# Aumentando a Segurança de Um Protocolo de Distribuição de Conteúdo P2P para MANETs

**Sidney Doria, Marco Aurélio Spohn**

[1] Departamento de Sistemas e Computação
Universidade Federal de Campina Grande – UFCG
Campina Grande – PB

{sidney, maspohn}@dsc.ufcg.edu.br

***Abstract.*** *Rogue peers are a concern because they decrease the utility of the resource-sharing systems, potentially towards to the system collapse. We are currently deploying Peer-to-MANET, a multicast peer-to-peer approach to distribute contents on mobile ad hoc networks. This work presents our efforts to improve trust, avoiding rogue and selfish peers in Peer-to-MANET. We employ a modified version of the Network of Favors as a decentralized reputation system to punish rogue peers activities. Through simulations in NS-2, we show that our solution minimizes download success rate by rogue peers, avoiding that maliciously peers cause resource depletion of other peers.*

***Resumo.*** *Nós desonestos são indesejáveis pois eles diminuem a utilidade dos sistemas de compartilhamento P2P, possivelmente até seu colapso. Atualmente estamos desenvolvendo o Peer-to-MANET (P2MAN), um protocolo de distribuição de conteúdo para MANETs. Este trabalho apresenta nossos esforços para aumentar a segurança do P2MAN, evitando nós desonestos e nós caroneiros. Empregou-se uma versão modificada da Rede de Favores, como sistema de reputação descentralizado, para punir atividades desonestas de nós. Através de simulações no NS-2, demonstramos que a solução proposta reduz a taxa de sucesso de download dos nós desonestos e evita que pares maliciosos tentem o esgotamento de recursos de outros pares.*

## 1. Introdução

A Internet é definida como um grupo global de redes de dispositivos computacionais interconectadas (e.g., redes domésticas, redes corporativas). Recentemente os usuários têm se valido de avanços nas tecnologias computacionais móveis e no aumento dos serviços móveis, de tal forma que o padrão de uso tem mudado e é possível vislumbrar um futuro onde a Internet será ubíqua, através da interconexão de muitos dispositivos computacionais pervasivos. Nessa trilha, os serviços celulares e as redes móveis são consideradas o futuro das infra-estruturas de rede [Stuckmann and Zimmermann 2009].

Uma rede móvel ad hoc (MANET) consiste em um conjunto de pares que desejam se conectar sem fio, mas sem se valer de nenhuma estrutura fixa de comunicação. A natureza móvel dos nós implica que eles podem agir como roteadores para outros nós, quando dois nós comunicantes estiverem a mais de um salto de distância. Defende-se na literatura que aplicativos que estejam sendo executados em uma MANET são essencialmente entre pares (P2P) por natureza. Provavelmente o problema das redes P2P mais discutido

é a distribuição de conteúdos entre os pares. Trabalhos recentes mostram os esforços para adaptar protocolos P2P populares, especialmente o BitTorrent [Cohen 2003], para o compartilhamento de dados em MANETs. Embora o BitTorrent e outros protocolos sejam conhecidos por eficiência na Internet, ele têm problemas de adaptação conhecidos quando funcionando sobre MANETs. Os protocolos P2P geralmente funcionam na camada de aplicação, empregando transmissões *unicast*, sem ciência da mobilidade dos nós. Por outro lado, MANETs geralmente fazem uso de transmissões por difusão não confiável, sobre um canal de rádio compartilhado, onde os nós são livres para se movimentar. Tais contrastes têm desafiado as pesquisas para otimização das redes P2P sobre as MANETs.

Atualmente, estamos desenvolvendo o protocolo *Peer-to-MANET* (P2MAN) de distribuição de conteúdo P2P para MANETs. P2MAN é um protocolo nativo, cuja inovação central está na abordagem *multicast* em malha de baixa sobrecarga, e por adotar um único grupo *multicast* para simplificar as operações de controle e reduzir sobrecarga. Além disso, foi projetado em uma abordagem holística, considerando as restrições típicas das MANETs, ao mesmo tempo que tenta se valer das suas peculiaridades (e.g., escala e propósito restritos, roteamento *multicast* em malha). Os primeiros resultados [Doria and Spohn 2009] do P2MAN são animadores, pois indicaram que P2MAN distribui conteúdos em MANETs de forma escalável e eficiente

Apesar dos potenciais benfícios do uso de redes P2P como o P2MAN, os nós desonestos são uma procupação, visto que eles podem degradar o desempenho do sistema, potencialmente até o colapso. Este trabalho visa aumentar a segurança do P2MAN, desencorajando as atividades de nós desonestos que tentam reduzir o desempenho do sistema de distribuição de conteúdo da seguinte maneira: (a) enviando pedaços de conteúdos falsos para outros nós, (b) com comportamento egoísta, sendo caroneiros. Propõe-se uma modificação da Rede de Favores [Andrade et al. 2004] (NoF), que originalmente foi projetada para redes P2P de compartilhamento de CPU em grades computacionais, como um mecanismo de reputação descentralizado para o P2MAN. Através de simulações no NS-2 [NS-2 2010], demonstra-se que a solução proposta minimiza as atividades dos nós maliciosos citados.

O restante deste artigo está organizado como segue. Na Seção 2 confronta-se o estado da arte com esta abordagem. Na Seção 3 a solução é detalhada. Na Seção 4 é detalhado o estudo baseado em simulações e os resultados são apresentads. Por fim, a Seção 5 conclui este trabalho e apresenta trabalhos futuros.

## 2. Trabalhos Relacionados

### 2.1. Distribuição de Conteúdo P2P sobre MANETs

Distribuir conteúdos com eficiência em MANETs é um problema difícil. Já foram empregados diversos protocolos P2P para realizar a distribuição de conteúdos. Trabalhos anteriores adaptaram algoritmos P2P populares em MANETs [Kortuem et al. 2001, Klemm et al. 2003, Androutsellis-Theotokis and Spinellis 2004]. Particularmente, destacam-se os esforços para adaptar o BitTorrent sobre MANETs [Krifa et al. 2009a, Krifa et al. 2009b, Sbai et al. 2008, Rajagopalan et al. 2006, Sbai and Barakat 2009, Souza and Nogueira 2008, Quental and Gonçalves 2010]. Um protocolo popular na Internet como o BitTorrent pode ter uma melhor aceitação dos usuário de MANETs, visto

que seu tempo de treinamento seria menor, considerando que há uma maior probabilidade de que alguns usuários já tenham experiência prévia com o protocolo. Entretanto, muitos protocolos de distribuição de conteúdo P2P apresentam problemas técnicos de adaptação quando executando sobre MANETs, como explicado a seguir.

Por exemplo, as redes populares de compartilhamento de conteúdo P2P foram originalmente projetadas para a Internet (i.e., escala global, milhões de nós) e as MANETs típicas têm escala de dezenas de nós. Em atenção à escala, alguns trabalhos [Ding and Bhargava 2004, Y. Charlie Hu and Pucha 2003] adaptaram a *Distributed Hash Table* (DHT) e outras tecnologias de localização das redes P2P para as MANETs. Também, as MANETs têm problemas intrísecos de infra-estrutura que os sistemas P2P não têm como preocupação. Por exemplo, o BitTorrent emprega *unicast*, o que é custoso para uma MANET devido à sobrecarga gerada por *handshakes* em camadas inferiores.

Ademais, protocolos P2P como o BitTorrent adotam o TCP como protocolo de transporte. Os problemas de desempenho do TCP em MANETs já foram demonstrados exaustivamente na literatura [Holland and Vaidya 1999] (e.g., o TCP interpreta as perdas de pacotes no enlace sem fio como contenção e reduz a velocidade da transmissão). O uso do TCP nas transmissões pode portanto degradar o desempenho do sistema de distribuição de conteúdos. Em atenção a esse problema, Anastasi et al. desenvolveram recentemente o TPA [Anastasi et al. 2009], um protocolo de transporte confiável mais eficiente do que o TCP em MANETs, que adota uma abordagem entre camadas. Mesmo considerando tais avanços recentes com protocolos de transporte para MANETs, ainda haveria a necessidade de adaptar o BitTorrent ou uma variante do protocolo para o TPA.

De fato, para contornar problemas de desempenho, novas pesquisas vêm tentando abordagens entre camadas, que estabelecem comunicação direta entre a camada de aplicação e as camadas inferiores, ao custo de contrariar o propósito das modelagens por camadas. Por exemplo, em [Y. Charlie Hu and Pucha 2003] os autores propõem um protocolo de roteamento que se apóia em uma rede P2P auxiliar sobreposta, de modo que as descobertas de rotas ficam limitadas a $O(logN)$. Os autores em [Conti et al. 2004] criaram uma camada adicional que se comunica com as demais camadas de rede, que consolida informações sobre o *status* da rede. Além disso, conjecturam *não ser possível* realizar certas operações em MANETs com eficiência (e.g., economia de energia nas transmissões) com o paradigma de camadas independentes, mas não reuniram provas para embasar tal afirmação. Em [Kozat et al. 2004] os autores também projetaram uma camada adicional que coleta informações da rede.

Mais recentemente, outros trabalhos utilizaram abordagens entre camadas, de redes P2P sobrepostas, para alcançar resultados otimizados para tarefas como roteamento *unicast* e *multicast* e distribuição de conteúdos [Passarella et al. 2006, Delmastro et al. 2008, Lee et al. 2006, Sbai and Barakat 2009]. Para preservar o modelo de camadas, optou-se por não utilizar uma abordagem entre camadas no desenvolvimento do P2MAN.

### 2.1.1. Peer-to-MANET

*Peer-to-MANET* (P2MAN) é um protocolo baseado em *multicast* para distribuição de conteúdo entre-pares em redes *ad hoc* móveis. Foi projetado para mitigar as limitações das MANETs e obter vantagem dos conceitos das redes P2P. P2MAN usa grupos *multicast* para entregar conteúdos e um grupo *multicast* especial, denominado *Canal Público*, para todas as operações de controle.

Quando um nó P2MAN inicia, junta-se ao *Canal Público* (CP) para poder trocar mensagens de controle. Todos os nós que desejam compartilhar conteúdo devem ser membros do CP. Não há servidor com informações para localização de conteúdos nem tais informações são copiadas (i.e., mantidas em *cache*) pelos nós na rede. Em vez disso, para localizar um conteúdo, um nó consulta o *Canal Público* sem a necessidade de inundar a rede com mensagens de controle. Caso algum nó ativo tenha o conteúdo, este será alcançado através do CP e uma resposta será retornada também via CP. A resposta também traz metadados gerados pelo nó proprietário do conteúdo, com informações detalhadas sobre o conteúdo.

Como em muitas redes P2P, P2MAN fraciona o conteúdo para a entrega. O nó proprietário decide como o objeto será dividido em pedaços e faz uma representação do conteúdo através de um mapa de *bits* (em que cada *bit* representa um pedaço do conteúdo). O proprietário também decide que grupo *multicast* será usado para transmitir o conteúdo. Os metadados são criados pelo nó proprietário, contendo as informações necessárias para guiar os nós solicitantes. Após receber a resposta, o nó solicitante junta-se ao grupo *multicast* anunciado pela fonte e envia uma mensagem de autorização ao Canal Público. Ao receber uma mensagem de autorização, o proprietário do conteúdo pode iniciar a transmissão.

Assumindo-se a adoção de um protocolo de roteamento *multicast* sem entrega confiável (e sem um protocolo de transporte multicast), a garantia de entrega é realizada na camada de aplicação, através de um mecanismo de retransmissão denominado *Modo de Reparação*. No modo de reparação, um nó pode solicitar os pedaços que ainda não recebeu. O proprietário então retransmite os pedaços que faltam. Enquanto houver pedaços faltando, novos pedidos e retransmissões ocorrerão, até que o nó solicitante receba todos os pedaços. A Tabela 1 resume as escolhas de projeto do P2MAN, confrontando-as com as abordagens comuns da literatura e mostrando as vantages esperadas.

### 2.1.2. Protocol for Unified Multicasting through Announcements (PUMA): uma breve descrição

Há uma preocupação da comunidade científica a respeito da sobrecarga gerada para se manter uma malha *multicast* em uma MANET, especialmente na presença de particionamentos de rede ou alta mobilidade. Esta procupação é a razão principal da escolha do protocolo *multicast Protocol for Unified Multicasting through Announcements* (PUMA) [Vaishampayan and Garcia-Luna-Aceves 2004] para este trabalho. PUMA foi escolhido como protocolo de roteamento para o P2MAN porque demonstrou-se que o PUMA tem baixa sobrecarga e manutenção rápida da malha, além de superar o desempenho dos protocolos *multicast* mais representativos.

**Tabela 1. P2MAN: Escolhas de Projeto.**

| Literatura | P2MAN | Vantagens |
|---|---|---|
| DHT adaptada ou inundação | Canal Público | Nativo, pouca sobrecarga, bem adaptado à escala |
| *Unicast* com mecanismo de incentivo | *Multicast* | Nativo, simples, sem necessidade de mecanismo de incentivo, menor sobrecarga de *handshakes* |
| TCP | UDP | Menos sobrecarga, desempenho máximo do transporte (menor degradação) |
| TCP | Modo de Reparação | Menos sobrecarga, confiabilidade por reparação oportunística |

PUMA é um protocolo de roteamento *multicast* baseado em malha, com a montagem da malha orientada aos receptores. Por padrão, o primeiro receptor de um grupo *multicast* se torna o líder do grupo (i.e., *core*). Caso múltiplos nós se juntem simultaneamente a um mesmo grupo, o nó com o maior endereço IP será eleito o líder do grupo. O que faz o PUMA simples e muito eficiente é sua baixa sobrecarga de pacotes de controle. Um único pacote de controle, denominado *anúncio multicast*, é usado para manter a malha. Além disso, na ocorrência de múltiplos grupos e múltiplas malhas, os pacotes de controle podem ser agrupados em um único anúncio. PUMA não requer quaisquer protocolos *unicast* para funcionar. Todas as transmissões são feitas por difusão. Apesar de usar difusões não confiáveis, a malha formada pelo PUMA introduz uma redundância aceitável. No PUMA, a malha inclui apenas membros do grupo *multicast* e os nós que interconectam os seus membros. Assim, as difusões ficam limitadas ao escopo da malha.

À medida que anúncios se propagam pela malha, os nós aprendem o caminho mais curto até o líder. Desta forma, pacotes de dados podem ser roteados rapidamente para o líder. No caminho para o líder, duas coisas podem acontecer a um pacote de dados: (a) o pacote percorre a rede até que alcance finalmente o líder, ou (b) pode alcançar um nó membro da malha antes do líder. De qualquer forma, quando um pacote chega até um membro da malha, será difundido apenas dentro da malha. O líder não é um ponto único de falha porque, em caso de falha, ocorre uma rápida eleição através de um algoritmo distribuído muito eficiente.

## 2.2. Mecanismos de Reputação Entre Pares

Um mecanismo de reputação para sistemas entre pares é uma técnica para guardar o comportamento prévio de pares para ser usado como guia para outros pares da rede. Um desafio que tais mecanismos têm de enfrentar é reaver as informações coletadas sobre os nós de forma confiável, visto que nós maliciosos podem adulterar as informações que armazenam. Em [Aberer and Despotovic 2001], de forma antecipada, os autores apresentam um mecanismo de reputação especificamente projetado para redes P2P. O algoritmo Eigen [Kamvar et al. 2003] mantém uma pontuação global para cada par $i$, computada através da pontuação de $i$ dada por todos os outros pares, aplicado o peso das próprias pontuações globais de tais pares. Alguns pares especiais computam, armazenam e replicam os valores globais de reputação para um par. Os pares especiais encontram os pares

para os quais devem manter a pontuação, e são encontrados por pares que necessitam dessa informação, através de uma tabela *hash* distribuída.

Entretanto, essas abordagens são sucetíveis aos ataques em conluio que podem acontecer. Nós desonestos podem conspirar para reduzir a reputação de nós honestos da rede. Chun et al. propuseram uma arquitetura [Chun et al. 2003] para aumentar a segurança de trocas entre nós baseada em troca de *tickets*. Esta arquitetura, porém, assume uma infra-estrutura de chaves criptográficas e o estabelecimento de relações de confiança entre os pares para que seja possível o acesso aos recursos. Em P2PRep [Cornelli et al. 2002], cada par armazena informação sobre suas próprias interações com outros pares. Para assegurar a confiabilidade dessa informação, P2PRep lança mão de votação para obtenção de opiniões sobre a reputação de um par. Também, P2PRep usa heurísticas para encontrar blocos de potenciais pares maliciosos e uma infra-estrutura de chaves criptográficas para verificar as identidades de pares envolvidos numa transação.

### 2.2.1. A Rede de Favores

A idéia central da *Rede de Favores* (NoF) é que os usuários que são os maiores colaboradores de recursos da rede devem receber maior prioridade de acesso aos recursos disponíveis na rede. Esse princípio segue como um guia para a distribuição balanceada dos recursos disponíveis entre os usuários e, portanto, como um incentivo para a colaboração. A NoF contorna a necessidade de prover confiabilidade dos dados coletados, visto que não agrega valores globais de reputação a um par. Em vez disso, pares somente usam as informações de reputação envolvendo suas próprias interações entre pares. Essa informação é armazenada localmente no nó. Estratégias maliciosas baseadas em mentiras sobre o comportamento de nós terceiros (e.g., ataques em conluio) não podem ser aplicadas.

Na NoF, alocar um recurso a um par que o requisita é prestar um favor, e o valor do favor é o valor do trabalho realizado para compartilhar o recurso ao par solicitante. Cada par mantém um registro local do total de favores prestados a e recebidos de cada par com quem tenha realizado transações no passado. Cada vez que um par presta um favor ou recebe um favor, ele atualiza o número apropriado. Um par calcula a reputação local de outro par baseando-se nesses números, de forma que um par que tem lhe prestado muitos favores e recebido poucos terá uma reputação maior. Um par usa a reputação atual para decidir para que outros pares ele prestará favores, quando tiver de arbitrar entre mais de um solicitante de recurso. Portanto, sempre que houver contenção de recursos, os pares com maior reputação terão prioridade.

Seja $v(A, B)$ o valor total de recursos doados do nó $A$ para o nó $B$ no passado do sistema, o nó $A$ calcula $r_A(B)$, a reputação do nó $B$, usando a Equação 1:

$$r_A(B) = max\{0, v(B, A) - v(A, B) + log(v(B, A))\} \quad (1)$$

Usando 1, o nó $A$ calcula a reputação do nó $B$ com o número de favores que $A$ recebeu de $B$, menos o número de favores que $B$ recebeu de $A$. Usando uma função de reputação não-negativa é possível evitar a priorização de nós que maliciosamente tro-

cam de identidade para se beneficiar daqueles nós que consumiram mais recursos do que contribuiram. O termo sub linear $log(v(B, A))$ foi introduzido na equação para que se possa distinguir entre nós que trocam de identidade maliciosamente e que nunca doaram quaisquer recursos de um nó $B$ que colaborou para $A$ no passado, mas recebeu o mesmo montante de favores que doou para $A$. Também, é possível identificar um colaborador mesmo se o colaborador tenha consumido mais recursos do que tenha doado, visto que ele já doou recursos no passado.

## 3. Aumentando a Segurança no P2MAN

Para aumentar a segurança do P2MAN, adotou-se uma versão modificada da Rede de Favores para computar a pontuação de reputação dos nós, baseada na interação entre esses nós, para identificar e desencorajar as atividades de nós desonestos. Foram combinados o mecanismo de pontuação da NoF, um mecanismo de *Lista Negra* e o mecanismo de envio de conteúdos do P2MAN para aumentar a robustez do sistema, sistematicamente evitando que nós maliciosos recebam pedaços de conteúdo dos seus vizinhos.

Como em trabalhos anteriores, assumindo-se que se o sistema possui algum mecanismo pelo qual seja possível ao nó identificar nós colaboradores com precisão suficiente, e que os colaboradores reconhecidos recebam prioridade nos recursos, então o nós pagarão para serem colaboradores. Como uma conseqüência esperada, os nós modificarão suas estratégias de colaboração e o sistema evoluirá para um estado em que não haverá nós desonestos. A abordagem usada neste trabalho é detalhada a seguir.

### 3.1. Adaptando a Rede de Favores ao P2MAN

De forma similar à NoF, um nó P2MAN atribui uma pontuação para cada nó vizinho com o qual ele interage, e armazena essa informação localmente, de acordo com os favores que o nó recebe ou doa. No P2MAN, transmitir um pedaço de um conteúdo requisitado é prestar um favor. Entretanto, um nó proprietário P2MAN deve decidir se vai ou não responder a requisições de conteúdo. Essa decisão é baseada num fator denominado *Saúde*. A Saúde é uma metáfora que representa a noção intuitiva de disponibilidade de uma coleção de recursos do nó. Por exemplo, como os nós móveis possuem recursos de energia limitados, deve-se poupar a energia disponível. Sendo assim, as transmissões são consideradas custosas. Para um nó que tenha a sua fonte de energia a plena carga é mais conveniente transmitir conteúdos do que para um nó com uma fonte de energia próxima da exaustão.

Seja $\rho \in \Re : 0 \leq \rho \leq 1$ a probabilidade de que um nó proprietário $A$ compartilhará seus conteúdos quando requisitado, $\theta_A$ seja o limiar de saúde do nó $A$ e $r_A(max)$ a máxima reputação de nós armazenada no nó $A$, define-se $\rho$ na Equação 2, como a seguir.

$$\rho = min(1, (\theta_A + \theta_A . \frac{r_A(B)}{r_A(max)})) : 0 \leq \theta \leq 1 \quad (2)$$

Assumindo que os nós P2MAN sabem medir seu estado interno, de forma a poder computar sua saúde, quando um nó P2MAN $A$ estiver plenamente *saudável*, $\theta_A$ será $1$. Da mesma forma, quando $A$ tiver exaurido seus recursos, $\theta_A$ será $0$. O segundo termo na Equação foi introduzido para comparar a reputação de um nó solicitante com a melhor

reputação armazenada no nó $A$. O objetivo deste segundo termo é aumentar a probabilidade de que um bom colaborador receba pedaços de conteúdo. Assim, quando um nó iniciante (i.e., com reputação nula) requisita um conteúdo ao nó $A$, a probabilidade de o nó $A$ atender à requisição depende somente do seu limiar de saúde (i.e., $\theta_A$). Se em algum momento o nó $A$ estiver plenamente saudável, ele atenderá às requisições de compartilhamento de conteúdo, mesmo a nós iniciantes na rede. Entretanto, quando o melhor colaborador (i.e., $rA(max)$) requisitar um conteúdo ao nó $A$, a probabilidade de o nó $A$ atender a sua requisição será duas vezes maior do que a probabilidade de $A$ atender um nó iniciante (i.e., $max(1, 2\theta_A)$). Essa abordagem captura a idéia de esforço de um nó para garantir a reciprocidade de favores aos seus colaboradores.

A NoF original não resolve o problema de ataques maliciosos por nós desonestos que desejam reduzir o desempenho do sistema através do envio de pedaços falsos de conteúdo para os vizinhos que solicitam. Destaca-se que o impacto da transmissão de pedaços falsos para pares de uma rede P2P de distribuição de conteúdo pode ser ordens de magnitude pior se a rede P2P estiver sobre uma MANET. Isso se deve ao fato de que as MANETs utilizam roteamento salto a salto em ambiente dinâmico. A medida que um pedaço falso atravessa uma MANET, muitos nós podem ser requisitados a repassar os pacotes que compõem o pedaço, desde o nó proprietário até o destino. No caso de um ataque em conluio, uns poucos nós desonestos podem saturar uma MANET inteira, enviando pedaços falsos para nós diametralmente opostos na rede.

Para contornar esse problema, foi feita uma modificação na NoF, adicionando um mecanismo de *Lista Negra*. O objetivo da lista negra é punir imediatamente quaisquer nós P2MAN que enviem pedaços falsos para os nós solicitantes. Dessa forma, assim que um pedaço falso é recebido por um nó solicitante, ele incorpora o nó em sua lista negra, evitando responder às requisições futuras de tal nó (e.g., resposta a requisições de conteúdo, envio de pedaços) por um período programado. O período programado pode ser ajustado convenientemente pelo usuário do sistema. Para calcular $r_A(B)$, assume-se que um nó P2MAN tem informações confiáveis sobre $v(B, A)$ e $v(A, B)$.

Particularmente, assume-se que um nó P2MAN genérico é capaz de: (i) medir o número de favores providos por outro nó P2MAN, e (ii) verificar se o favor prestado é válido ou não (i.e., que os dados enviados são válidos).

### 3.2. Coibindo Atividades de Nós Desonestos

Por se tratar de um protocolo P2P *multicast* para MANETs, uma estratégia do P2MAN é evitar as múltiplas transmissões de conteúdo um para um, o que reduz a saturação da transmissão. Em vez disso, P2MAN reforça a seleção de únicos nós transmissores para cada conteúdo, por um processo de seleção de nós proprietários. Note-se que, como parte da implementação do P2MAN, uma requisição de conteúdo deve ser realizada através de uma mensagem para o Canal Público (i.e., grupo *multicast* especial).

Ao receber uma mensagem de solicitação, um nó proprietário pode responder ao Canal Público, se desejar, informando que possui o conteúdo e enviando os metadados com detalhes do conteúdo (e.g., fracionamento, grupo *multicast*). Todos os nós proprietários podem responder às solicitações no Canal Público. Após analisar as múltiplas opções, o nó solicitante autoriza um único nó proprietário a enviar pedaços, através de uma mensagem específica. Particularmente, o processo de seleção e envio de pedaços é

relevante para evitar atividades maliciosas no P2MAN, como explicado a seguir.

Supondo que um nó desonesto deseja enviar pedaços falsos para obter vantagem desonesta na rede, ou para reduzir o desempenho do sistema, ele pode responder positivamente a quaisquer requisições de conteúdo na rede. Para completar o ataque, o nó malicioso deve aguardar por uma autorização, visto que pedaços enviados por nós não autorizados são ignorados pelo solicitante, que nem estará associado ao grupo *multicast* correto. Quando receber uma autorização, o nó poderá enviar os pedaços falsos ao grupo *multicast* alvo. Quando o primeiro pedaço falso for recebido pelos nós solicitantes do grupo, o remetente será incluído nas listas negras dos participantes, que se desconectarão imediatamente do grupo *multicast* indicado pelo nó malicioso.

Por um período programado, os nós atacados vão ignorar as comunicações seguintes do nó atacante incluído na lista negra. Defende-se que esta abordagem é suficiente para minimizar as atividades maliciosas de nós desonestos, evitando que haja transmissão de pedaços para esses nós desonestos. A atividade dos nós caroneiros (*free riders*) será minimizada também, visto que tais nós terão baixa reputação na rede, como explicado a seguir.

Supondo agora que um nó desonesto deseja ser um caroneiro, não respondendo a quaisquer solicitações. A partir daí, sua reputação não aumentará com o tempo. Mesmo no caso de um ataque de mudança de identidades, o nó desonesto permanecerá com a reputação nula, exatamente como um nó iniciante.

## 4. Avaliação

Nesta Seção o desempenho da solução proposta é medido, apresentando-se os resultados de simulações que mostram que as modificações aplicadas à Rede de Favores são suficientes para evitar que nós maliciosos tenham êxito e levem um sistema P2MAN ao colapso.

### 4.1. Cenário de Simulação

Foram realizadas simulações em um cenário típico de MANETs, no simulador Network Simulator $2.34$. Foi modelada uma rede com $100$ nó móveis homogêneos. No modelo proposto, é possível ajustar o período programado de penalidade, o número de pares que enviam pedaços falsos, e o número de pares caroneiros. Os resultados são representados por uma média de $20$ rodadas de simulação, com um intervalo de confiança de $95\%$.

Os nós estão espalhados aleatoriamente sobre o terreno e movem-se de acordo com o modelo de mobilidade *Random Waypoint* (excluindo-se a velocidade mínima $zero$). Os conteúdos compartilhados são fracionados em pedaços de $1000$ $Bytes$, de acordo com as recomendações de tamanho de pacote UDP de Lee et al. [Lee et al. 2002]. O tamanho do conteúdo é de $100$ $KBytes$. Foram considerados $70$ nós solicitantes. Desses, $25$ nós são caroneiros, $25$ nós são desonestos e enviarão pedaços falsos, e $20$ nós são honestos. A Tabela 2 mostra os parâmetros de configuração do P2MAN.

Quando a simulação inicia, todos os nós têm $zero$ favores e, em algum momento, os nós solicitantes iniciam a descoberta de conteúdos na rede. Quando o primeiro nó honesto inicia solicitações, os respectivos nós proprietários respondem, se estiverem com saúde suficiente. Então, nós proprietários saudáveis e autorizados enviam pedaços para

**Tabela 2. Parâmetros de Simulação do P2MAN.**

| Parâmetro | Descrição |
|---|---|
| Simulador | 2.34 |
| Número de Rodadas | 20 |
| Tamanho do Terreno | $1000x1000$ |
| Modelo de Mobilidade | Random Waypoint |
| Tempo de Pausa | $0\ s$ |
| Alcance de Rádio | $250\ m$ |
| Largura de Banda | $2\ Mbps$ |
| Protocolo de Enlace | $802.11DCFMode$ |
| Velocidade Máxima | $5\ m/s$ |
| Tamanho do Pedaço | $1000\ Bytes$ |
| Tamanho do Conteúdo | $100\ KBytes$ |
| Período de Penalidade | $300\ s$ |
| Limiar de Saúde ($\theta$) | 0.8 |
| Número de Nós | 100 |
| Número de Nós Proprietários | 30 |
| Número de Nós Solicitantes | 70 |
| Número de Caroneiros (i.e., não colaboram) | 25 |
| Número de Nós Desonestos (i.e., enviam pedaços falsos) | 25 |
| Número de Nós Honestos (i.e., colaboradores) | 20 |

os solicitantes. Ao receber e validar os pedaços, os solicitantes então incrementam suas tabelas de reputação. De forma similar, quando o primeiro nó solicita conteúdos, nós proprietários saudáveis também respondem, visto ser impossível determinar quais nós são caroneiros ou maliciosos antes das interações. Portanto, o resultado esperado é que ambos nós honestos e maliciosos recebam pedaços nas primeiras interações e, após um período de tempo, os colaboradores serão pontuados e conseqüentemente privilegiados. Nós maliciosos permanecerão com reputação nula. Quando nós maliciosos iniciarem as respostas com conteúdos falsos, todos os solicitantes envolvidos devem incluí-lo em suas listas negras. Dessa forma, o resultado esperado é que, em um período curto de tempo, os nós desonestos sejam incapazes de enviar pedaços falsos com êxito e suas reputações permaneçam nulas para todo o sistema, visto que eles não colaboram.

A duração das simulações é de $5000s$. Um nó solicitante pede um conteúdo por vez e quando recebe integralmente um conteúdo, uma nova requisição é feita imediatamente, de forma que o sistema está em constante atividade. A Figura 1 mostra os resultados das simulações, com a taxa de sucesso de *download* dos nós honestos, nós desonestos e nós caroneiros, coletados a cada $500s$ de simulação. Assume-se que os nós não mudam de estratégia, de forma que um nó honesto permanece honesto durante toda a simulação. Note-se que, mesmo entre nós honestos, a taxa de sucesso de *download* não é máxima, visto que o *download* de alguns pedaços pode falhar.

A Figura 1 mostra uma redução substancial na taxa de sucesso dos nós desonestos. Também, os nós caroneiros têm suas atividades minimizadas após um período. Nas simulações foram usados conteúdos pequenos para *download*. Ressalte-se que, quando o *download* de um conteúdo é concluído, um novo *download* inicia. Portanto, para novos

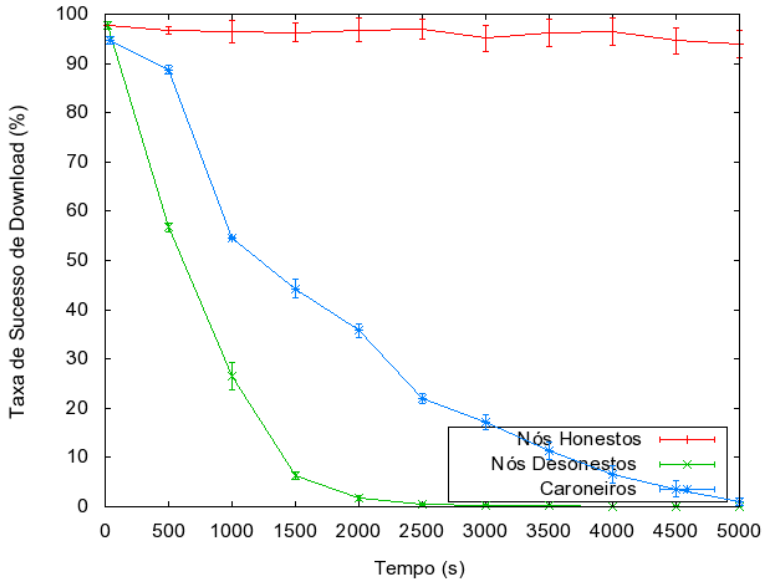


**Figura 1. Taxa de Sucesso de Download de Nós Honestos, Nós Desonestos, e Nós Caroneiros.**

conteúdos, potencialmente novos proprietários são requisitados e os nós caroneiros podem se beneficiar recebendo alguns pedaços desses novos nós proprietários, o que explica a inclinação mais suave no decaimento do gráfico, até serem finalmente detectados por uma quantidade suficiente de nós para serem coibidos.

## 5. Conclusão

Este trabalho tratou do problema de aumentar a segurança do P2MAN, que é um protocolo de distribuição de conteúdo P2P para MANETs, minimizando as atividades de nós caroneiros e nós desonestos. A abordagem utilizada foi uma adaptação da Rede de Favores como mecanismo de reputação distribuído. Na versão modificada foi incorporada uma funcionalidade de lista negra para auxiliar a NoF a combater os nós desonestos no P2MAN. Também, foi definido o conceito de saúde do nó, em um esforço para modelar as restrições de recursos dos nós móveis sem fio no contexto de distribuição das MANETs. Com essa modelagem foi possível evitar o problema de drenagem maliciosa de recursos por nós desonestos.

Através do simulador NS-2, foi demonstrado que a abordagem proposta é suficiente para minimizar as atividades de nós maliciosos, reduzindo a taxa de sucesso de *download* dos nós desonestos a quase zero.

Pretende-se estender este trabalho, incluindo a informação de energia e outras restrições de recursos nas simulações e realizando análises mais completas para medir o impacto da saúde do nó na habilidade do P2MAN de distribuir conteúdos em MANETs.

## Referências

Aberer, K. and Despotovic, Z. (2001). Managing trust in a peer-2-peer information system. In *Proceedings of the tenth international conference on Information and knowledge management*, pages 310–317, New York, NY, USA. ACM.

Anastasi, G., Ancillotti, E., Conti, M., and Passarella, A. (2009). Design and performance evaluation of a transport protocol for ad hoc networks. *The Computer Journal Advance*, 52:186–209.

Andrade, N., Brasileiro, F., Cirne, W., and Mowbray, M. (2004). Discouraging free riding in a peer-to-peer cpu-sharing grid. *High-Performance Distributed Computing, International Symposium on*, 0:129–137.

Androutsellis-Theotokis, S. and Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. *ACM Computer Surveys*, 36(4):335–371.

Chun, B., Fu, Y., and Vahdat, A. (2003). Bootstrapping a distributed computational economy with peer-to- peer bartering. In *1st Workshop on Economics of Peer-to-Peer Systems*.

Cohen, B. (2003). Incentives build robustness in bittorrent. In *Workshop on Economics of Peer-to-Peer Systems*, Berkeley, CA, EUA.

Conti, M., Gregori, E., and Turi, G. (2004). Towards scalable p2p computing for mobile ad hoc networks. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, page 109.

Cornelli, F., Damiani, E., di Vimercati, S. D. C., Paraboschi, S., and Samarati, P. (2002). Choosing reputable servents in a p2p network. In *Proceedings of the 11th international conference on World Wide Web*, pages 376–386, New York, NY, USA. ACM.

Delmastro, F., Passarella, A., and Conti, M. (2008). P2p multicast for pervasive ad hoc networks. *Pervasive and Mobile Computing*, 4(1):62 – 91.

Ding, G. and Bhargava, B. (2004). Peer-to-peer file-sharing over mobile ad hoc networks. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, page 104.

Doria, S. and Spohn, M. A. (2009). A multicast approach for peer-to-peer content distribution in mobile ad hoc networks. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6.

Holland, G. and Vaidya, N. (1999). Analysis of tcp performance over mobile ad hoc networks. In *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pages 219–230.

Kamvar, S. D., Schlosser, M. T., and Garcia-Molina, H. (2003). The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th international conference on World Wide Web*, pages 640–651, New York, NY, USA. ACM.

Klemm, A., Lindemann, C., and Waldhorst, O. (2003). A special-purpose peer-to-peer file sharing system for mobile ad hoc networks. *IEEE 58th Vehicular Technology Conference*, 4:2758–2763.

Kortuem, G., Schneider, J., Preuitt, D., Thompson, T., Fickas, S., and Segall, Z. (2001). When peer-to-peer comes face-to-face: Collaborative peer-to-peer computing in mobile ad hoc networks. In *Proceedings of the First International Conference on Peer-to-Peer Computing*, page 75.

Kozat, U., Koutsopoulos, I., and Tassiulas, L. (2004). A framework for cross-layer design of energy-efficient communication with qos provisioning in multi-hop wireless networks. In *Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, volume 2, pages 1446–1456.

Krifa, A., Sbai, M. K., Barakat, C., and Turletti, T. (2009a). Bithoc: A content sharing application for wireless ad hoc networks. *Pervasive Computing and Communications, IEEE International Conference on*, 0:1–3.

Krifa, A., Sbai, M. K., Barakat, C., and Turletti, T. (2009b). A standalone content sharing application for spontaneous communities of mobile handhelds. In *MobiHeld '09: Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds*, pages 77–78, New York, NY, USA. ACM.

Lee, J., Kim, G., and Park, S. (2002). Optimum udp packet sizes in ad hoc networks. In *Workshop on High Performance Switching and Routing. Merging Optical and IP Technologies*, pages 214–218, Seoul, South Korea.

Lee, U., Park, J.-S., Yeh, J., Pau, G., and Gerla, M. (2006). Code torrent: content distribution using network coding in vanet. In *MobiShare '06: Proceedings of the 1st international workshop on Decentralized resource sharing in mobile computing and networking*, pages 1–5, New York, NY, USA. ACM.

NS-2 (2010). The network simulator. `http://www.isi.edu/nsnam/ns`.

Passarella, A., Delmastro, F., and Conti, M. (2006). Xscribe: a stateless, cross-layer approach to p2p multicast in multi-hop ad hoc networks. In *MobiShare '06: Proceedings of the 1st international workshop on Decentralized resource sharing in mobile computing and networking*, pages 6–11, New York, NY, USA. ACM.

Quental, N. C. and Gonçalves, P. A. (2010). Cds-bittorrent: Um sistema de disseminação de conteúdo para a melhoria do desempenho de aplicações bittorrent sobre manets. In *VI Workshop de Redes Dinâmicas e Sistemas Peer-to-Peer (WP2P)*.

Rajagopalan, Sundaram, Shen, and Chien-Chung (2006). A cross-layer decentralized bittorrent for mobile ad hoc networks. In *Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, pages 1–10.

Sbai, M. K. and Barakat, C. (2009). Revisiting p2p content sharing in wireless ad hoc networks. *Lecture Notes in Computer Science*, 5918:13–25.

Sbai, M. K., Barakat, C., Choi, J., Hamra, A. A., and Turletti, T. (2008). *Adapting BitTorrent to Wireless Ad Hoc Networks*, volume 5198, pages 189–203. Springer Berlin / Heidelberg.

Souza, C. and Nogueira, J. M. (2008). Um estudo do bittorrent em redes ad hoc sem fio críticas com localidade espaço-temporal. In *XXV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 329–342.

Stuckmann, P. and Zimmermann, R. (2009). European research on future internet design. *IEEE Wireless Communications*, 16:14–22.

Vaishampayan, R. and Garcia-Luna-Aceves, J. J. (2004). Efficient and robust multicast routing in mobile ad hoc networks. *IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, pages 304–313.

Y. Charlie Hu, S. D. and Pucha, H. (2003). Exploiting the synergy between peer-to-peer and mobile ad hoc networks. In *9th Workshop on Hot Topics in Operating Systems*, pages 37–42, Lihue, HI, USA.