DÉGRADÉ: Usando Anotações para Aumentar a Qualidade de Downloads em Sistemas de Compartilhamento de Arquivos

Flávio Roberto Santos, Weverton Luis da Costa Cordeiro, Marinho Pilla Barcellos, Luciano Paschoal Gaspary

Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Porto Alegre – RS – Brasil

{flavio.santos,weverton.cordeiro,marinho,paschoal}@inf.ufrgs.br

Abstract. *The user autonomy to publish contents in file sharing systems allows contents to be published inaccurately/incorrectly, either due to diverse users' opinions (subjectivity), or due to malice. The lack of a proper mechanism to deal with these issues leads to download of undesired contents, waste of resources (such as time and bandwidth), and decreased user satisfaction. To bridge this gap, we propose a mechanism to regulate content dissemination based on users' perception. The proposed tag-based mechanism controls the dissemination of poorly, misdescribed content while it aids the dissemination of sufficiently and correctly characterized ones. Results obtained by means of simulation provide evidence about the efficacy and efficiency of the proposed mechanism.*

Resumo. *A autonomia que usuários possuem para publicar conteúdos em sistemas de compartilhamento de arquivos possibilita a publicação de arquivos descritos de forma imprecisa/incorreta, quer seja devido a diferentes percepções dos usuários (subjetividade), quer seja por ações maliciosas dos mesmos. A falta de um mecanismo apropriado para lidar com essas questões leva à recuperação de conteúdos indesejados, desperdício de recursos (tais como tempo e largura de banda), e à diminuição do grau de satisfação de usuários. Para preencher essa lacuna, propõe-se um mecanismo para regular a disseminação de conteúdos com base na percepção dos usuários. O mecanismo proposto, apoiado pelo emprego de tags, controla a disseminação de conteúdo mal descrito ao mesmo tempo que favorece a disseminação de outros suficientemente e corretamente avaliados. Resultados obtidos por meio de simulações evidenciam a eficácia e eficiência do mecanismo proposto.*

1. Introdução

Sistemas *Peer-to-Peer* (P2P) de compartilhamento de arquivos têm sido responsáveis por uma fatia representativa do tráfego na Internet [Schulze and Mochalski 2007, Schulze and Mochalski 2009]. Esses sistemas são formados, em sua maioria, por comunidades de usuários que compartilham de diferentes interesses e preferências [Andrade et al. 2005]. Em todas essas comunidades, seus integrantes têm autonomia para publicar novos conteúdos, descrevendo-os de acordo com suas próprias percepções.

Em decorrência dessa autonomia, torna-se natural o surgimento de conteúdos descritos indevidamente [TorrentFreak 2009]. Tal fenômeno é consequência das diferentes percepções que usuários têm sobre um mesmo conteúdo ou, ainda, de ações maliciosas de grupos de atacantes. Por exemplo, usuários maliciosos podem promover peças publicitárias utilizando, para tal, descrições falsas e atrativas para grandes proporções de usuários. Se não tratado devidamente pelos administradores, o grau de satisfação dos usuários pode diminuir e, em casos extremos, levar usuários a abandonar o sistema.

Para contornar esse problema, diversas soluções foram propostas para identificar (e marginalizar) conteúdos *poluídos*[1]. Uma limitação comum a essas soluções é a falta de um tratamento adequado à *subjetividade* em torno do conceito de poluição. Por exemplo, uma música publicada com o metadado "*rock*" pode ser contestada por um grupo de usuários, que a classificaria exclusivamente como "*pop*". Por outro lado, um usuário pode considerar o metadado "*chato*" inapropriado para um vídeo, enquanto outro usuário pode considerá-lo uma descrição perfeita.

Diante do exposto, nota-se a importância de lidar com a diversidade de opiniões, a fim de evitar o descontentamento dos usuários e o desperdício de recursos com a recuperação de conteúdos indesejados. Sistemas de anotação social (*social tagging systems*) – nos quais os usuários descrevem os conteúdos acessados usando anotações (*tags*) – têm sido largamente adotados para flexibilizar a descrição dos conteúdos em plataformas como Delicious, YouTube, e Flickr [Benevenuto et al. 2008, Koutrika et al. 2008]. Apesar das potencialidades, o uso de anotações colaborativas em sistemas de compartilhamento de arquivos, visando a promoção de uma melhor qualidade de experiência aos seus usuários, não foi, até onde sabemos, investigada pela comunidade de pesquisa.

Indo além da polarização binária (entre positiva e negativa) para opiniões de usuários, propõe-se DÉGRADÉ, um mecanismo baseado em anotações para a contenção da disseminação de conteúdo indesejado em sistemas de compartilhamento de arquivos. Em contraste com as soluções para contenção de poluição existentes, nossa abordagem – apoiada pelo emprego de *tags* – permite que os usuários expressem de forma mais flexível e confiável a percepção sobre conteúdos sendo disseminados, assim lidando com as questões de subjetividade mencionadas anteriormente. A disseminação mais ampla do conteúdo será favorecida quando existir uma percepção formada da comunidade em relação ao conteúdo disseminado, e controlada quando houver maior incerteza sobre o vocabulário que descreve o conteúdo.

As demais seções deste trabalho estão organizadas conforme descrito a seguir. A Seção 2 discute as principais estratégias propostas para combater a poluição de conteúdo, e descreve o uso de *tags* no contexto de sistemas baseados em anotações. O mecanismo proposto e o conjunto de equações que governa seu comportamento são apresentados na Seção 3 e, em seguida, na Seção 4, são discutidos os resultados obtidos por meio de simulações. Por fim, a Seção 5 apresenta as considerações finais e perspectivas de trabalhos futuros.

2. Trabalhos Relacionados

O presente trabalho se relaciona particularmente a dois tópicos: controle de poluição em sistemas de compartilhamento de arquivos e sistemas baseados em anotações. Esta seção

[1]No contexto deste trabalho, "poluição" se refere a conteúdos publicados com metadados inadequados.

comenta sobre trabalhos relacionados a esses tópicos e sua organização reflete esse fato.

2.1. Contenção de Poluição em Sistemas de Compartilhamento de Arquivos

Soluções para contenção de poluição têm sido largamente investigadas pela comunidade de Redes *Peer-to-Peer* (o leitor mais interessado pode referir-se ao *survey* publicado em [Hoffman et al. 2007]). Em geral, as mesmas podem ser classificadas entre baseadas em opiniões (*feedbacks*) dos usuários e baseadas em moderação.

Credence [Walsh and Sirer 2006], Scrubber [Costa et al. 2007] e Hybrid [Costa and Almeida 2007] são alguns dos exemplos mais importantes de sistemas de reputação baseados em *feedbacks* dos usuários. O Credence baseia-se na idéia de que pares honestos emitirão votos similares ao estabelecer a autenticidade de um determinado conteúdo. Nesse caso, pares com maior similaridade podem ser mais confiáveis do que outros com menor similaridade. O Scrubber, análogo ao Credence, adota uma abordagem mais agressiva para penalizar poluidores. O Hybrid, por sua vez, combina reputação do conteúdo com reputação do par, de modo a penalizar pares que apenas ocasionalmente fazem *upload* de conteúdo poluído. Uma crítica comum a essas soluções reside na vulnerabilide a ataques de *whitewashing* [Josang et al. 2007], uma vez que conteúdos recém publicados iniciam com reputação neutra. Mais importante, nenhum desses implementa um modelo que permita expressar subjetividade na avaliação dos conteúdos sendo disseminados.

Como uma primeira iteração sobre o tópico de contenção de poluição, propusemos, em um trabalho anterior, FUNNEL [Santos et al. 2009, Santos et al. 2010] – um mecanismo para tornar mais efetiva a contenção de poluição no estágio inicial de disseminação de conteúdos em comunidades BitTorrent. Embora FUNNEL seja resistente a ataques de *whitewashing*, não fez parte daquele trabalho, como uma premissa simplificatória, abordar a questão de subjetividade dos usuários na avaliação de conteúdos.

No rol de soluções baseadas em moderação, as mesmas variam desde estratégias mais centralizadas – nas quais administradores inspecionam todos os conteúdos publicados pelos usuários – até mais colaborativas – nas quais usuários podem enviar comentários ou mesmo denunciar algum conteúdo da comunidade. Em todas as abordagens, no entanto, a figura do administrador pode representar um fator limitante, especialmente em comunidades com intensa atividade de publicação de conteúdo.

Em resumo, observa-se que as soluções que tratam sobre contenção de poluição em sistemas de compartilhamento de arquivos não lidam adequadamente com a diversidade de opiniões dos usuários. Na subseção seguinte é descrito como o uso de *tags* permite resolver esse problema no contexto de sistemas colaborativos.

2.2. Sistemas Colaborativos Baseados em Anotações

O uso de *tags* criadas pelo usuário para classificação de diferentes tipos de recursos na Internet (páginas *web*, documentos, fotos, vídeos, etc.) emergiu como uma alternativa aos metadados gerados por profissionais e pelos próprios autores para descrever recursos disponibilizados *online* [Mathes 2004]. Desde então, *tags* têm sido largamente exploradas em plataformas colaborativas como Delicious, YouTube, Flickr, entre outros. Uma vez que tais plataformas dependem essencialmente do comportamento e da estrutura social

dos usuários que os utilizam, é comum classificar as *tags* mais populares nessas plataformas como "folksonomia" [Mathes 2004] – termo formado pela combinação das palavras *folk* (povo) e *taxonomia*.

Em virtude da crescente popularidade dos sistemas de anotação social, os mesmos têm recebido grande atenção por parte da comunidade científica. Enquanto alguns autores têm se concentrado em entender a semântica de *tags* associadas a tipos de recursos diferentes [Heckner et al. 2008], outros têm dedicado atenção ao estudo da estrutura e da dinâmica [Golder and Huberman 2005, Marlow et al. 2006], apenas para mencionar alguns dos rumos de pesquisa existentes na área.

É consenso na literatura que *tags* melhoram substancialmente o processo de busca e obtenção de recursos disponíveis publicamente em plataformas colaborativas, e têm potencial para aperfeiçoar sistemas de reputação [Marlow et al. 2006]. Tal é justificado pelo fato de *tags* adicionarem uma camada adicional de informação descritiva sobre o conteúdo, além de permitirem lidar com a subjetividade associada à descrição dos recursos. Apesar das potencialidades, um dos principais problemas existentes é a atribuição de *tags* imprecisas/incorretas a recursos. Esse comportamento, conhecido na literatura como *tag spamming*, tem sido amplamente abordado em pesquisas recentes [Bian et al. 2008, Benevenuto et al. 2008, Koutrika et al. 2008].

Existem dois desafios relacionados à adoção de *tags* como um mecanismo para lidar com a subjetividade em sistemas de compartilhamentos de arquivos: identificar o momento em que a nuvem de *tags* efetivamente reflete a natureza de um conteúdo, e lidar com os danos causados por ataques de *tag spamming*. As seções seguintes detalham como esses desafios são abordados pela solução proposta.

3. Modelo Proposto

Esta seção introduz o modelo para contenção de *downloads* baseado na variação do vocabulário dos conteúdos. Primeiramente será apresentada a dinâmica tipicamente observada em vocabulários de sistemas que empregam técnicas de anotações colaborativas. Em seguida, será definida uma métrica que expressa a variação do vocabulário. Por fim, será discutida a idéia chave do mecanismo DÉGRADÉ: quanto maior a variação (e consequentemente o valor da métrica), menos *downloads* são autorizados.

3.1. Dinâmica dos vocabulários

No modelo aqui proposto, usuários do sistema descrevem os conteúdos através de *tags*. Dado um conjunto $\mathcal{T}$ de *tags* possíveis para descrever um conteúdo qualquer, definimos a atribuição de um usuário através de um vetor de n elementos binários indexados por essas *tags*. Dessa forma, o vetor $\vec{v_i} = \langle v_{i,t_1}, \ldots, v_{i,t_n} \rangle$ (assumindo $|\mathcal{T}| = n$) possui o elemento v_{i,t_j} igual a 1 caso a *tag* t_j esteja na i-ésima atribuição feita por usuários, ou 0 caso contrário. A partir desse conceito, é possível definir o vocabulário que descreve um conteúdo qualquer em função das frequências relativas de suas *tags*, que representa a razão entre o número de ocorrências de uma *tag* em relação ao total de *tags* do vocabulário. Considere a matriz M formada por m atribuições:

$$M_{m\times n} = \begin{pmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \vdots \\ \vec{v}_m \end{pmatrix} = \begin{pmatrix} v_{1,t_1} & v_{1,t_2} & \cdots & v_{1,t_n} \\ v_{2,t_1} & v_{2,t_2} & \cdots & v_{2,t_n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m,t_1} & v_{m,t_2} & \cdots & v_{m,t_n} \end{pmatrix}$$

A Equação 1 define a frequência relativa de uma *tag* t_k após a m-ésima atribuição.

$$f_{m,t_k} = \frac{\sum_{1\leq i\leq m} v_{i,t_k}}{\sum_{\substack{1\leq i\leq m \\ 1\leq j\leq n}} v_{i,t_j}} \tag{1}$$

Exemplificando, dado um conjunto $\mathcal{T} = \{t_1, t_2, t_3, t_4\}$ e as atribuições $\{\langle 1,0,0,0\rangle, \langle 1,0,1,0\rangle, \langle 1,1,1,0\rangle\}$, as frequências relativas calculadas são $f_{3,t_1} = \frac{3}{6}$, $f_{3,t_2} = \frac{1}{6}$, $f_{3,t_3} = \frac{2}{6}$ e $f_{3,t_4} = 0$. A cada nova atribuição, as frequências relativas das *tags* são atualizadas. Dessa forma, se uma nova atribuição $\langle 0,1,0,1\rangle$ for realizada, as frequências relativas assumem os valores $f_{4,t_1} = \frac{3}{8}$, $f_{4,t_2} = \frac{2}{8}$, $f_{4,t_3} = \frac{2}{8}$ e $f_{4,t_4} = \frac{1}{8}$. À medida em que o número de atribuições cresce, os valores das frequências relativas variam e tendem a se estabilizar conforme ilustrado na Figura 1. Os resultados foram obtidos através de análises em traços coletados do Delicious[2].

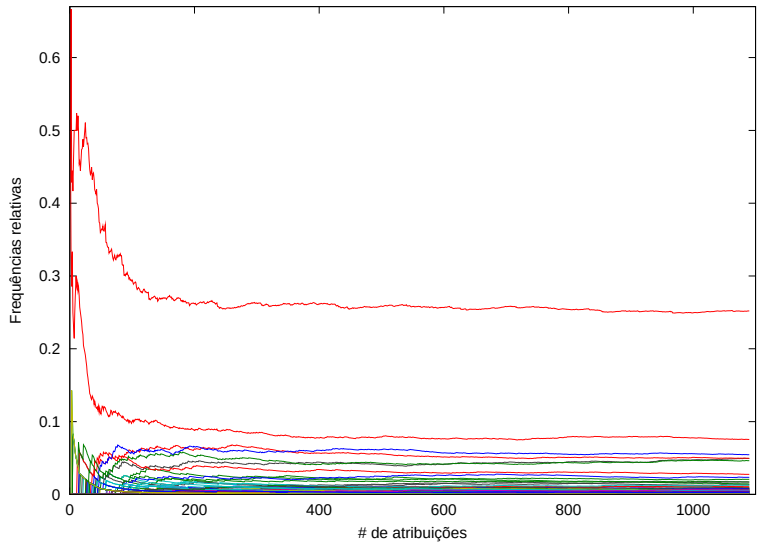


Figura 1. Convergência das frequências relativas das *tags*

Em [Golder and Huberman 2006], os autores analisaram empiricamente diversos traços semelhantes e constataram que as frequências relativas das *tags* relacionadas a um conteúdo estabilizam por volta da centésima atribuição. A seguir é apresentada a métrica de variação dessas frequências e a estratégia para contenção de *downloads* à luz do seu valor.

[2]Disponível em http://www.tagora-project.eu/data/#delicious

3.2. Métrica de variação

Esta subseção discute a métrica utilizada para avaliar diferentes estágios da dinâmica dos vocabulários. Considerando uma janela com w atribuições $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_w$ e uma sequência de frequências $\Phi_t = \langle f_{1,t}, f_{2,t}, \ldots, f_{w,t} \rangle$ que reflete a sequência de atribuições, definimos a variação de uma *tag* t em função do desvio padrão das suas frequências relativas ($\sigma(\Phi_t)$). O cálculo da métrica que avalia a variação no vocabulário em uma janela com w atribuições resulta do somatório dos desvios padrão observados para cada *tag* ao longo das w últimas atribuições, conforme Equação 2 a seguir.

$$\Delta_w = \sum_{t \in \mathcal{T}} \sigma(\Phi_t) \tag{2}$$

Diversas outras medidas de dispersão podem ser utilizadas em alternativa ao desvio padrão. Algumas delas, como a variância e a amplitude máxima, foram consideradas no contexto deste trabalho e descartadas por fatores discutidos a seguir. A primeira delas possui um efeito semelhante no cálculo de Δ, porém apresenta a unidade de medida igual ao quadrado da unidade original, causando uma difícil interpretação dos seus valores. A segunda mostra-se inadequada, pois representa uma aproximação da variabilidade do conjunto, além de ser sensível apenas a valores extremos.

A matriz $M_{7,4}$ abaixo ilustra uma sequência de 7 atribuições (da linha 1 a linha 7). A partir dela, deriva-se ao lado outra matriz em que um elemento f_{i,t_j} representa a frequência relativa considerando as i primeiras atribuições da *tag* t_j, calculada de acordo com a Equação 1.

$$M_{7,4} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad \left[f_{i,t_j}\right]_{7\times 4} = \begin{pmatrix} {}^1\!/_2 & {}^1\!/_2 & 0 & 0 \\ {}^1\!/_4 & {}^2\!/_4 & {}^1\!/_4 & 0 \\ {}^1\!/_5 & {}^3\!/_5 & {}^1\!/_5 & 0 \\ {}^2\!/_7 & {}^3\!/_7 & {}^1\!/_7 & {}^1\!/_7 \\ {}^2\!/_9 & {}^3\!/_9 & {}^2\!/_9 & {}^2\!/_9 \\ {}^3\!/_{13} & {}^4\!/_{13} & {}^3\!/_{13} & {}^3\!/_{13} \\ {}^3\!/_{14} & {}^5\!/_{14} & {}^3\!/_{14} & {}^3\!/_{14} \end{pmatrix}$$

Dessa forma, para o exemplo apresentado temos:

$$\begin{aligned} \Delta_7 &= \sigma(\Phi_{t_1}) + \sigma(\Phi_{t_2}) + \sigma(\Phi_{t_3}) + \sigma(\Phi_{t_4}) \\ &= 0,10436 + 0,10667 + 0,086232 + 0,11196 \\ &= 0,409222 \end{aligned}$$

3.3. Controlando o número de *downloads*

O mecanismo aqui proposto busca fornecer uma visão confiável (estável) sobre o vocabulário aos usuários do sistema. Ao invés de simplesmente oferecer uma descrição instantânea do conteúdo, o histórico das atribuições é empregado no cálculo da variação do vocabulário. A fim de reduzir as chances de um usuário recuperar um conteúdo que ainda

não foi devidamente descrito, o mecanismo atua autorizando *downloads* gradativamente de acordo com a métrica Δ. Nesse contexto, o mecanismo emprega duas variáveis: D e A, definidas a seguir. D representa o número de *downloads* atualmente ocorrendo, enquanto que A representa o número máximo de *downloads* concorrentes autorizados pelo mecanismo. O valor de D é incrementado quando um novo *download* inicia e decrementado quando ele termina. O valor de A é definido com base em um comportamento esperado, conforme a seguir. Sejam δ um parâmetro de limiar, e A_{min} e A_{max} os limites para os valores de A enquanto o mecanismo estiver atuando, temos:

- Se $\Delta \rightarrow 1$, então $A \rightarrow A_{min}$;
- Se $\Delta \rightarrow \delta^{+}$, então $A \rightarrow A_{max}$;
- Se $\Delta < \delta$, então $A = \infty$.

O comportamento almejado para A é obtido através da Equação 3.

$$A = \begin{cases} \infty & \text{se } \Delta < \delta, \\ \frac{(\Delta-\delta)\times A_{min}+(1-\Delta)\times A_{max}}{1-\delta} & \text{caso contrário.} \end{cases} \quad (3)$$

O parâmetro $\delta \in [0; 1)$ deve ser ajustado de acordo com o rigor exigido pelo administrador do sistema. Se configurado com seu valor mínimo, a condição $\Delta < \delta$ nunca será satisfeita e o mecanismo sempre atua controlando os *downloads*. Em contraste, à medida que δ se aproxima do seu limite superior, menos rigoroso se torna o mecanismo, permitindo que *downloads* prossigam indiscriminadamente. Dessa forma, ao requisitar um conteúdo, o mecanismo calcula o valor de A e o compara com o valor de D. O pedido em questão é, então, autorizado caso $D < A$.

4. Avaliação do Modelo

Esta seção apresenta uma avaliação do mecanismo proposto, com o objetivo de responder a três questões fundamentais. Primeiro, qual a eficácia do mecanismo ao tentar fornecer uma visão mais estável do vocabulário aos seus usuários. Segundo, qual a sobrecarga decorrente do retardo das entradas dos usuários. Terceiro, como o mecanismo se comporta na presença de ataques em conluio. Para responder a essas perguntas, um extenso conjunto de simulações foi executado. A seguir, são apresentados os cenários avaliados, a descrição dos traços adotados e do simulador, bem como os resultados obtidos.

4.1. Cenários avaliados

Os cenários avaliados consistem em *C* pares legítimos, *M* maliciosos e *I* usuários que iniciam a distribuição de um conteúdo e permanecem disponíveis durante toda a simulação. Neste estudo, o valor de *I* foi fixado em 20 e o valor de *M* foi variado entre 0 e 1000 para analisar o efeito do ataque em conluio. O valor de *C* foi definido de acordo com o traço de atribuições utilizado. Os usuários maliciosos chegam no sistema antes de todos os usuários legítimos. Esse comportamento foi adotado na avaliação por representar o pior cenário para o mecanismo. Em seguida, os *C* usuários legítimos chegam seguindo uma taxa definida pela função $\lambda(t) = \frac{\alpha_0}{1+\beta t}$, em que o fator de decaimento β foi definido como 0,01 e a taxa inicial α_0 ajustada de modo que todos os usuários cheguem até o instante $t \approx 4h$ [Andrade et al. 2009].

Ao finalizarem seus *downloads*, os usuários legítimos classificam o conteúdo com um conjunto de *tags* extraídas de traços reais do Delicious (esses traços serão devidamente descritos na Subseção 4.2). Por outro lado, os usuários maliciosos realizam suas atribuições assim que obtêm acesso ao sistema. Tal comportamento malicioso representa uma vantagem explorada pelos atacantes, pois ignora a premissa de que o conteúdo precisa ser recuperado antes de ser avaliado e a atribuição de *tags* ser realizada. Diferentemente dos usuários maliciosos, que saem do sistema após a atribuição das *tags*, os usuários legítimos permanecem indefinidamente fazendo *upload* para os demais. Para fins de avaliação, foi utilizado um modelo de distribuição de conteúdo baseado em enxames (*swarms*), sendo o mesmo apresentado na Subseção 4.3.

4.2. Descrição dos traços

Para avaliar o mecanismo proposto, os usuários precisam atribuir *tags* aos conteúdos recuperados. Ao invés de gerar conjuntos sintéticos de dados, foi utilizado e estudado um conjunto de traços coletados do Delicious, sob o contexto do Projeto Tagora, durante 2006. Em sua totalidade, o traço contém 532.924 usuários, 2.481.698 *tags* diferentes, 17.262.480 itens (endereços de sítios da Internet, neste caso) e 140.126.586 atribuições, somando 1,1 GB de dados.

A estratégia para escolha do conjunto de traços a ser utilizado na avaliação é descrita a seguir. Inicialmente, separamos um conjunto de 2000 itens que apresentam os maiores números de atribuições. Cada um desses itens corresponde a um traço, composto de sequências de atribuições de *tags*. Esses traços foram agrupados através de uma técnica conhecida como "*hierarchical clustering*" de acordo com três parâmetros: número de *tags* diferentes utilizadas pelos usuários, número médio de *tags* em cada atribuição, e a proporção de *tags* diferentes em relação ao número total de *tags* utilizadas. Identificamos 6 grupos significativos dentre o total de traços considerados. Para cada grupo, escolhemos como uma observação representativa o traço com a menor distância Euclidiana para o ponto representado pelos valores médios de todas as observações do grupo. A Tabela 1 ilustra os grupos identificados em função da média dos seus parâmetros.

Tabela 1. Lista de grupos de traços

Grupo	# de traços	# de *tags* diferentes	# de *tags*/atribuição	Fração de *tags* únicas
G1	13	2299	3,285	0,065
G2	44	1449	3,283	0,086
G3	231	853	3,444	0,074
G4	686	457	3,380	0,068
G5	371	360	3,397	0,078
G6	654	317	3,454	0,083

4.3. Modelo do simulador

O modelo empregado na avaliação do mecanismo foi inicialmente proposto por Qiu e Srikant [Qiu and Srikant 2004] e estendido por Guo *et al.* [Guo et al. 2005]. Trata-se de um modelo de fluidos para representação de enxames de usuários utilizando o protocolo BitTorrent. Utilizando esse modelo, é possível calcular analiticamente a evolução dos *downloads* dentro de intervalos de tempo. Para isso, são necessários alguns parâmetros

de entrada para as equações, por exemplo o número de sugadores x, o número de semeadores y, as taxas de *upload* μ e de *download* c, e um índice de eficiência do sistema de compartilhamento de conteúdo η, que define a probabilidade de dois sugadores estarem interessados em trocar dados. Dessa forma, a quantidade de tráfego gerado no enxame por unidade de tempo pode ser calculada por $min\{\mu(\eta x + y), cx\}$.

Qiu e Srikant mostraram que para um conteúdo dividido em P partes, se cada usuário mantém conexões com k outros, $\eta \approx 1 - \left(\frac{\log P}{P}\right)^k$. No instante em que um usuário chega, o mecanismo emprega a Equação 3 para determinar se este pode entrar no sistema ou deve aguardar. Em caso positivo, o número de sugadores é incrementado. Caso contrário, o usuário deve esperar T unidades de tempo para tentar novamente. O processo se repete até que todos os usuários entrem no sistema e recuperem o conteúdo.

À medida que os usuários completam seus *downloads*, as atribuições de *tags* vão sendo realizadas. Considerando um conteúdo de tamanho F, o modelo assume que o i-ésimo usuário finaliza seu *download* após $i \times F$ unidades de tráfego serem geradas no sistema.

4.4. Resultados Obtidos

Nesta subseção, apresentamos os resultados alcançados através de simulações realizadas com traços coletados do Delicious. O objetivo é responder às três perguntas anteriormente enumeradas. Foram analisadas a eficácia do mecanismo e a sobrecarga proveniente da sua política de contenção de *downloads*, assim como a resistência a dois tipos de ataques em conluio. No primeiro, os usuários buscam manipular a variância do vocabulário atribuindo conjuntos de *tags* sempre aleatórias. No segundo, os usuários atribuem um mesmo conjunto de *tags*, definidas aleatoriamente, ao conteúdo.

As avaliações realizadas referem-se aos grupos $G1$ a $G6$, definidos na Subseção 4.2, para designar seus traços mais representativos. Os efeitos dos ataques para $100 < M \leq 1000$ mantiveram-se inalterados e foram omitidos por restrições de espaço. O estudo foi auxiliado por dois tipos de gráficos. O primeiro ilustra o valor da métrica Δ no instante em que os usuários ganham acesso ao conteúdo. Um ponto (x, y) no gráfico significa que y usuários obtiveram um valor $\Delta \leq x$. Dessa forma, quanto mais ascendente a curva, mais usuários obtiveram uma visão estável do conteúdo. O segundo tipo de gráfico quantifica o atraso decorrente da ação do mecanismo. Um ponto (x, y) nesse gráfico significa que y usuários consumiram no máximo x minutos desde as suas chegadas até a recuperação total do conteúdo.

Os parâmetros utilizados na avaliação estão resumidos na Tabela 2. Dentre os parâmetros do modelo, w representa o tamanho da janela de atribuições que é considerado no cálculo de Δ_w e os demais são empregados diretamente no cálculo de A. Os parâmetros da simulação determinam o tamanho do conteúdo (F), a largura de banda dos usuários (μ e c), o índice de interesse entre os sugadores (η, calculado segundo equação proposta por Qiu e Srikant, em que $k = 4$ e o conteúdo é subdividido em peças de 16 KB) e o tempo de espera dos usuários até retornar ao sistema (T).

As Figuras 2 e 3 ilustram os efeitos do primeiro e do segundo ataques, respectivamente, sobre três grupos de traços ($G1$, $G3$ e $G6$). Cada coluna da figura representa um grupo. Os demais grupos apresentaram comportamentos semelhantes e foram omitidos por restrições de espaço. A fim de responder o primeiro questionamento sobre a

Tabela 2. Informações sobre o ambiente considerado na avaliação experimental

Parâmetros do modelo	
w	50
A_{min}	10
A_{max}	500
δ	0,3
Parâmetros da simulação	
F	512 MB
μ	256 Kbps
c	1024 Kbps
η	99,99%
T	1 min

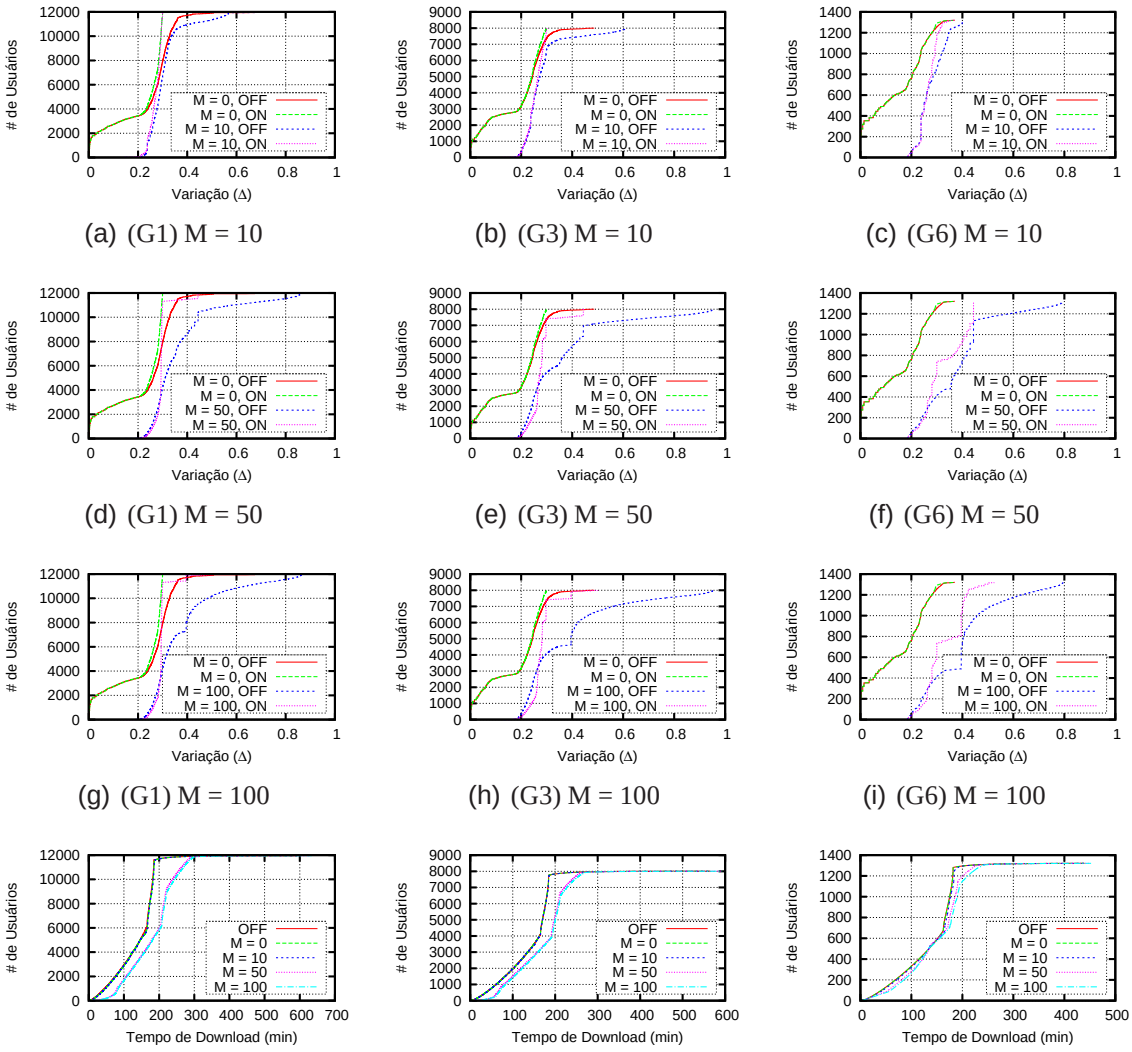
eficácia do mecanismo ao tentar fornecer uma visão mais estável do vocabulário aos seus usuários, comparamos as curvas com e sem mecanismo (*ON* e *OFF*, respectivamente) de cada gráfico para um mesmo número de atacantes. Com isso, notamos o efeito significativo da estratégia de contenção em proporcionar uma visão mais estável do vocabulário.

A Figura 2 ilustra o efeito do primeiro ataque. O objetivo dos atacantes é inserir *tags* aleatórias e aumentar a variação do vocabulário, provocando um retardo nos *downloads* dos usuários em decorrência do mecanismo de contenção. A efetividade do ataque, nesse caso, se traduz em mais usuários legítimos fazendo *download* do conteúdo quando a variação do vocabulário que descreve o conteúdo é alta. Em termos de gráficos, se traduz em curvas mais deslocadas para o ponto $\Delta = 1$.

Os resultados mostram que, na ausência de controle do mecanismo (*OFF*), os atacantes conseguem fazer com que mais usuários legítimos acessem os conteúdos em instantes em que é alta a variação do vocabulário que os descreve. Por exemplo, na Figura 2(d), na ausência do mecanismo e com 50 atacantes (*M = 50, OFF*), apenas 4000 usuários fazem *download* do conteúdo quando a sua variação é menor ou igual a $0,3$. Em outras palavras, 8000 usuários acessam o conteúdo quando este apresenta variações no vocabulário maiores que $0,3$. Ao ativar o mecanismo (*ON*), os ganhos na retenção dos *downloads* são bastante expressivos. Por exemplo, 11500 usuários fazem *download* do conteúdo quando a sua variação é menor ou igual a $0,3$ (em contraste com os 4000 iniciais). Posto de outra forma, apenas 500 obtêm acesso quando as variações são maiores que $0,3$. Um comportamento semelhante pode ser observado nos demais grupos de traços presentes na figura.

A fim de avaliar a sobrecarga do mecanismo nos tempos de *download* dos usuários, observamos as Figuras 2(j), 2(k) e 2(l). Elas ilustram o atraso à medida que aumenta o número de atacantes. É possível notar que esse atraso é inferior a 30 minutos ($\sim 18\%$) em maior parte dos cenários e, em um pior caso, chega a 100 minutos no traço do grupo 1 (Figura 2(j)).

A Figura 3 ilustra o efeito do segundo ataque, em que a atribuição do mesmo conjunto de *tags* repetidas vezes causa uma redução na métrica Δ. Dado que o mecanismo deixa de agir quando $\Delta < \delta$, as curvas com e sem mecanismo, *ON* e *OFF* respectivamente, aparecem próximas nos gráficos. Esse efeito pode ser observado nos diversos



(a) (G1) M = 10 (b) (G3) M = 10 (c) (G6) M = 10

(d) (G1) M = 50 (e) (G3) M = 50 (f) (G6) M = 50

(g) (G1) M = 100 (h) (G3) M = 100 (i) (G6) M = 100

(j) (G1) Atraso (k) (G3) Atraso (l) (G6) Atraso

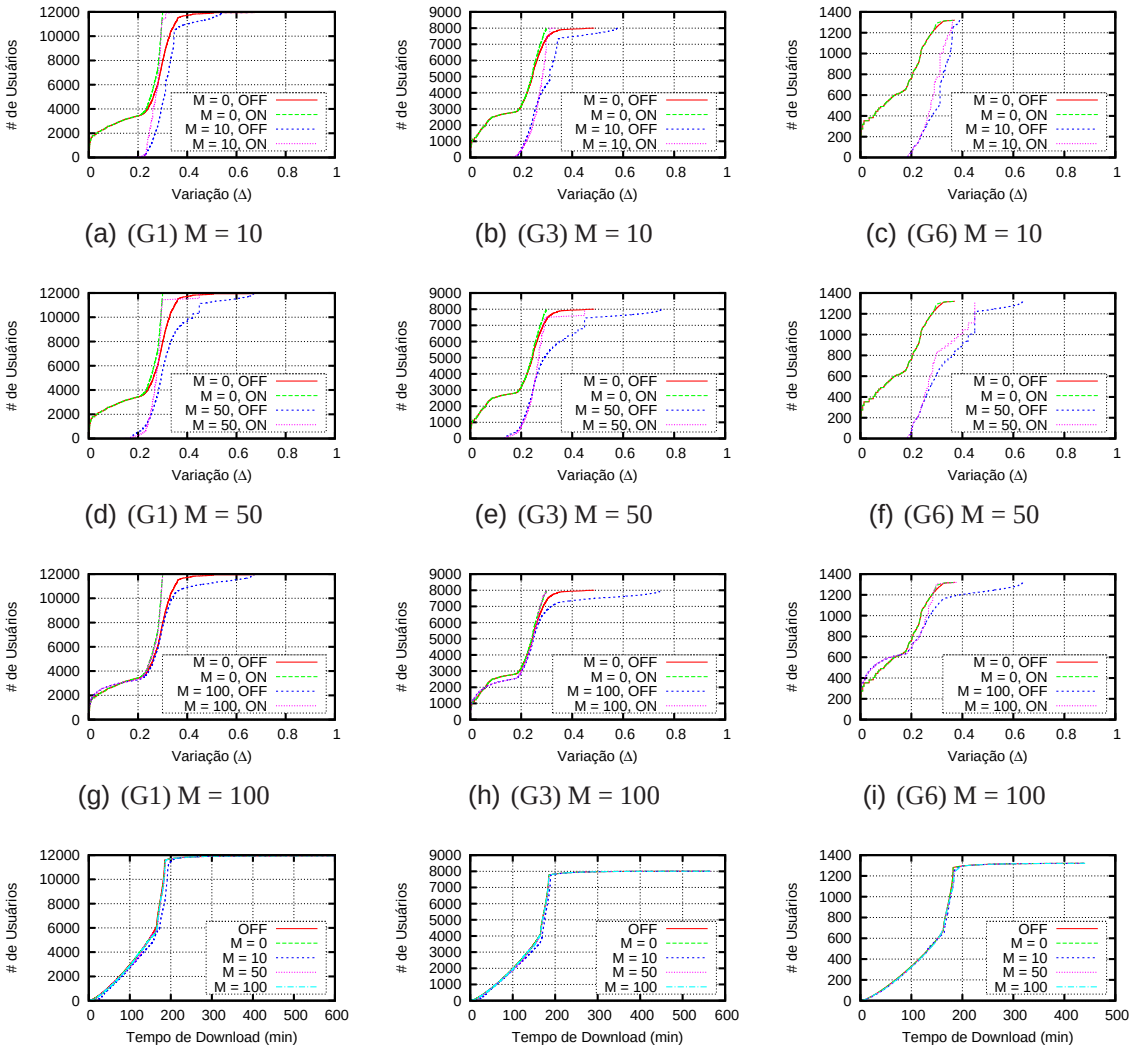
Figura 2. Resultados obtidos considerando a primeira estratégia de ataque

grupos analisados e é evidenciado à medida que o número de atacantes cresce. Uma outra evidência do ataque aparece nas Figuras 3(g), 3(h) e 3(i). As curvas na presença de atacantes têm seus inícios próximos ao eixo y, destacando o efeito provocado pela estabilização temporária do vocabulário.

As Figuras 3(j), 3(k) e 3(l) mostram, ainda, que esse ataque não produz o efeito desejado: acelerar a disseminação de algum conteúdo (*e.g.*, vírus ou *malware*) entre os usuários. É possível observar através das curvas que não há redução no tempo de *download* dos usuários, o que demonstra a resistência do mecanismo a esse tipo de manipulação.

5. Conclusões e Trabalhos Futuros

O combate à disseminação de conteúdos poluídos em sistemas de compartilhamentos de arquivos é um tópico que tem recebido forte atenção da comunidade científica. Em geral, a estratégia adotada no combate à poluição tem sido considerar os *feedbacks* dos



(a) (G1) M = 10 (b) (G3) M = 10 (c) (G6) M = 10

(d) (G1) M = 50 (e) (G3) M = 50 (f) (G6) M = 50

(g) (G1) M = 100 (h) (G3) M = 100 (i) (G6) M = 100

(j) (G1) Atraso (k) (G3) Atraso (l) (G6) Atraso

Figura 3. Resultados obtidos considerando a segunda estratégia de ataque

usuários para diminuir a reputação de arquivos corrompidos, descritos de forma imprecisa e/ou incorreta, e mesmo arquivos contendo vírus ou outro *malware*. Entretanto, tais propostas tem negligenciado a questão da subjetividade dos usuários na avaliação de conteúdos sendo disseminados. Sem levar em conta esse aspecto, usuários podem obter conteúdos que não necessariamente condizem com suas expectativas, gerando descontentamentos e até mesmo desperdício de recursos. Para lidar com essa limitação, neste artigo foi proposto DÉGRADÉ, um mecanismo baseado em anotações para a contenção da disseminação de conteúdos indesejados em sistemas de compartilhamento de arquivos.

Os experimentos realizados mostraram a efetividade do uso de *tags* como um mecanismo para expressar subjetividade na avaliação de conteúdos sendo disseminados. Além disso, a solução proposta mostrou-se eficaz e eficiente na contenção da disseminação mais ampla de conteúdos enquanto não havia uma caracterização mais nítida sobre a natureza dos mesmos. Ao manter controle sobre a variação no vocabulário, menos usuários foram autorizados a fazer o *download*, em um momento em que seria mais

alta a probabilidade de que os conteúdos que desejassem obter não correspondessem às expectativas dos mesmos.

Apesar dos resultados promissores alcançados, existe uma ampla perspectiva de pesquisa nesse tópico. Direções potenciais para trabalhos futuros incluem (*i*) a avaliação do impacto de tamanhos diversos (em termos de quantidades de *tags*) das anotações postadas por usuários a um determinado conteúdo sendo disseminado, (*ii*) a avaliação da eficácia da solução perante diferentes probabilidades de que usuários legítimos atribuirão *tags* aos conteúdos recuperados (fazendo uma analogia com os sistemas de reputação existentes, probabilidade de que os usuários irão votar), (*iii*) a proposta de um mecanismo adicional que procure, a partir dos *downloads* realizados e das *tags* atribuídas, sintetizar uma medida da "qualidade da experiência" percebida pelos usuários, e (*iv*) a análise do desempenho e do impacto da instanciação da solução proposta em um arcabouço P2P real (por exemplo, BitTorrent).

Agradecimentos

Os autores deste trabalho agradecem a Flavio Vinicius Diniz de Figueiredo pelos valiosos comentários sob o viés de sistemas de recuperação de informação e sistemas colaborativos baseados em anotações.

Referências

Andrade, N., Mowbray, M., Lima, A., Wagner, G., and Ripeanu, M. (2005). Influences on cooperation in bittorrent communities. In *ACM SIGCOMM workshop on Economics of peer-to-peer systems (P2PEcon 2005)*, pages 111–115, New York, NY, USA. ACM.

Andrade, N., Santos-Neto, E., Brasileiro, F., and Ripeanu, M. (2009). Resource demand and supply in bittorrent content-sharing communities. *Computer Networks: The International Journal of Computer and Telecommunications Networking*, 53(4):515–527.

Benevenuto, F., Rodrigues, T., Almeida, V., Almeida, J., Zhang, C., and Ross, K. (2008). Identifying video spammers in online social networks. In *AIRWeb '08: Proceedings of the 4th international workshop on Adversarial information retrieval on the web*, pages 45–52, New York, NY, USA. ACM.

Bian, J., Liu, Y., Agichtein, E., and Zha, H. (2008). A few bad votes too many?: towards robust ranking in social media. In *AIRWeb '08: Proceedings of the 4th international workshop on Adversarial information retrieval on the web*, pages 53–60, New York, NY, USA. ACM.

Costa, C. and Almeida, J. (2007). Reputation systems for fighting pollution in peer-to-peer file sharing systems. In *7th IEEE International Conference on Peer-to-Peer Computing (P2P 2007)*, pages 53–60. IEEE.

Costa, C., Soares, V., Almeida, J., and Almeida, V. (2007). Fighting pollution dissemination in peer-to-peer networks. In *22nd ACM Symposium on Applied Computing (SAC 2007)*, pages 1586–1590, New York, NY, USA. ACM.

Golder, S. and Huberman, B. A. (2005). The structure of collaborative tagging systems. http://arxiv.org/abs/cs.DL/0508082.

Golder, S. A. and Huberman, B. A. (2006). Usage patterns of collaborative tagging systems. *Journal of Information Science*, 32(2):198–208.

Guo, L., Chen, S., Xiao, Z., Tan, E., Ding, X., and Zhang, X. (2005). Measurements, analysis, and modeling of bittorrent-like systems. In *5th Conference on Internet Measurement (IMC 2005)*, pages 4–4, Berkeley, CA, USA. USENIX Association.

Heckner, M., Neubauer, T., and Wolff, C. (2008). Tree, funny, toread, google: what are tags supposed to achieve? a comparative analysis of user keywords for different digital resource types. In *SSM '08: Proceeding of the 2008 ACM workshop on Search in social media*, pages 3–10, New York, NY, USA. ACM.

Hoffman, K., Zage, D., and Nita-Rotaru, C. (2007). A survey of attack and defense techniques for reputation systems. *ACM Computing Surveys*.

Josang, A., Ismail, R., and Boyd, C. (2007). A survey of trust and reputation systems for online service provision. In *Elsevier Decision Support Systems*. Elsevier.

Koutrika, G., Effendi, F. A., Gyöngyi, Z., Heymann, P., and Garcia-Molina, H. (2008). Combating spam in tagging systems: An evaluation. *ACM Transactions on the Web*, 2(4):1–34.

Marlow, C., Naaman, M., Boyd, D., and Davis, M. (2006). Ht06, tagging paper, taxonomy, flickr, academic article, to read. In *HYPERTEXT '06: Proceedings of the seventeenth conference on Hypertext and hypermedia*, pages 31–40, New York, NY, USA. ACM.

Mathes, A. (2004). Folksonomies - cooperative classification and communication through shared metadata. http://www.adammathes.com/academic/computer-mediated-communication/folksonomies.html.

Qiu, D. and Srikant, R. (2004). Modeling and performance analysis of bittorrent-like peer-to-peer networks. In *ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM 2004)*, pages 367–378, New York, NY, USA. ACM.

Santos, F. R., da Costa Cordeiro, W. L., Gaspary, L. P., and Barcellos, M. P. (2010). Choking polluters in bittorrent file sharing communities. In *IEEE/IFIP Network Operations and Management Symposium (NOMS 2010)*, pages 1–8. IEEE Communications Society.

Santos, F. R., Gaspary, L. P., and Barcellos, M. P. (2009). Separando Joio de Trigo com Funnel: Combate à Poluição de Conteúdo em Comunidades BitTorrent. In *27o Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2009)*, pages 393–406, Recife, PE, Brazil.

Schulze, H. and Mochalski, K. (2007). Internet study 2007. http://www.ipoque.com/userfiles/file/internet_study_2007.pdf.

Schulze, H. and Mochalski, K. (2009). Internet study 2008-2009. https://portal.ipoque.com/downloads/index/get/id/265/.

TorrentFreak (2009). Fake aXXo Torrents Bombard BitTorrent. http://torrentfreak.com/fake-axxo-torrents-bombard-bittorrent-090313/.

Walsh, K. and Sirer, E. G. (2006). Experience with an object reputation system for peer-to-peer filesharing. In *3rd USENIX Symposium on Networked Systems Design & Implementation (NSDI 2006)*, page 1, Berkeley, CA, USA. USENIX Association.