Kephart e D. M. Chess, "The vision of autonomic computing", *IEEE Computer*, vol. 36, no. 1, pp. 41–52, janeiro de 2003.

[2] D. H. McKnight e N. L. Chervany, "What is trust? a conceptual analysis and an interdisciplinary model", in *Proceedings of Americas Conference on Information Systems (AMCIS 2000)*, Long Beach, EUA, agosto de 2000.

[3] S. Zhong, J. Chen e Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks", in *IEEE INFOCOM*, San Francisco, EUA, abril de 2003.

[4] L. Buttyan e J. P. Hubaux, "Enforcing service availability in mobile ad-hoc wans", in *IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Boston, EUA, agosto de 2000.

[5] L. Buttyan e J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks", *ACM/Kluwer Mobile Networks and Applications (MONET)*, vol. 8, no. 5, pp. 579–592, outubro de 2003.

[6] Z. Liu, A. W. Joy e R. A. Thompson, "A dynamic trust model for mobile ad hoc networks", in *IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04)*, Suzhou, China, maio de 2004.

[7] Z. Yan, P. Zhang e T. Virtanen, "Trust evaluation based security solution in ad hoc networks", in *Proceedings of the Seventh Nordic Workshop on Secure IT Systems, (NordSec'03)*, GjÃ¸vik, Noruega, outubro de 2003.

[8] A. A. Pirzada e C. McDonald, "Establishing trust in pure ad-hoc networks", in *Proceedings of 27th Australasian Computer Science Conference (ACSC'04)*, Dunedin, Nova Zelândia, outubro de 2004.

[9] E. Gray, J.-M. Seigneur, Y. Chen e C. Jensen, "Trust propagation in small world", in *Proceedings of 1st International Conference on Trust Management (iTrust 03)*, Creta, GrÃ©cia, maio de 2003.

[10] E. Gray, P. O'Connell, C. Jensen, S. Weber, J.-M. Seigneur e C. Yong, "Towards a framework for assessing trust-based admission control in collaborative ad hoc applications", tech. rep., Trinity College, Dublin, 2002.

[11] S. Buchegger e J.-Y. Le Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks", in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt03)*, Sophia-Antipolis, FranÃ§a, março de 2003.

[12] G. Theodorakopoulos e J. S. Baras, "Trust evaluation in ad-hoc networks", in *Proceedings of the ACM Workshop on Wireless Security (WiSE'04)*, Philadelphia, EUA, outubro de 2004.

[13] M. Virendra, M. Jadliwala, M. Chandrasekaran e S. Upadhyaya, “Quantifying trust in mobile ad-hoc networks”, in *Proceedings of IEEE International Conference on Integration of Knowledge Intensive Multi-Agent Systems (KIMAS’05)*, Waltham, EUA, abril de 2005.

[14] H. Deng, W. Li e D. P. Agrawal, “Routing security in wireless ad hoc networks”, *IEEE Communiations Magazine*, pp. 70–75, outubro de 2002.