

Análise de um modelo de confiança para redes móveis ad hoc *

Pedro B. Velloso¹, Rafael P. Laufer², Otto Carlos M. B. Duarte³, Guy Pujolle¹

¹Laboratoire d'Informatique de Paris 6 - LIP6
UPMC, França

²Computer Science Department
UCLA, E.U.A.

³Grupo de Teleinformática e Automação
PEE/COPPE - DEL/POLI
UFRJ, Brasil

{pedro.velloso,guy.pujolle}@lip6.fr, rlaufer@ucla.edu, otto@gta.ufrj.br

Abstract. *This paper presents and analyzes a trust model for mobile ad hoc networks. We aim to provide nodes a mechanism to build a trust relationship with their neighbours. The proposed model considers the recommendation of trustworthy neighbours and the experience of the node itself. The interactions are limited to direct neighbours in order to scale on mobile networks. The results show the efficiency and the trade-off of our model in the presence of mobility. We also analyze the advantages of considering the relationship maturity, i.e. for how long nodes know each other, to evaluate the trust level. The maturity parameter can decrease the trust level error up to 50%.*

Resumo. *Este artigo apresenta e analisa um modelo de confiança para redes móveis ad hoc. O objetivo é prover aos nós da rede um mecanismo para construir relações de confiança com seus vizinhos. O modelo proposto se baseia na coleta de informações locais e na troca de recomendações, restringindo as interações aos vizinhos diretos a fim de privilegiar as redes móveis. Os resultados mostram a eficiência e os compromissos do modelo proposto em redes com mobilidade. A análise dos resultados revelou as vantagens da utilização da maturidade do relacionamento, isto é, há quanto tempo os nós se conhecem, no cálculo do grau de confiança. A maturidade possibilitou uma redução de até 50% no erro do grau de confiança.*

1. Introdução

A principal diferença entre uma rede convencional e uma rede ad hoc é a ausência de infra-estrutura. Por este motivo, os nós acumulam as funções de roteador, servidor e cliente, obrigando-os a colaborar para o bom funcionamento da rede. Esta característica peculiar impede que aplicações e protocolos concebidos para as redes convencionais funcionem de forma eficiente nas redes ad hoc. Por isso, tem-se observado o surgimento e desenvolvimento de novos protocolos específicos para este tipo de rede. No entanto, a maioria dos protocolos e aplicações projetados para redes ad hoc considera a colaboração perfeita entre os nós da rede. Assume-se, então, que todos os nós da rede se comportarão

*Este trabalho foi realizado com recursos do CNPq, CAPES, FAPERJ, FINEP (Brasil) e ANR (França).

de acordo com as especificações das aplicações e dos protocolos utilizados. Contudo, seja por restrições de recursos ou por má fé, esta premissa nem sempre é verdadeira. Conseqüentemente, o comportamento dos nós pode não corresponder exatamente ao definido pelo protocolo ou aplicação, prejudicando ou, em alguns casos, inviabilizando o funcionamento da rede. Deste modo, depender do correto funcionamento de todos os nós pode levar a uma baixa eficiência da rede, um alto consumo de recursos e uma elevada vulnerabilidade a ataques. Portanto, surge a necessidade de um mecanismo a partir do qual os nós da rede possam inferir o grau de confiabilidade de seus vizinhos. Esta necessidade não se restringe apenas a questão da falta de colaboração, mas também tem impacto na questão da autonomia dos nós.

Em uma rede ad hoc não existe uma entidade responsável por configurar, gerenciar e reparar as estações, conseqüentemente, esta tarefa deve ser realizada pelos próprios nós. Segundo o paradigma de redes autonômicas, um nó deve ser capaz de aprender, se auto-configurar e se auto-gerenciar a partir da coleta de informações locais e da troca de informações com os outros nós da rede. Desta maneira, é importante poder escolher cuidadosamente os vizinhos com os quais o nó irá se comunicar, pois a troca de informações com nós comprometidos pode levar à ineficiência de um sistema autonômico para os nós de uma rede ad hoc.

Este trabalho tem como objetivo prover aos nós ad hoc um mecanismo que os permita avaliar a índole de seus vizinhos de maneira distribuída. Assim, esta informação sobre a confiabilidade dos nós vizinhos poderá ser utilizada posteriormente por protocolos e aplicações a fim de maximizar seus desempenhos.

O modelo de confiança proposto permite a construção de uma relação de confiança entre os nós da rede a partir da troca de recomendações e do monitoramento do comportamento dos vizinhos. Desta forma, o protocolo REP (*Recommendation Exchange Protocol*) é proposto para viabilizar esta troca de recomendações. Todas as interações são restritas aos vizinhos diretos de modo a maximizar a eficiência do modelo em redes móveis. Em um trabalho inicial [Velloso et al. 2006b, Velloso et al. 2006a], a validade e exatidão do modelo foi analisada em uma rede ad hoc de comunicação direta, onde todos os nós estão ao alcance um dos outros. Este trabalho apresenta uma análise do sistema de confiança perante uma rede móvel ad hoc de múltiplos saltos, mostrando o efeito dos principais parâmetros na eficiência do modelo. Os resultados mostram também a vantagem da utilização do parâmetro de maturidade, ou seja, uma informação a respeito da longevidade do relacionamento entre dois nós, quando o nível de mobilidade aumenta.

Este trabalho está organizado da seguinte forma. Os principais trabalhos relacionados são apresentados na Seção 2. A Seção 3 apresenta 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 apresentados as conclusões e os trabalhos futuros.

2. Trabalhos Relacionados

Existem diversos trabalhos 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.* [Liu et al. 2004] 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.* [Yan et al. 2003] 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, a influência de cada fator no cálculo não é especificada. 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 [Deng et al. 2002]. Novamente, o foco principal são os ataques ao protocolo de roteamento e não a construção de uma informação de confiança útil para diferentes aplicações e protocolos.

Pirzada e McDonald [Pirzada and McDonald 2006] 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 totalmente a segurança, o modelo proposto permite aos nós escolherem a rota mais confiável. Uma extensão ao protocolo DSR (*Dynamic Source Routing*) 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 [Buchegger and Le Boudec 2003] investigam 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 [Theodorakopoulos and Baras 2006] analisam 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.* [Virendra et al. 2005] apresentam uma arquitetura baseada na confiança que permite aos nós da rede tomarem decisões referentes ao estabelecimento de chaves e à 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 procedimento utilizado na avaliação 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.

Sun *et al.* [Sun et al. 2006] desenvolveram um *framework* capaz de medir o grau de confiança e propagá-lo através da rede a fim de tornar o roteamento mais seguro e auxiliar sistemas de detecção de intrusos. O *framework* inclui também um mecanismo de defesa contra nós maliciosos. O modelo probabilístico utilizado é baseado na incerteza de um vizinho executar uma determinada ação e considera apenas as informações locais.

He *et al.* [He et al. 2006] propõem uma arquitetura de incentivo à colaboração baseada na reputação dos nós. O sistema baseia-se apenas nas informações locais para avaliar a reputação. O objetivo é detectar e punir os nós que não participam do roteamento.

As duas principais diferenças deste trabalho para os citados acima são a restrição das interações aos vizinhos diretos e a introdução do conceito de maturidade da relação na recomendação dos vizinhos. Ambas as características visam permitir a convergência do sistema quando há mobilidade. Além disso, o modelo proposto considera não apenas as informações locais como também a troca de recomendações entre os nós vizinhos.

3. O modelo de confiança proposto

O objetivo do modelo é obter uma estimativa da confiabilidade, isto é, um grau de confiança, para cada vizinho direto a partir da coleta de informações locais e da troca de mensagens entre os vizinhos. Assim, o modelo de confiança proposto é dividido em duas camadas como mostra a Figura 1. A camada de confiança é responsável por calcular um grau de confiança para cada vizinho direto com base nas informações enviadas por seus vizinhos e nas informações recebidas da camada de aprendizado. Este grau de confiança é disponibilizado para todas as outras camadas, podendo ser utilizado como métrica por protocolos e aplicações. A camada de aprendizado é responsável por julgar o comportamento dos nós vizinhos a partir das informações coletadas. Para isso, é preciso que esta camada possua acesso a todas as outras camadas e ao mesmo tempo monitore os vizinhos, sempre que possível. Este julgamento resulta nas informações passadas para camada de confiança.

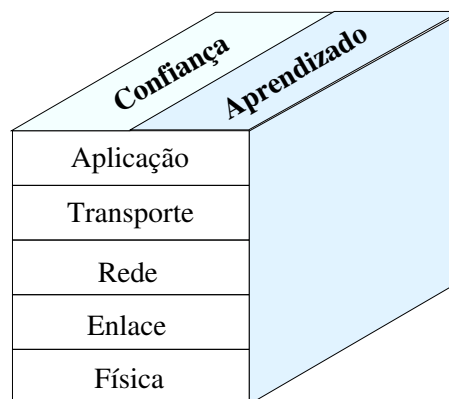


Figura 1. A arquitetura do modelo de confiança.

Cada nó irá computar e armazenar um grau de confiança para cada vizinho direto, isto é, os vizinhos que estão dentro do raio de alcance do rádio. Este valor é continuamente atualizado segundo as informações recebidas. Deve-se destacar que os nós são inteiramente responsáveis pelos seus próprios processos de avaliação do grau de confiança.

A recomendação dos nós vizinhos pode ser considerada no cálculo do grau de confiança. Uma recomendação inclui o grau de confiança, sua precisão e um parâmetro denominado maturidade da relação. O grau de confiança é um valor contínuo que pode variar de $[0,1]$. O conceito de maturidade de relacionamento, introduzido neste trabalho [Velloso et al. 2006b], reflete a duração do relacionamento de confiança entre dois nós. Este conceito permite aos nós atribuírem maior importância às recomendações baseadas em relacionamentos de mais longa duração. A fim de considerar as recomendações de outros vizinhos, os nós devem utilizar o protocolo de troca de recomendações (*Recommendation Exchange Protocol* - REP) [Velloso et al. 2006b].

A autenticação é imprescindível em modelos de confiança, por isso, neste trabalho é considerado que os nós possuem sempre algum mecanismo de autenticação. No entanto, a autenticação apenas garante que um nó seja realmente quem se diz ser e não que ele apresentará um bom comportamento.

3.1. Cálculo do grau de confiança

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. Em seguida, o nó inicia o processo de cálculo do grau de confiança que começa com um pedido de recomendações para os vizinhos diretos e o monitoramento e avaliação do comportamento do novo vizinho.

O cálculo do grau de confiança de um nó a em um vizinho b ($T_a(b)$) é definido como a soma da sua própria confiança com a contribuição dos nós vizinhos, Esta parte do modelo é similar ao apresentado em [Virendra et al. 2005], como mostra a Equação 1.

$$T_a(b) = (1 - \alpha)Q_a(b) + \alpha C_a(b), \quad (1)$$

onde $Q_a(b)$ representa a capacidade de um nó de avaliar o grau de confiança baseado nas suas próprias informações e $C_a(b)$ representa a contribuição de seus vizinhos. O parâmetro α permite priorizar o fator mais relevante entre a contribuição dos vizinhos e as informações locais disponibilizadas pela camada de aprendizado. A Equação 2 mostra como obter $Q_a(b)$ no modelo proposto.

$$Q_a(b) = \beta E_T + (1 - \beta)T_a^*(b), \quad (2)$$

onde E_T representa um valor de grau de confiança obtido através do julgamento do próprio nó a a respeito do comportamento do seu vizinho b . Esta informação é fornecida pela camada de aprendizado (Figura 1). T_a^* indica o valor do grau de confiança atribuído anteriormente. O parâmetro β permite priorizar o termo mais relevante. Desta forma, os parâmetros α e β podem variar segundo o evento desencadeando 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 2. Por outro lado, caso a atualização tenha sido desencadeada por uma reação do próprio nó a , este nó pode escolher $\alpha = \beta = 1$, ignorando a contribuição dos nós vizinhos (Equation 1) e o valor antigo para o grau de confiança sobre o nó b (Equação 2).

3.2. O Cálculo da contribuição

O processo de avaliação do grau de confiança de um nó vizinho pode levar em conta a recomendação de outros nós. O conjunto das recomendações de todos os vizinhos (diretos) comuns ao nó avaliador e avaliado é denominado de contribuição dos vizinhos ($C_a(b)$ da Equação 1). As recomendações podem ser obtidas através de um pedido expresso com o envio de um *Trust Request* (TREQ) ou com o recebimento de mensagens de anúncio de grau de confiança (*Trust Advertisement* - TA). Esta recomendação não solicitada é sempre enviada quando uma atualização de grau de confiança gera um novo grau cuja diferença, em relação ao valor anunciado na última mensagem TA enviada, for maior que um determinado limiar ($TA_{threshold}$). Os nós vizinhos respondem o pedido de recomendação com uma mensagem de *Trust Reply* (TREP).

$C_a(b)$ representa o conjunto das recomendações de todos os nós i pertencente ao conjunto de nós K_a , que representa os vizinhos em comum entre os nós a e b . Cada uma destas recomendações ($X_i(b)$) é ponderada pelo grau de confiança do nó a sobre o nó i ($T_a(i)$), como mostra a Equação 3.

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

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 recomendação inclui não somente o grau de confiança ($T_i(b)$), 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 $X_i(b)$ é uma variável aleatória de distribuição normal que pode ser expressa por

$$X_i(b) = N(T_i(b), \sigma_i(b)) \quad (4)$$

onde σ representa a precisão e é definida como o desvio padrão. Esta definição é similar àquela de Theodorakopoulos e Baras [Theodorakopoulos and Baras 2004].

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:

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

onde S_k representa o conjunto das k últimas amostras de grau de confiança sobre o nó b , dado $k \in \mathbb{N} \mid 2 \leq k \leq 10$. \bar{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 da relação ($M_i(b)$) entre o nó i e 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. A utilização deste parâmetro é uma das contribuições principais do modelo proposto

Nós maliciosos podem tentar falsificar graus de confiança por diversas razões. Por exemplo, um nó pode querer difamar um vizinho, ou tentar convencer seus vizinhos de que um determinado nó malicioso é, na verdade, um nó de boa índole. 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:

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

Para o correto funcionamento do sistema, o limiar da maturidade (M_{max}) deve ser baseado na média dos valores de maturidade de relacionamento de todos seus vizinhos.

4. Resultados

Em uma rede ad hoc, um nó pode realizar diversas operações, tais como o envio de um pacote, o encaminhamento de pacotes, resposta a mensagens de roteamento, o envio de uma mensagem CTS (*Clear to Send*) da camada MAC (*Medium Access Control*), entre outras. O conjunto de operações realizadas por um nó define o seu comportamento. O objetivo da camada de aprendizado é monitorar estas operações e avaliar o comportamento de um determinado vizinho. No simulador, todas as operações são modeladas através de ações que podem ser consideradas como boas ou más. Assim, durante a simulação, cada nó executa ações segundo uma distribuição exponencial. A qualidade da ação executada depende exclusivamente da índole do nó. Cada nó possui um comportamento pré-definido que está associado a sua índole e que é representado por um grau de confiança. Desta forma, quanto maior for o grau de confiança associado a um nó, melhor será sua índole. Portanto, uma índole igual a 0,8 significa que o nó executa 8 ações boas a cada 10. Assim, existem apenas ações boas e más que representam o conjunto de possíveis operações em uma rede ad hoc.

O conceito de percepção dos nós é utilizado para abstrair a camada de aprendizado. Desta maneira, cada nó possui uma capacidade de perceber as ações realizadas por seus vizinhos. A percepção representa a probabilidade de que uma ação seja percebida. Assim, um nó com percepção 0,7 percebe 70% das ações realizadas por seus vizinhos. O maior consumo de energia está principalmente relacionado com o monitoramento dos nós vizinhos. Assim, o consumo dependerá do nível de percepção de cada nó, ou seja, a capacidade de monitoramento. Espera-se que um nó com restrições de energia economizará no monitoramento e, por consequência, terá um nível de percepção inferior. Por isso, neste trabalho foi avaliado nós com diferentes níveis de percepção.

A camada aprendizado julga um vizinho a partir das n últimas ações realizadas por este vizinho e que foram percebidas. O resultado deste julgamento é um valor de grau de confiança atribuído ao vizinho baseado na observação de seu comportamento. Este valor representa o primeiro termo da Equação 2 e será utilizado pela camada de confiança para fazer o cálculo do grau de confiança global.

O principal objetivo deste trabalho é avaliar o funcionamento do sistema de confiança em uma rede ad hoc móvel e, sobretudo, verificar o impacto do parâmetro de maturidade da relação entre os nós na eficiência do sistema.

Para isso, foi desenvolvido um simulador em C++. Optou-se por um simulador próprio para que fosse possível uma análise detalhada do modelo proposto. A utilização deste simulador permite, entre outras coisas, o total controle sobre a camada de aprendizado. Todos os resultados possuem um intervalo de confiança de 95% representados pelas barras de erro. O objetivo de um nó nas simulações é inferir o valor exato da índole de seus vizinhos. Em todos os gráficos, no eixo das coordenadas é representado o erro do grau de confiança (*Trust Level Error* - TLE), isto é, o módulo da diferença entre o valor encontrado na avaliação da índole e o valor correto. Isto significa que quando um nó de índole 0,4 é avaliado por seu vizinho como tendo índole 0,5, o erro é de 0,1. Em um sistema de confiança ideal, o erro deve ser igual a zero.

O cenário utilizado compreende uma rede em forma de grade constituída por 21 nós distantes entre si de 150 metros em uma área de 1000 X 400 m², como mostra a Figura 2. O raio de cobertura de cada nó é de 250 metros.

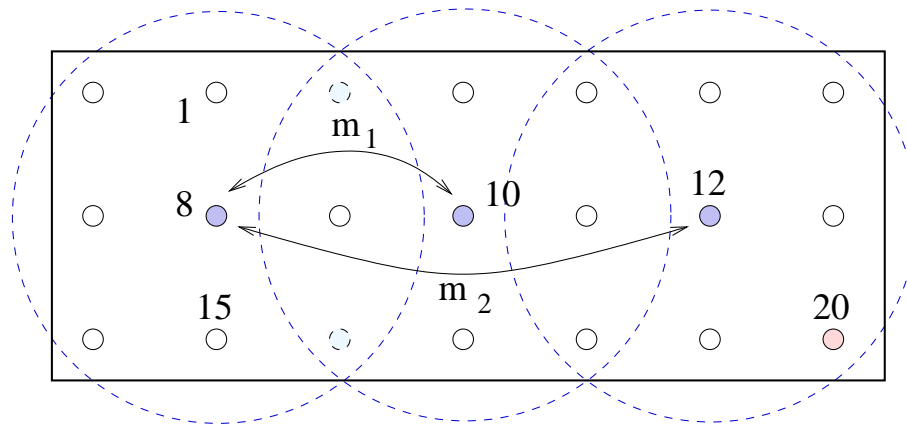


Figura 2. O cenário.

Foram definidos alguns valores padrão para os principais parâmetros nas simulações. O valor de $\alpha = \beta = percepcao = 0,5$, o valor de confiança atribuído inicialmente quando um novo vizinho é encontrado (F_a) é 0,9 e todos os nós possuem a mesma índole igual a 0,2. Estes dois últimos valores foram escolhidos como pior caso. Em cada configuração das simulações, apenas são mencionados os parâmetros que foram alterados em relação ao valor padrão.

Na primeira configuração, o nó 8 se movimenta em direção a um lugar específico. Após chegar ao seu destino, o nó 8 retorna a sua posição de origem. Depois de chegar à origem, ele segue repetindo o mesmo movimento durante o restante da simulação. As Figuras 3 e 4 mostram a média dos valores de TLE para todos os vizinhos do nó 8. No

movimento mais curto (m_1 da Figura 2), o nó 8 mantém ainda três antigos vizinhos, enquanto que no movimento mais longo (m_2 da Figura 2), ele vai para um lugar onde não conhece ninguém. Para garantir que o tempo de locomoção seja equivalente em ambas as curvas, definiu-se as velocidades de deslocamento como sendo uma o dobro da outra.

Pode-se observar, pela Figura 3, a existência de dois períodos distintos. Um período inicial em que o erro do grau de confiança ainda alto e apresenta grande variação, e outro onde o erro atinge seu valor mínimo e apresenta um comportamento estável. Esta característica tinha sido observada anteriormente para as redes de comunicação direta onde foram definidos como período transiente e período estacionário [Velloso et al. 2006a]. O segundo aspecto a ser observado é a diferença no valor de pico inicial quando o nó chega em um novo destino. No começo da simulação, os nós ainda não se conhecem e, portanto, não possuem informações sobre seus vizinhos. Quando o nó 8 chega em outro destino e não conhece ninguém, ele deve começar novamente o processo de avaliação de seus vizinhos, porém, desta vez, seus vizinhos já se conhecem. Assim, o nó 8 recebe informações mais precisas dos seus vizinhos diminuindo assim o pico do período transiente. Por fim, percebe-se também que o fato de manter vizinhos antigos também contribui para diminuir o pico do transiente devido ao deslocamento, pois o erro do grau de confiança para esses vizinhos já atingiu o estado estacionário. A Figura 4 possui exatamente a mesma configuração anterior exceto pelas

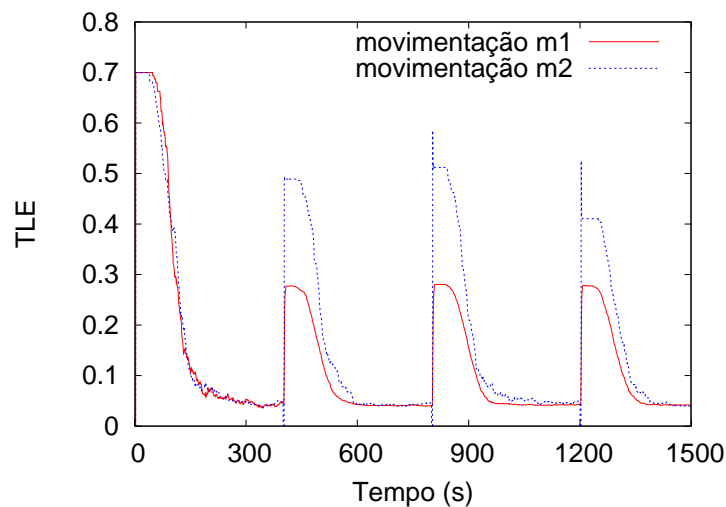


Figura 3. velocidades de 1 m/s e 2 m/s.

velocidades. Neste caso, o nó 8 se desloca 3 vezes mais rápido. Nota-se que, pela falta de tempo, o nó 8 não foi capaz de chegar no período estacionário. Este resultado indica a existência de um compromisso entre a velocidade do nó e a exatidão do processo de avaliação de seus vizinhos. Os resultados das Figuras 5 e 6 são obtidos com o mesmo padrão de deslocamento descrito para a Figura 3. Na Figura 5, o parâmetro α é alterado para 0,8 e na Figura 6 a percepção é alterada para 0,2. Nota-se pela Figura 5 que o aumento no valor do parâmetro α implica a diminuição do tempo do período transiente, comparado com o da figura Figura 3. Isto significa que valorizar mais as recomendações dos vizinhos agiliza o processo de convergência do grau de confiança. Isto ocorre porque quando um nó chega a um novo lugar onde os vizinhos já se conhecem, vale mais a pena

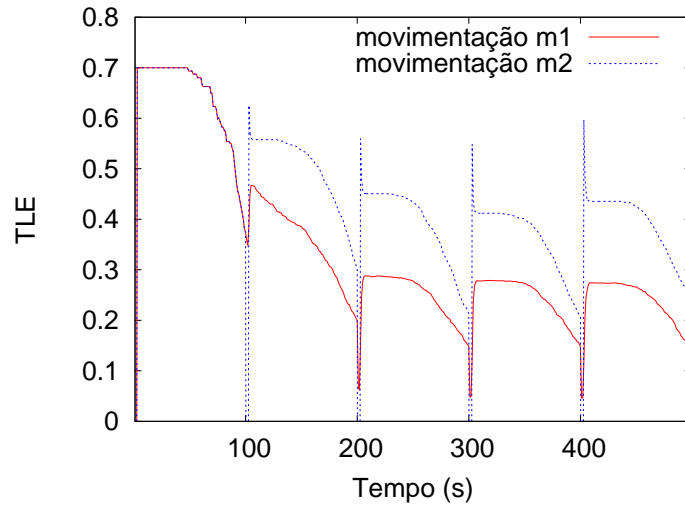


Figura 4. velocidades de 3 m/s e 6 m/.

considerar a opinião deles que esperar para convergir com a própria avaliação do comportamento dos vizinhos. Assim, um nó com maior mobilidade, pode aumentar o valor do parâmetro α para reduzir o tempo de transiente. No entanto, existe sempre o compromisso entre o aumento da velocidade de convergência e o aumento da vulnerabilidade a ataques de nós mentirosos ou de conluios. Ambos os efeitos são proporcionados pelo incremento deste parâmetro. A Figura 6 mostra o efeito da perda de percepção no erro

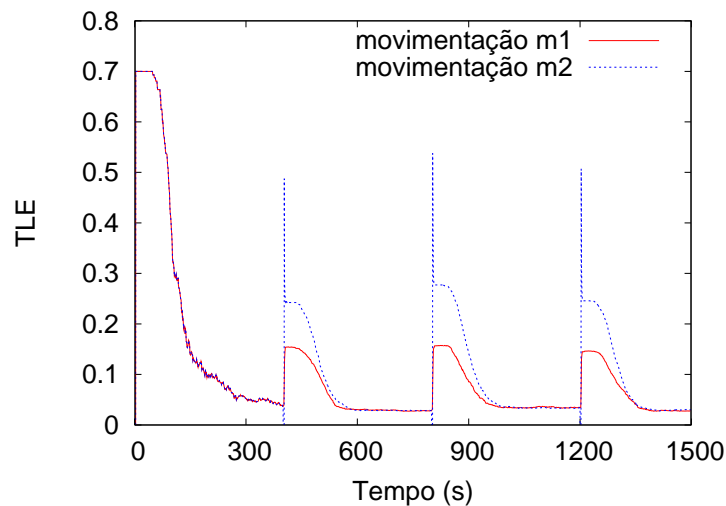


Figura 5. Efeito do aumento do parâmetro α .

do grau de confiança. Percebe-se que a queda na percepção de um nó provoca um aumento no tempo transiente prejudicando a convergência do processo de obtenção do grau de confiança. A falta de percepção implica um tempo maior de coleta de informações para a obtenção de um julgamento a respeito do comportamento do vizinho, tarefa esta realizada pela camada de aprendizado. Desta forma, um nó que possua baixa capacidade de percepção estaria restrito a uma baixa mobilidade. Neste caso, o aumento do α poderia ser interessante a fim de diminuir o período transiente, visto que com a baixa percepção,

ele já estaria mais dependente das recomendações dos vizinhos e necessariamente mais vulnerável a um ataque de conluio. Um nó que possua baixa percepção por estar economizando recursos, por exemplo, teria a opção de trocar economia de recursos por maior mobilidade para manter o mesmo TLE.

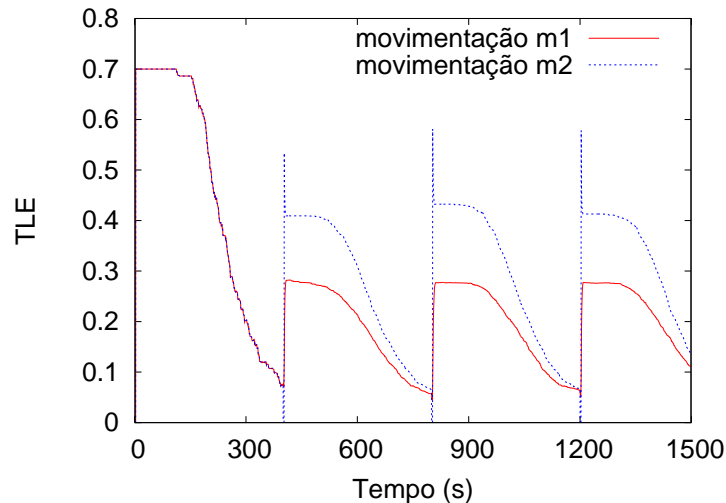


Figura 6. Efeito da perda na percepção.

4.1. Maturidade da relação

Em seguida, ainda utilizando o mesmo cenário da Figura 2 mas com outro padrão de movimentação, novas simulações foram realizadas a fim de verificar o impacto do parâmetro da maturidade da relação no processo de avaliação do grau de confiança dos vizinhos em redes móveis ad hoc. Desta vez, os nós 1, 8 e 15 irão se deslocar para o lugar onde se encontra o nó 12. Diferentemente das simulações anteriores, ao invés de fazer a média dos graus de confiança de todos os vizinhos do nó 8, será medido apenas a avaliação do nó 8 a respeito do nó 20, depois que ele chega ao seu destino. Isto significa, que no momento em que o nó 8 iniciar seu processo de obtenção de grau de confiabilidade do nó 20, existirão apenas três vizinhos que já conhecem o nó 20, que já alcançaram o período transiente e que poderão dar recomendações mais exatas sobre o nó 20. Pois os outros dois nós (1 e 15) acabaram de chegar neste lugar junto com o nó 8. A maturidade da relação tenta justamente priorizar a recomendação de quem conhece mais o nó avaliado. Neste caso, não considerar a maturidade da relação dos nós mais antigos seria desperdiçar esta informação. É importante ressaltar que a maturidade é relativa ao relacionamento entre os nós que está fornecendo a recomendação, ou seja, os vizinhos do nó 20, e o nó avaliado (nó 20). Estas maturidades não dependem do nó avaliador (nó 8). Neste caso, a maturidade do relacionamento é entre o nó 20 e seus vizinhos.

Os resultados mostrados nas Figuras 7 e 8 comprovam que o uso da maturidade do relacionamento pode reduzir o período transiente, o que possibilita uma maior mobilidade. Na Figura 8, os nós priorizam as recomendações dos vizinhos em detrimento das informações locais ($\alpha = 0,8$). Neste caso, as vantagens do uso da maturidade do relacionamento são mais evidentes. As Figuras 9 e 10 apresentam os resultados no caso de baixa percepção. Em ambos os gráficos, o nó 8 não consegue alcançar o estado estacionário devido ao aumento do tempo necessário para a coleta de informações

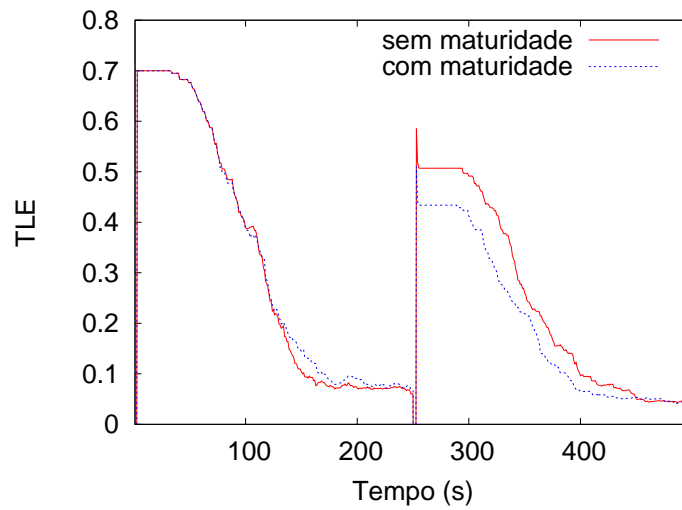


Figura 7. $\alpha = 0,5$.

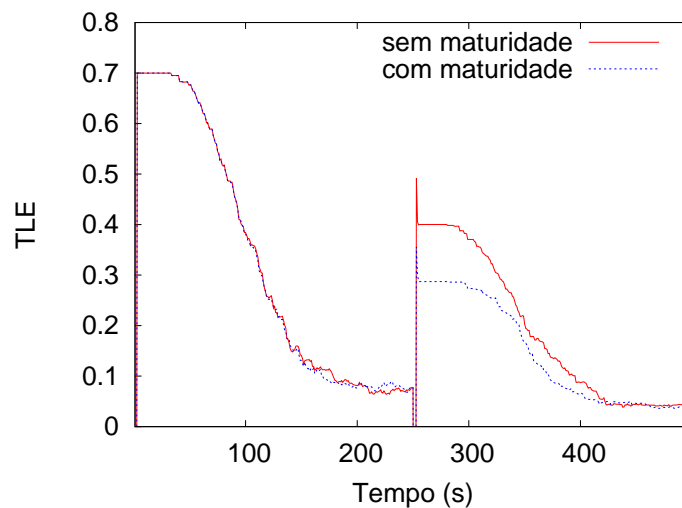


Figura 8. $\alpha = 0,8$.

dos vizinhos. Esta situação é semelhante àquela descrita durante a análise da Figura 6, como já mencionado anteriormente. No entanto, nota-se que o aumento do parâmetro α (Figura 10) permite o nó 8 de chegar mais próximo do período estacionário. Neste caso, a maturidade do relacionamento proporcionou uma melhora ainda maior na convergência do grau de confiança. Foi possível obter um erro até 50% menor. Portanto, pode-se concluir que a melhor configuração para usufruir das vantagens do uso da maturidade do relacionamento são para nós com baixa percepção e um valor alto α .

5. Conclusões

Este artigo apresenta e analisa um modelo de confiança para redes móveis ad hoc. O objetivo é oferecer aos nós da rede um mecanismo para avaliar a índole de seus vizinhos. O modelo proposto limita as interações aos vizinhos diretos, de modo a se adequar às redes móveis. Uma análise da eficiência e do impacto dos principais parâmetros do modelo foi realizada através de simulações. Os resultados indicaram que o modelo de

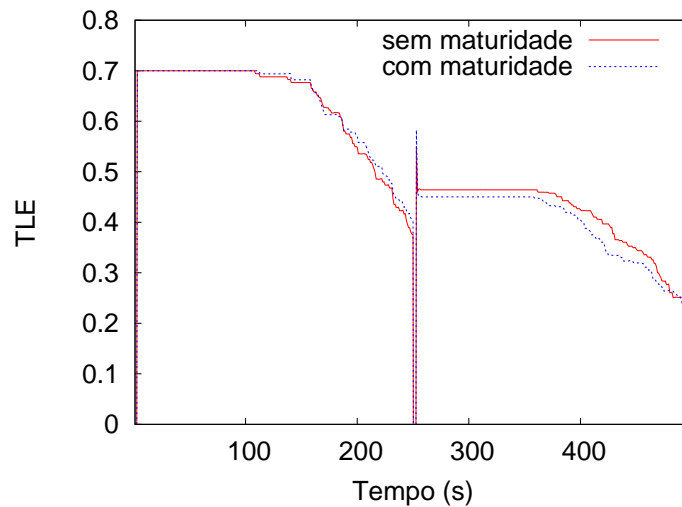


Figura 9. percepção = 0,2 e alpha = 0,5.

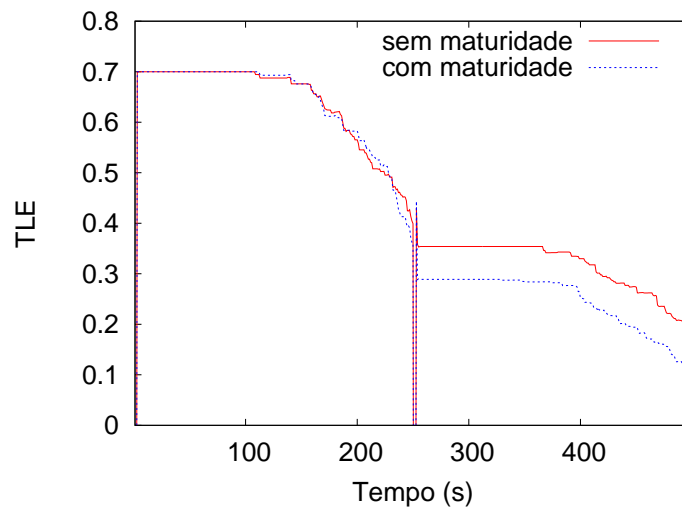


Figura 10. percepção = 0,2 e alpha = 0,8.

confiança proposto possui um compromisso entre o nível de mobilidade e a convergência do grau de confiança. Pode-se identificar que o fator que influencia no nível de mobilidade é o tamanho do período transiente. Além disto, percebeu-se que este período pode ser alterado variando-se alguns parâmetros do modelo. Através dos resultados, pode-se concluir que o uso da maturidade do relacionamento pode ser utilizado para compensar um nível mais alto de mobilidade, sobretudo em nós de baixa percepção, ou seja, dificuldade de monitorar seus vizinhos. Outra possibilidade para obter um melhor desempenho do sistema de confiança em redes móveis é privilegiar as recomendações dos vizinhos aumentando o valor do parâmetro α .

Na seqüência deste trabalho, pretende-se analisar o efeito de vizinhos mentirosos no modelo proposto e posteriormente, a definição e implementação da camada de aprendizado.

Referências

- Buchegger, S. and Le Boudec, J.-Y. (2003). 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, França.
- Deng, H., Li, W., and Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communications Magazine*, pages 70–75.
- He, Q., Wu, D., and Khosla, P. (2006). A secure incentive architecture for ad hoc networks. *Wireless Communications and Mobile Computing*, 6(3):333–346.
- Liu, Z., Joy, A. W., and Thompson, R. A. (2004). A dynamic trust model for mobile ad hoc networks. In *IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04)*, Suzhou, China.
- Pirzada, A. A. and McDonald, C. (2006). Trust establishment in pure ad-hoc networks. *Wireless Personal Communications: An International Journal*, 37(1):139–168.
- Sun, Y., Han, Z., Yu, W., and Liu, K. J. R. (2006). A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. In *IEEE IN-FOCOM'06*, Barcelona, Espanha.
- Theodorakopoulos, G. and Baras, J. S. (2004). Trust evaluation in ad-hoc networks. In *Proceedings of the ACM Workshop on Wireless Security (WiSE'04)*, Philadelphia, EUA.
- Theodorakopoulos, G. and Baras, J. S. (2006). On trust models and trust evaluation metrics for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 24(2):318–328.
- Velloso, P. B., Laufer, R. P., Duarte, O. C. M. B., and Pujolle, G. (2006a). HIT: A human-inspired trust model. In *8th IFIP IEEE International Conference on Mobile and Wireless Communication Networks - MWCN'2006*, Santiago, Chile.
- Velloso, P. B., Laufer, R. P., Duarte, O. C. M. B., and Pujolle, G. (2006b). Um novo modelo para confiança em rede ad hoc. In *XXIV Simpósio Brasileiro de Redes de Computadores - SBRC'2006*, Curitiba, Brasil.
- Virendra, M., Jadliwala, M., Chandrasekaran, M., and Upadhyaya, S. (2005). 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.
- Yan, Z., Zhang, P., and Virtanen, T. (2003). Trust evaluation based security solution in ad hoc networks. In *Proceedings of the Seventh Nordic Workshop on Secure IT Systems, (NordSec'03)*, Gjøvik, Noruega.