

MAPA: Mecanismo de Avaliação e Punição de nós egoístas em redes Ad hoc

Reinaldo B. Braga¹, Danilo M. Taveira¹ e Otto Carlos M. B. Duarte^{1*}

¹Grupo de Teleinformática e Automação (GTA)
Universidade Federal do Rio de Janeiro (UFRJ)
Rio de Janeiro, RJ – Brasil

{reinaldo,danilo,otto}@gta.ufrj.br

Abstract. *Ad hoc networks rely on node cooperation to perform routing and data forwarding. Therefore, nodes with selfish behavior can benefit from this cooperation to drop packets, decreasing the network performance. One of the main challenges is to correctly detect the selfish nodes, since false positives can be generated due to temporary problems in ad hoc networks. This paper presents the MAPA, a mechanism that performs evaluations and punishments of selfish nodes based on the results of detections locally collected only. Finally, the mathematical analysis and simulations show that the MAPA is efficient on evaluations and punishments to the selfish nodes, decreasing the number of false positives and improving the network delivery rate.*

Resumo. *As redes ad hoc confiam na cooperação dos nós para que as funções de roteamento e encaminhamento de pacotes sejam realizadas. Entretanto, os nós com comportamento egoísta podem se beneficiar da característica de cooperação destas redes para não encaminhar pacotes, reduzindo o desempenho da rede. Dentro deste contexto, um dos principais desafios é detectar e punir corretamente os nós egoístas, pois os falso-positivos podem ocorrer devido aos problemas temporários das redes ad hoc. Neste artigo, é apresentado o Mecanismo de Avaliação e Punição de nós egoístas em redes Ad hoc (MAPA). A avaliação e a punição dos nós egoístas são realizadas com base nos resultados das detecções coletadas localmente por cada nó. Através de uma análise matemática e de simulações, é apresentada a eficiência do MAPA no processo de avaliação e punição de nós egoístas, reduzindo o total de falso-positivos e aumentando a taxa de entrega de pacotes da rede.*

1. Introdução

As redes ad hoc são caracterizadas pela ausência de infra-estrutura ou de administração centralizada. Portanto, estas redes confiam na cooperação dos nós para realizarem as funções de roteamento e encaminhamento de dados. A partir desta característica, um nó pode decidir não cooperar no encaminhamento de pacotes com o objetivo de atacar a rede ou de simplesmente economizar os seus recursos computacionais. Estes nós que não cooperam no encaminhamento são chamados de nós egoístas e podem reduzir o desempenho da rede ao descartarem os pacotes que deveriam ser encaminhados. Desta

*Este trabalho foi realizado com recursos do CNPq, FINEP, RNP, FAPERJ e CAPES

forma, é necessário utilizar mecanismos capazes de evitar que estes nós mal comportados sejam usados na comunicação entre os nós cooperativos das redes ad hoc.

As propostas convencionais contra maus comportamentos utilizam mecanismos criptográficos para identificar e autenticar os nós, além de proteger o conteúdo das mensagens. Entretanto, estes mecanismos sozinhos não garantem que toda estação autenticável se comportará corretamente na rede. Portanto, torna-se necessária a utilização de mecanismos para detectar e punir os nós autenticados que realizam maus comportamentos. Estes mecanismos são conhecidos na literatura como sistemas de detecção de intrusão.

De acordo com Kang *et al*, dois modelos de detecção de maus comportamentos podem ser utilizados em redes ad hoc [Kang et al., 2005]. No primeiro modelo, baseado em assinaturas, cada nó mantém uma base de assinaturas dos eventos de maus comportamentos conhecidos. Dessa forma, qualquer evento que possua uma assinatura semelhante a uma assinatura da base é classificado como um mau comportamento. Já no segundo modelo, baseado em anomalias, todo nó usa uma base de eventos normais conhecidos e classifica como mau comportamento qualquer evento diferente dos eventos da base. De acordo com Anantvalee e Wu, os modelos baseados em anomalias não requerem a análise de uma grande quantidade de assinaturas de maus comportamentos, tais como as análises realizadas pelos modelos baseados em assinaturas [Anantvalee e Wu, 2006]. Além disso, os modelos baseados em anomalias não necessitam de atualizações constantes em sua base de eventos e possibilitam a análise de detecções localmente.

Em redes ad hoc, ambos os modelos de detecção geram falso-positivos nas punições, que ocorrem, por exemplo, quando um nó cooperativo é punido por ter sido classificado como um nó egoísta. Os principais fatores causadores das detecções incorretas são os problemas temporários que ocorrem nas redes ad hoc, tais como as colisões e a disputa de acesso ao meio [Marti et al., 2000]. Nas colisões, os falso-positivos ocorrem quando um nó não percebe que o pacote foi corretamente encaminhado pelo seu vizinho, devido a uma colisão. Já na disputa de acesso ao meio, um nó pode ser detectado enquanto aguarda a liberação do meio para encaminhar os pacotes que estão na fila. Portanto, ao considerar os problemas em redes ad hoc, é importante que o mecanismo de detecção e punição seja eficiente para reduzir a quantidade de falso-positivos nas punições.

Neste artigo, é apresentado um mecanismo que aumenta a precisão nas respostas aplicadas aos nós egoístas da rede. Esta precisão é obtida através de avaliações realizadas pelo Mecanismo de Avaliação e Punição de nós egoístas em redes Ad hoc (MAPA), que utiliza as informações dos eventos monitorados por um sistema de detecção baseado em anomalias, chamado de Sistema de Detecção de nós Egoístas (SDE). O SDE monitora o encaminhamento de pacotes realizado pelo próximo salto na rota e contabiliza todos os pacotes encaminhados ou não. Após observar uma quantidade determinada de pacotes não encaminhados, o SDE passa estas informações para o MAPA, que é responsável por avaliar todos estes eventos monitorados e por determinar se o nó avaliado será bloqueado temporariamente ou definitivamente da comunicação com o nó que o avaliou. O objetivo principal é reduzir o número de bloqueios definitivos enviados aos nós cooperativos, aumentando a oportunidade do nó cooperativo, que foi incorretamente detectado, provar que não é um nó egoísta. Além disto, o MAPA tem o propósito de punir uma maior quantidade de nós egoístas sem gerar uma elevada quantidade de falso-positivos. Os resultados da simulação mostram que o SDE e o MAPA são mais eficientes do que as outras propostas

analisadas, devido à menor razão entre a quantidade de falso-positivos gerada para cada punição corretamente aplicada. A partir dos resultados, é observado que o SDE/MAPA aumenta a taxa de entrega da rede em até 27%, mesmo com a presença de 12,5% dos nós da rede descartando pacotes que deveriam ser encaminhados.

Este artigo está organizado como se segue. Na Seção 2 são apresentados os trabalhos relacionados. Na Seção 3 são apresentados o SDE e o MAPA. Na Seção 4 são descritos os parâmetros assumidos e os resultados da análise matemática do mecanismo proposto. Na Seção 5 são apresentadas as premissas assumidas para os cenários de rede ad hoc e discutidos os resultados obtidos na simulação. Finalmente, na Seção 6 é apresentada a conclusão deste artigo.

2. Trabalhos Relacionados

O Watchdog foi o primeiro sistema criado para detectar nós maliciosos em redes ad hoc [Marti et al., 2000]. Este mecanismo baseia-se no monitoramento de eventos realizados pelos nós vizinhos. O Watchdog foi implementado usando o protocolo de roteamento *Dynamic Source Routing* (DSR) [Johnson e Maltz, 1996] e tem como principal objetivo observar se o pacote enviado para um nó intermediário da rota é encaminhado para o próximo salto. Para evitar que o nó malicioso seja utilizado nas rotas da rede, os autores implementaram o mecanismo Pathrater, que usa uma métrica baseada nas detecções locais de cada nó da rede. Para calcular a métrica, cada nó utiliza uma variável associada para cada vizinho, que decremента no caso do nó ser detectado como malicioso e incrementa a cada intervalo de 200ms sem o nó ser detectado. Ao usar esta variável como métrica de roteamento para a seleção de rotas na rede, é possível a formação de rotas somente com nós cooperativos, evitando os nós maliciosos. A desvantagem do Watchdog está relacionada com a quantidade de falso-positivos gerada devido aos problemas das redes ad hoc. Estes falso-positivos são prejudiciais para o Pathrater, pois os nós maliciosos deixam de ser evitados nas rotas, causando uma degradação no desempenho da rede. Como os nós maliciosos não são bloqueados da rede, eles podem ser usados em rotas futuras e continuar descartando os pacotes, reduzindo a taxa de entrega da rede.

Com base no modelo de detecção do Watchdog, Buchegger e Boudec criaram o CONFIDANT [Buchegger e Boudec, 2002]. Este protocolo continua seguindo a idéia de que cada nó da rede monitora seus nós vizinhos. Os autores introduzem os conceitos de gerenciador de confiança, sistema de reputação e gerenciador de caminhos. Ao usar as informações de reputação de todos os nós pertencentes às rotas encontradas, o nó é capaz de determinar a rota mais segura. A desvantagem deste protocolo é o controle que um nó malicioso pode ter nas decisões referentes às punições realizadas na rede, pois as punições são realizadas a partir da troca de informações sobre detecções realizadas por terceiros. Desta forma, um nó malicioso pode enviar falsas acusações na rede e provocar punições de nós cooperativos. Portanto, existe a necessidade de implementação de um mecanismo de confiança para analisar a reputação dos nós que enviam alertas de detecção. Por exemplo, um nó malicioso é capaz de ganhar uma boa reputação encaminhando pacotes corretamente por um determinado tempo. Após conseguir essa boa reputação, o nó pode iniciar uma inundação de falsas acusações na rede, incentivando a ocorrência de falso-positivos. Para resolver este problema, os autores apresentaram soluções usando estatísticas Bayesianas [Buchegger e Boudec, 2003].

De acordo com Anantvalee e Wu, o Watchdog e o Pathrater são eficazes na escolha de rotas que evitam os nós maliciosos nas redes ad hoc. Entretanto, esses mecanismos permitem que os nós egoístas continuem encaminhando seus pacotes sem receber nenhum tipo de punição [Anantvalee e Wu, 2006]. Desta forma, os nós egoístas são detectados, mas não são excluídos, podendo degradar o desempenho da rede. O MAPA tenta solucionar este problema bloqueando qualquer comunicação do nó egoísta com os nós vizinhos que o detectaram, reduzindo o número de falso-positivos e impossibilitando que os nós egoístas continuem usando a rede.

3. SDE e MAPA

Este artigo apresenta a proposta de um mecanismo de avaliação e punição que calcula a probabilidade de um nó detectado ser realmente um nó egoísta. Com base nessa probabilidade, o MAPA determina se o nó será bloqueado temporariamente ou definitivamente. Enquanto o nó estiver bloqueado, toda rota armazenada ou recém descoberta contendo o endereço do nó egoísta é descartada. Portanto, um novo procedimento de descoberta de rota é iniciado a partir do nó que detectou o nó egoísta e uma mensagem de erro de rota é enviada ao nó fonte. Estas mensagens de erro são utilizadas pelo protocolo de roteamento *Dynamic Source Routing* (DSR) no procedimento de manutenção de rotas [Johnson e Maltz, 1996]. Para evitar que os nós egoístas continuem utilizando a rede, os pacotes criados pelos nós egoístas não são encaminhados pelos nós vizinhos que o bloquearam. Todos os procedimentos de detecção, avaliação e punição são realizados localmente em cada nó.

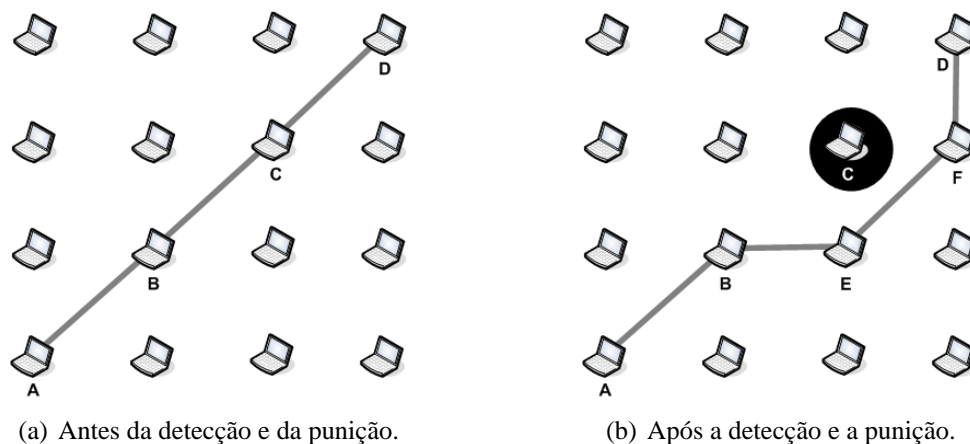


Figura 1. Exemplo do funcionamento do SDE e do MAPA em uma rede ad hoc.

A Figura 1(a) ilustra uma rota conhecida do nó fonte A até o nó destino D, passando pelos nós intermediários B e C. Ao receber os pacotes do nó A, o nó B os encaminha para o nó C, que é o próximo salto na rota. Em certo instante, o nó B percebe que o nó C não está encaminhando os pacotes e, então, inicia o procedimento de avaliação. Após a avaliação, o nó C é bloqueado pelo nó B. Neste momento, o nó B pode utilizar uma segunda rota armazenada em *cache* ou iniciar um procedimento de descoberta de rota a partir dele mesmo. Ao encontrar a nova rota, o nó B envia uma mensagem de erro de rota para o nó fonte, inserindo a nova rota descoberta nesta mensagem, evitando o nó C. Como ilustrado na Figura 1(b), o nó A passará a utilizar a nova rota para enviar os pacotes para D. Este procedimento de descoberta de rota a partir de um nó intermediário é uma

ferramenta adicional utilizada pelo DSR para evitar que os pacotes presentes em um nó intermediário sejam descartados durante o procedimento de manutenção de rotas.

Os mecanismos de detecção, avaliação e punição foram implementados em uma camada criada acima da camada de rede. As detecções são realizadas pelo Sistema de Detecção de nós Egoístas (SDE), que baseia-se no modelo de detecção do Watchdog [Martí et al., 2000]. As avaliações e as punições são executadas pelo MAPA e ocorrem após uma ou mais detecções de eventos egoístas detectados pelo SDE.

3.1. Sistema de Detecção de nós Egoístas (SDE)

O SDE observa os eventos de envio, recebimento e encaminhamento do protocolo de roteamento *Dynamic Source Routing* (DSR). Para realizar a detecção, o SDE armazena um identificador para cada pacote enviado. O identificador possui um temporizador que será removido somente se o pacote encaminhado pelo nó monitorado for recebido pelo nó que está monitorando. Este temporizador do SDE usa o mesmo valor do temporizador utilizado pelo DSR para aguardar a resposta de uma descoberta de rota. Portanto, se o temporizador do identificador expirar, a detecção de evento egoísta é realizada e o identificador é removido. Assim, o SDE é capaz de monitorar o encaminhamento de pacotes executado pelo próximo salto na rota, quando este não for o destinatário do pacote.

No SDE, o nó não observa os eventos realizados na comunicação entre dois vizinhos adjacentes, somente quando ele faz parte da rota. Após a detecção e o bloqueio serem executados, caso não seja encontrada uma rota secundária que evite o nó bloqueado, o nó destino é classificado como inalcançável. Entretanto, o nó fonte pode optar pelo envio de pacotes por rotas com a presença de nós egoístas, pois existe a possibilidade do nó egoísta estar executando um descarte seletivo. Para isso, o nó fonte teria que utilizar um marcador indicando aos vizinhos dos nós bloqueados que encaminhem os pacotes.

Apesar de usarem a mesma forma de detecção, o SDE e o Watchdog se diferem em alguns aspectos. O SDE contabiliza todos os eventos de encaminhamento do nó monitorado, pois o MAPA utiliza as informações sobre os pacotes que foram encaminhados ou não. Por outro lado, o Watchdog não contabiliza os pacotes corretamente encaminhados, pois ele necessita somente das informações sobre os eventos de não encaminhamento. Além disso, após o nó ser bloqueado, o SDE é responsável por requisitar uma nova rota para o protocolo de roteamento e por solicitar a inserção da nova rota na mensagem de erro que será enviada ao nó fonte. Uma vez que o SDE trabalha observando as mensagens de controle do roteamento, é possível que um nó atacante utilize essas mensagens para tentar enganar os nós da rede. Este ataque é conhecido na literatura como ataque bizantino. Portanto, o SDE foi implementado para ser capaz de trabalhar em conjunto com as soluções de defesa contra o ataque bizantino, tais como as soluções apresentadas em [Yu et al., 2005] [Marano et al., 2006].

Como citado anteriormente, os falso-positivos nas punições ocorrem devido às detecções incorretas realizadas pelo SDE. Estas detecções incorretas são provocadas por problemas temporários que ocorrem nas redes ad hoc. Para tentar reduzir a influência que as detecções incorretas exercem nas punições aplicadas aos nós da rede, o SDE utiliza um limiar de tolerância D . Este limiar determina o número de vezes que os eventos egoístas devem ser detectados. Quando este limiar é atingido, o total de eventos normais e egoístas contabilizados são passados para o MAPA, que realiza a avaliação. O parâmetro que con-

tabiliza todos os eventos observados até a ocorrência do D -ésimo evento é representado por e . Dessa forma, se $e = 100$ e $D = 5$, então pode-se afirmar que a quinta detecção ocorreu no centésimo evento monitorado. Logo, sabe-se que foram observados 95 eventos normais e 5 eventos egoístas.

3.2. Mecanismo de Avaliação e Punição de nós egoístas em redes Ad hoc (MAPA)

O MAPA é responsável por aplicar com precisão as punições aos nós detectados, com base nas informações coletadas pelo SDE. Para realizar as punições, o MAPA utiliza estas informações e inicia a avaliação no instante em que a D -ésima detecção de evento egoísta é observada. A avaliação então retorna um resultado que indica a probabilidade do nó ser egoísta. Esta probabilidade é representada por p e é obtida através de

$$p = \frac{D}{e}. \quad (1)$$

A cada avaliação realizada, o MAPA determina se o nó receberá um bloqueio temporário ou um bloqueio definitivo. Nos bloqueios temporários o nó é bloqueado, por um determinado intervalo de tempo, para executar qualquer funcionalidade da rede com o nó que o bloqueou, ou seja, qualquer pacote originado pelo nó bloqueado não será encaminhado. Já nos bloqueios definitivos, este bloqueio é permanente. Para identificar os nós bloqueados, é considerada a existência de um mecanismo seguro de identificação e autenticação dos nós, como o mecanismo apresentado em [Bouassida et al., 2006].

Para um nó receber uma punição máxima, ou seja, ser bloqueado definitivamente da rede, ele deve persistir em realizar eventos egoístas. O parâmetro que determina a quantidade de bloqueios temporários aplicados até o bloqueio definitivo é representado por k . Por exemplo, se $k = 2$, então o nó detectado é temporariamente bloqueado na primeira avaliação do MAPA e será definitivamente bloqueado quando a segunda avaliação for requisitada pelo SDE.

Outro parâmetro utilizado pelo MAPA é o limiar L , que determina o tempo de duração dos bloqueios temporários. O valor de L é atribuído de acordo com a tolerância desejada. Este limiar é comparado ao valor de p (Equação 1), calculado a cada avaliação realizada. A partir desta comparação, o tempo que o nó permanecerá bloqueado em cada bloqueio temporário é definido da seguinte forma:

- Se $L > p$, o nó é bloqueado durante um período de $t_{b(curto)}$ unidades de tempo;
- Se $L \leq p$, o nó é bloqueado durante um período de $t_{b(longo)}$ unidades de tempo.

3.3. Bloqueios Temporários e Bloqueios Definitivos

Para determinar a tolerância do número de eventos detectados até o nó ser definitivamente bloqueado, o SDE e o MAPA utilizam os parâmetros D e k . De acordo com a Figura 2(a), se $k = 1$, então o nó é definitivamente bloqueado no instante em que o D -ésimo evento egoísta é detectado, sem receber um bloqueio temporário anteriormente. Portanto, o nó detectado como egoísta tende a usar os recursos da rede por um menor intervalo de tempo. Na Figura 2(b), quando o valor de $k = 2$, o nó é temporariamente bloqueado uma vez, ou seja, $k - 1$ vezes antes de ser bloqueado definitivamente.

Além dos parâmetros citados anteriormente, o SDE e o MAPA utilizam o parâmetro I , que determina a quantidade de eventos normais que devem ser executados pelo nó para que o último bloqueio temporário seja desconsiderado. Quando o SDE

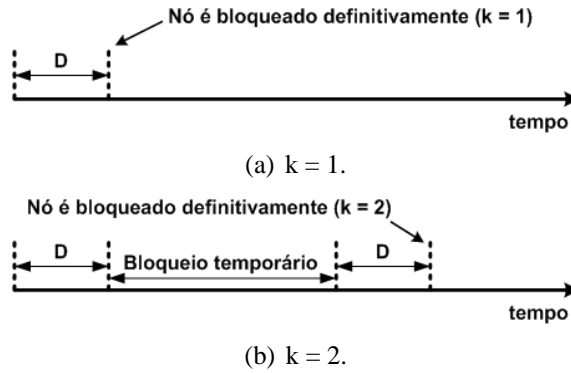


Figura 2. Intervalo de tempo da primeira detecção até o bloqueio definitivo.

observa que I eventos normais foram executados após um bloqueio temporário ter sido realizado, ele solicita que o MAPA desconsidere o último incremento realizado no contador de bloqueios temporários. Por exemplo, se $k = 3$ e o nó realizou I eventos normais após ter recebido o segundo bloqueio temporário, então este segundo bloqueio temporário será desconsiderado pelo MAPA. No entanto, se este mesmo nó executar mais I eventos normais, ele não terá o primeiro bloqueio temporário desconsiderado, pois o parâmetro I é determinado a partir das informações obtidas na última avaliação.

4. Análise Matemática

Nesta Seção são descritos os parâmetros utilizados na análise matemática, assim como as conclusões de acordo com os resultados obtidos. A análise matemática foi realizada na ferramenta Maple versão 11 [Char et al., 1991]. Para calcular a probabilidade de cada nó detectado ser um nó egoísta é usada uma função de probabilidade de massa baseada em uma distribuição binomial negativa, representada por $p_X(e)$ e calculada através da equação

$$p_X(e) = \binom{e-1}{D-1} p_{nó}^D (1 - p_{nó})^{e-D}; \quad (2)$$

ou seja, $p_{nó}$ representa a probabilidade do nó executar D eventos egoístas em e eventos observados. Com base nesta probabilidade, a média do número de eventos realizados até D eventos egoístas ocorrerem pode ser obtida por

$$e = \frac{D}{p_{nó}}. \quad (3)$$

Portanto, a probabilidade de punição calculada a cada D eventos egoístas detectados, dado um total de e eventos observados, é representada pela equação

$$P_p(e) = \sum_1^e p_X(e). \quad (4)$$

Finalmente, a probabilidade de bloqueio definitivo ao nó que recebeu $(k - 1)$ bloqueios temporários pode ser representada pela seguinte equação:

$$P_b(e) = \sum_1^e \binom{e-1}{kD-1} p_{nó}^{kD} (1 - p_{nó})^{e-kD}. \quad (5)$$

A partir da Equação 5 a análise matemática foi realizada. Para observar um possível caso de falso-positivo na punição, foi atribuído o valor de 0.05 para $p_{nó}$. A Figura 3 ilustra a quantidade de eventos observados antes do bloqueio definitivo ocorrer. Na Figura 3(a), ao assumir o valor de k igual a 1 é possível analisar a influência do parâmetro D no bloqueio definitivo. Assim, quanto maior for o valor de D , maior será a quantidade de eventos observados. Como k é ortogonal ao parâmetro D , a Figura 3(b) mostra que se o valor de $D > 1$ e os valores de k forem aumentados, então o total de eventos observados será ainda maior. Com esses resultados é possível analisar a influência dos parâmetros D e k na tolerância do nó em executar os bloqueios definitivos. Entretanto, não pode ser analisada a influência que o tempo exerce na punição dos nós e na eficiência da proposta. A partir destes resultados obtidos, foram realizadas simulações para observar a eficiência do SDE e do MAPA em uma rede ad hoc.

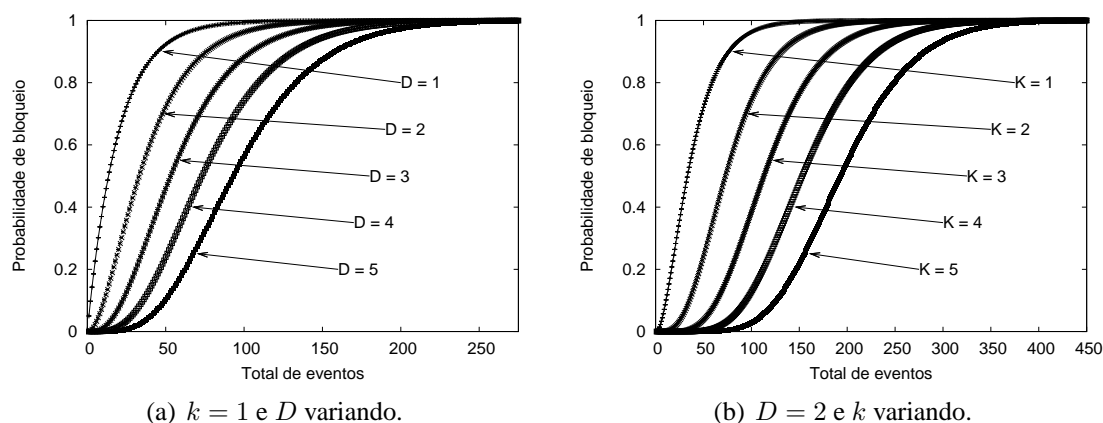


Figura 3. Probabilidade de bloqueio definitivo.

5. Ambiente de Simulação

Nesta Seção são mostrados os parâmetros utilizados e as premissas estabelecidas para a configuração da rede nos cenários simulados. Em seguida, são mostrados os resultados obtidos através destas simulações. As simulações foram realizadas no *Berkeley Network Simulator* versão 2.31 [Fall e Varadhan, 2006].

5.1. Parâmetros e Premissas

Para a simulação foram criados cenários nos quais a quantidade de nós geradores de tráfego foi variada. Desta forma, foi possível avaliar os mecanismos de detecção e punição em diferentes condições de carga da rede. Além disso, foi assumido que ataques de conluio não ocorrem na rede. No entanto, o SDE pode trabalhar em conjunto com um mecanismo de prevenção específico para este tipo de mau comportamento [Younis et al., 2005]. Os nós da rede foram configurados para não utilizarem informações de detecções realizadas por terceiros nas avaliações do MAPA. Portanto, todas as avaliações são realizadas somente através das informações de detecção observadas localmente.

Foram utilizados 81 nós nos cenários simulados, nos quais 10 desses nós eram escolhidos aleatoriamente para serem nós egoístas. Os nós foram dispostos em forma de grade de 9 linhas por 9 colunas. A dimensão desta grade foi de 180 metros para cada lado e o alcance do rádio de cada nó foi definido em 26 metros. O protocolo de roteamento

utilizado foi o *Dynamic Source Routing* (DSR) e o protocolo MAC foi o IEEE 802.11g com a taxa de 54 Mbps. O tráfego de dados utilizado foi o *Constant Bit Rate* (CBR), variando entre 200 kbps e 250 kbps. Foram executadas 50 rodadas, com o tempo de simulação igual a 250 segundos por rodada. A cada rodada os nós assumiam posições aleatórias na rede. Os resultados mostrados nos gráficos foram obtidos com um intervalo de confiança igual a 95%.

Dois tipos de descartes de pacotes foram simulados nos cenários analisados, seguindo os modelos de descarte executados por dois ataques comuns em redes ad hoc, conhecidos na literatura como buraco negro [Al-Shurman et al., 2004] e buraco cinza [Hu et al., 2005]. No ataque do tipo buraco negro o nó egoísta descarta todos os pacotes que chegam até ele e que deveriam ser encaminhados. Já no ataque do tipo buraco cinza os nós descartam os pacotes aleatoriamente selecionados que deveriam ser encaminhados. Para o ataque do tipo buraco cinza é sorteado um valor entre 0 e 20, que determina o número de pacotes que devem ser encaminhados até o descarte ser realizado. Por exemplo, caso seja sorteado um valor igual a 12, o nó atacante encaminhará 12 pacotes normalmente e descartará o próximo pacote que ele receber. Após realizar o descarte, o nó atacante repetirá este procedimento de sorteio. Este tipo de ataque tem como objetivo enganar os mecanismos de detecção de nós egoístas.

Para o limiar de tolerância L foi atribuído um valor igual a 0,2. Com esse valor pode-se dizer que o MAPA é mais tolerante, pois para ser executado um bloqueio temporário de maior período de tempo, a probabilidade do nó ser egoísta tem que ser maior do que 0,2. Os bloqueios temporários foram configurados para serem de 2 segundos quando $L > p$ e 4 segundos quando $L \leq p$. Para registrar os endereços dos nós bloqueados é utilizada uma lista. O tamanho dessa lista depende da capacidade computacional de cada nó. Caso a lista fique cheia, os endereços registrados há mais tempo são removidos para que os novos endereços dos nós detectados sejam registrados.

Para determinar o valor de I foi considerada a condição de que o SDE não conseguiria diferenciar os dois ataques de egoísmo na rede, já que o ataque do tipo buraco negro é considerado o caso extremo do ataque do tipo buraco cinza. Isso foi considerado porque o SDE poderia simplesmente usar um valor de $I = 1$ para não bloquear definitivamente os nós cooperativos em uma rede sob ataque de buraco negro, ou seja, como os nós egoístas descartam todos os pacotes no ataque de buraco negro, o SDE só precisaria observar um encaminhamento correto para desconsiderar o último bloqueio temporário enviado ao nó cooperativo. No entanto, o ataque de buraco cinza não permite esta facilidade na atribuição do valor de I , pois os descartes são realizados de forma aleatória. Neste contexto, o valor de I foi escolhido de forma a tornar a proposta adaptável às diferentes formas de comportamentos egoístas na rede. Portanto, o valor de I é determinado a partir dos valores dos parâmetros L , p , e e D de cada avaliação, como mostrado a seguir:

- Quando $L > p$ na avaliação atual, então I assume o valor de e .
- Quando $L \leq p$ na avaliação atual, então I assume o valor do resultado de $D \cdot e$.

Para analisar o impacto do SDE/MAPA, foram implementados o Watchdog e o Pathrater, que são mecanismos de referência na área de detecção de maus comportamentos em redes ad hoc. Além destes mecanismos, foi implementado também um mecanismo que bloqueia definitivamente os nós a cada detecção realizada, chamado de mecanismo Intolerante.

Na análise dos resultados foi observado que ambos os mecanismos de detecção, SDE e Watchdog, geram aproximadamente a mesma quantidade de detecções incorretas ao utilizarem o mesmo valor no limiar de detecção. Portanto, conclui-se que o principal fator causador do falso-positivo na punição está na relação entre a detecção realizada e a punição máxima aplicada ao nó. Por exemplo, no SDE/MAPA, está na relação entre a detecção de D eventos egoístas no SDE e o bloqueio definitivo em k incidências de avaliações no MAPA. Já no Watchdog/Pathrater está na relação entre a quantidade de detecções de eventos egoístas determinada pelo limiar do Watchdog e a redução de reputação no Pathrater.

Para comparar os resultados de falso-positivos e de detecções corretas, a quantidade de detecções e punições de eventos egoístas foi definida de forma equivalente para as propostas SDE/MAPA e Watchdog/Pathrater. Além disso, esta quantidade de detecções foi escolhida com o objetivo de analisar o quanto a tolerância em observar um determinado número de eventos egoístas pode afetar negativamente o desempenho da rede. Portanto, o valor do limiar de detecção utilizado na proposta do Watchdog/Pathrater foi igual a 10, ou seja, o Pathrater reduzirá a reputação do nó após 10 detecções realizadas pelo Watchdog. Para assumir com equivalência a quantidade de detecções utilizada pelo Watchdog/Pathrater, o SDE/MAPA pode ser analisado de quatro diferentes formas, variando os valores de k e D , ou seja: $k = 1$ e $D = 10$, não analisando a influência dos bloqueios temporários utilizados pelo MAPA; $D = 1$ e $k = 10$, aplicando um bloqueio temporário a cada detecção realizada pelo SDE; $k = 5$ e $D = 2$, executando uma punição temporária a cada duas detecções realizadas pelo SDE; e $k = 2$ e $D = 5$, realizando um bloqueio temporário a cada 5 eventos egoístas detectados.

Como se pretende analisar a influência de todos os parâmetros da proposta apresentada, foi escolhida a opção que atribui a quantidade mínima de bloqueios temporários, ou seja, $D = 5$ para o SDE e $k = 2$ para o MAPA. Desta forma, foi possível analisar a influência de um bloqueio temporário e um bloqueio definitivo, totalizando 10 eventos detectados para o nó ser evitado definitivamente, equivalente a quantidade de detecções utilizada pelo Watchdog/Pathrater.

5.2. Resultados

As Figuras 4 e 5 apresentam a quantidade de nós egoístas que recebem as punições corretamente e a taxa de falso-positivos gerada por cada proposta. Estes resultados foram divididos em cenários onde os nós egoístas executavam o descarte total de pacotes (buraco negro) ou o descarte aleatório de pacotes (buraco cinza).

De acordo com os resultados apresentados nas Figuras 4 e 5, a proposta que mais detectou nós egoístas na rede foi a proposta Intolerante. Entretanto, esta proposta foi considerada a mais ineficiente, devido à elevada quantidade de falso-positivos gerada. Ao observar a Figura 6, pode-se concluir que este mecanismo de detecção e punição não é recomendado em uma rede ad hoc, pois para conseguir punir uma maior quantidade de nós egoístas este mecanismo realiza diversas punições incorretas aos nós cooperativos da rede e, conseqüentemente, reduz o desempenho da rede.

Apesar de ter obtido uma maior quantidade de punições corretas, o Pathrater gerou uma maior quantidade de falso-positivos quando comparado com o MAPA. O Pathrater assume que cada nó da rede inicia com a reputação neutra, ou seja, igual a 0,5 e pode

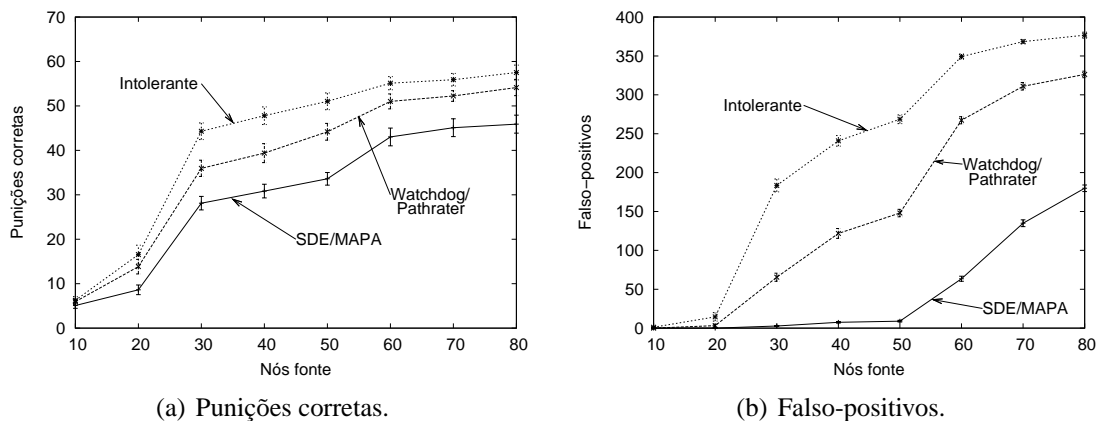


Figura 4. Rede ad hoc com buraco negro.

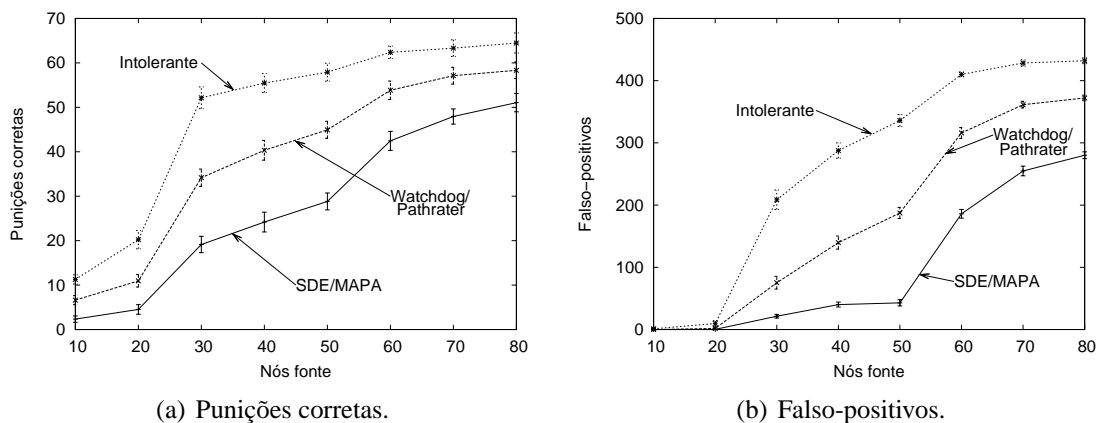


Figura 5. Rede ad hoc com buraco cinza.

atingir um valor máximo de 0,8. A partir destes valores estabelecidos, o Pathrater reduz a reputação do nó em 0,1 ao detectar uma quantidade de eventos egoístas determinada pelo limiar do Watchdog, ou seja, 10 eventos egoístas nas simulações realizadas. Para tentar minimizar a influência que os falso-positivos exercem no mecanismo de escolha de rotas, o Pathrater assume que se um nó não for detectado pelo Watchdog durante um período de 200 ms de simulação, então a sua reputação será incrementada em 0,01. O problema está na possibilidade do nó egoísta ter a sua reputação aumentada enquanto não está sendo usado, ou seja, a reputação do nó será aumentada em 0,1 a cada 2 segundos de simulação.

Ao analisar os resultados apresentados, é possível notar que o MAPA é mais eficiente na punição máxima aplicada ao nó monitorado em ambos os cenários, pois ele é capaz de bloquear corretamente uma quantidade significativa de nós egoístas gerando uma menor taxa de falso-positivos. Esta eficiência na detecção é consequência da avaliação que o MAPA realiza, considerando todos os eventos executados pelo nó monitorado, tanto os eventos normais como os eventos egoístas. Além da avaliação, outro fator que favorece a redução dos falso-positivos e o aumento das punições corretas é o parâmetro I . O parâmetro I faz com que os bloqueios definitivos sejam mais precisos, ou seja, se um nó foi bloqueado temporariamente devido a algum problema temporário da rede ad hoc, então ele poderá provar que é um nó cooperativo ao realizar I encaminhamentos de pacotes. Desta forma, os nós egoístas são detectados com uma maior facilidade, pois para

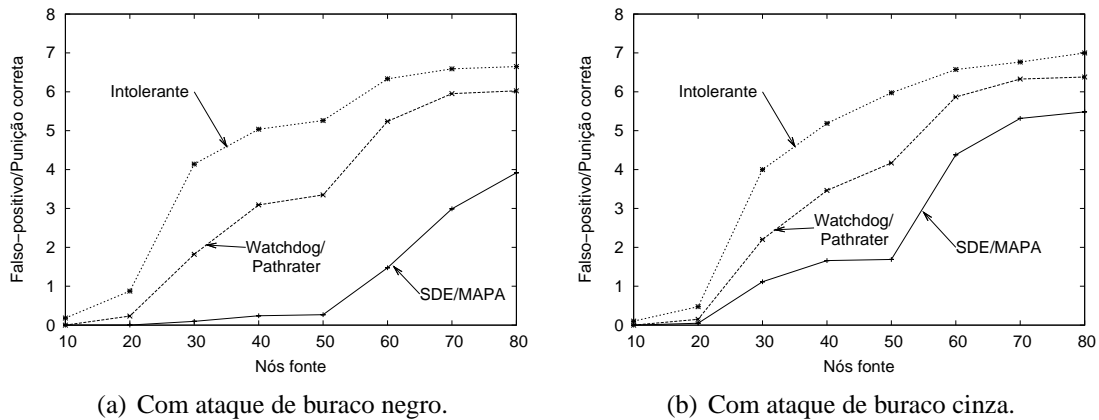


Figura 6. Quantidade de falso-positivos gerada para cada punição correta.

afetar significativamente o desempenho da rede ao tentar economizar os seus recursos ou atacar a rede, os nós egoístas terão que descartar os pacotes com uma maior frequência. Assim, quanto mais frequentes forem os descartes realizados, mais facilmente o nó egoísta será detectado.

O bloqueio temporário é um fator que influencia na menor quantidade de punições corretas realizadas pelo MAPA, pois a cada bloqueio temporário os nós egoístas são bloqueados da comunicação e removidos da tabela de rota dos nós que os detectaram. A queda na quantidade de detecções corretas ocorre porque os nós cooperativos começam a usar as rotas que evitam estes nós bloqueados, fazendo com que os nós egoístas sejam requisitados com uma menor frequência. Além disso, como o DSR armazena as rotas em *cache*, o nó egoísta poderá não ser usado por um tempo maior do que o período determinado pelo bloqueio temporário, pois as novas rotas utilizadas para evitá-lo poderão ser usadas por um longo período de tempo.

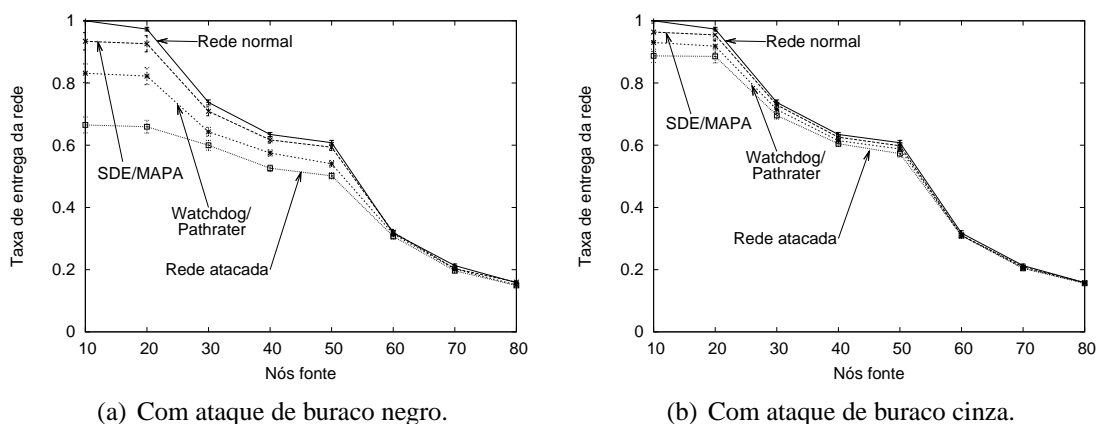


Figura 7. Taxa de entrega da rede.

Para analisar a taxa de entrega da rede foi simulado um cenário para servir de referência como o melhor caso, sem a presença de nós egoístas, observando somente a influência da saturação da rede na taxa de entrega. Para o pior caso foi simulado um cenário com 10 nós egoístas, que representam 12,5% do total de nós, e não foi usado nenhum

mecanismo de detecção e punição na rede. De acordo com Buchegger *et al*, quando mais de 10% dos nós da rede são maliciosos, o desempenho da rede começa a ser degradado significativamente [Buchegger e Boudec, 2002]. Ao observar os resultados apresentados, nota-se uma queda nos valores a partir do instante em que 20 nós estão gerando tráfego na rede. Analisando a Figura 7, este instante representa o início da saturação da rede.

A partir dos resultados obtidos na Figura 7, foi observado que tanto o SDE/MAPA quanto o Watchdog/Pathrater alcançaram melhores resultados quando comparados com uma rede que não utiliza um mecanismo de detecção e punição de nós egoístas, mesmo quando a rede está próxima da saturação. No entanto, o SDE/MAPA foi a proposta que mais se aproximou da curva ideal da taxa de entrega da rede. Isto é consequência da utilização de bloqueios temporários enviados aos nós detectados antes do bloqueio definitivo ser executado, fazendo com que o nó seja punido ao descartar a metade dos pacotes que o Pathrater necessitaria para punir um nó egoísta. Portanto, mesmo com a baixa saturação na rede, o Pathrater obteve um pior desempenho devido ao dobro de pacotes que precisariam ser descartados para que o nó egoísta tivesse a sua reputação reduzida. Além disso, os falso-positivos no Pathrater causam a redução na reputação dos nós cooperativos, fazendo com que a reputação de um nó cooperativo possa tornar-se menor ou igual à reputação de um nó egoísta. Como a reputação é uma métrica para a seleção de rotas, os nós egoístas continuam sendo usados nas rotas escolhidas pelo Pathrater. As Figuras 7(a) e 7(b) mostram a influência destes problemas na taxa de entrega da rede.

6. Conclusão

Neste artigo foi apresentado o MAPA, um mecanismo eficiente para evitar nós egoístas em redes ad hoc. Além do MAPA, foi implementado um mecanismo de detecção de nós egoístas, chamado de SDE. Estes dois mecanismos são usados em conjunto para detectar, avaliar e punir os nós egoístas em redes ad hoc. O principal objetivo do MAPA é reduzir a quantidade de falso-positivos nas punições aplicadas aos nós detectados pelo SDE, calculando a probabilidade de um nó detectado ser realmente um nó egoísta.

A partir dos resultados obtidos nas simulações, pôde-se concluir que ao utilizar o SDE/MAPA a taxa de entrega da rede foi aumentada em até 27% quando comparado com uma rede que não utiliza um mecanismo de detecção e punição de nós egoístas. Além disso, o SDE/MAPA também aumentou a taxa de entrega da rede em até 12% em relação ao Watchdog/Pathrater. Portanto, a proposta que se mostrou mais eficiente na detecção e punição de nós egoístas em redes ad hoc foi o SDE/MAPA.

Os principais fatores que influenciaram na eficiência do MAPA foram: os menores valores obtidos na razão entre a quantidade de falso-positivos gerada para cada punição aplicada corretamente (Figura 6); a menor influência que os falso-positivos exercem sobre o SDE/MAPA; e o uso do parâmetro I , que observa os comportamentos normais realizados, possibilitando que um nó cooperativo avaliado e punido prove que não é um nó egoísta. Além destes fatores, o MAPA não permite que os nós punidos se beneficiem dos nós da rede como acontece no Pathrater, pois o nó que é bloqueado temporariamente ou definitivamente está proibido de realizar qualquer comunicação com os nós que o bloquearam.

Referências

- Al-Shurman, M., Yoo, S.-M. e Park, S. (2004). Black hole attack in mobile ad hoc networks. Em *ACM-SE 42: Proceedings of the 42nd annual Southeast regional conference*, p. 96–97, New York, NY, USA. ACM Press.
- Anantvalee, T. e Wu, J. (2006). A survey on intrusion detection in mobile ad hoc networks. *Wireless/Mobile Network Security - Springer*, (7):170–196.
- Bouassida, M. S., Chrisment, I. e Festor, O. (2006). Efficient group key management protocol in manets using the multipoint relaying technique. Em *Proceedings of the International Conference on Networking (ICNICONSMCL'06)*, p. 64, Washington, DC, USA. IEEE Computer Society.
- Buchegger, S. e Boudec, J.-Y. L. (2002). Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. Em *Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing*, p. 403–410, Canary Islands, Spain. IEEE Computer Society.
- Buchegger, S. e Boudec, J.-Y. L. (2003). The effect of rumor spreading in reputation systems for mobile ad-hoc networks. Em *WiOpt'2003: Modeling and Optimization in Mobile, Ad hoc and Wireless Networks*.
- Char, B. W., Geddes, K., Leong, B., Monagan, M. e Watt, S. (1991). *Maple V Language Reference Manual*. Springer-Verlag, New York.
- Fall, K. e Varadhan, K. (2006). *The ns Manual*. UC Berkeley, LBL, USC/ISI, and Xerox.
- Hu, Y.-C., Perrig, A. e Johnson, D. B. (2005). Ariadne: a secure on-demand routing protocol for ad hoc networks. volume 11, p. 21–38, Hingham, MA, USA. Kluwer Academic Publishers.
- Johnson, D. B. e Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. Number 5, p. 153–181, Kluwer Academic Publisher.
- Kang, D.-K., Doug, F. e Vasant, H. (2005). Learning classifiers for misuse and anomaly detection using a bag of system calls representation. Em *Systems, Man and Cybernetics Information Assurance Workshop*, p. 118–125. IEEE Computer Society.
- Marano, S., Matta, V. e Tong, L. (2006). Distributed detection in the presence of byzantine attack in large wireless sensor networks. Em *Military Communications Conference, MILCOM 2006*, volume 1, p. 1–4.
- Marti, S., Giuli, T. J., Lai, K. e Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. Em *Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom)*, p. 255–265, New York, NY, USA.
- Younis, M., Ghumman, K. e Eltoweissy, M. (2005). Key management in wireless ad hoc networks: collusion analysis and prevention. *Performance, Computing, and Communications Conference. IPCCC 2005. 24th IEEE International*, p. 199–203.
- Yu, M., Kulkarni, S. e Lau, P. (2005). A new secure routing protocol to defend byzantine attacks for ad hoc networks. Em *13th IEEE International Conference on Network*, volume 2, p. 1126–1131.