Caracterização de Falhas Relacionadas a Aplicações de *Live Streaming* na Internet

Ingrid Jansch-Pôrto

Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brazil

ingrid@inf.ufrgs.br

Abstract. *Live streaming multicast applications that use Internet support – and especially those that use a peer-to-peer overlay – are subject to natural and human faults. In order to survive and to be attractive from the point-of-view of its (many) thousands of users, many management mechanisms must be implemented. This paper aims at presenting the main fault types that affect this kind of systems. Some comments on fault modeling, and about problems and reasons related to handling these faults are added. This paper is not supposed to offer solutions, but intends to give insights to novice researchers in this domain.*

Resumo. *Sistemas de difusão de conteúdos em tempo real – live streaming – construídos sobre a Internet, e especialmente aqueles que exploram arquiteturas peer-to peer, estão sujeitos a falhas naturais e humanas. Para que as aplicações não só sobrevivam, mas apresentem características atrativas aos (muitos) milhares de usuários, diversos mecanismos precisam ser usados como suporte. Este artigo visa apresentar os principais tipos de falhas que afetam estes sistemas e bem como tecer comentários sobre dificuldades relacionadas ao seu tratamento, além de informações sobre a modelagem de falhas. O artigo não pretende oferecer soluções, mas servir como um alerta a pesquisadores iniciantes na área.*

1. Introdução

Atualmente, a difusão de vídeo e áudio ocupa um alto percentual dos conteúdos que são do interesse de usuários da Internet. No Brasil, a forma mais conhecida ainda é a "sob demanda", na qual os usuários buscam arquivos pré-armazenados. Neste caso, o ritmo da operação de transferência depende das características de origem e destino – tais como as capacidades de *download* e *upload*; do momento de busca – quando pode haver competição entre usuários que tentam ter acesso simultaneamente a conteúdos recém disponibilizados, sobrecarregando o servidor; ou estarem disponíveis apenas em raros usuários cujos recursos de acesso à rede são modestos. Estes arquivos podem estar subdivididos em partes, coletáveis em qualquer ordem e depois remontadas. Apesar da ansiedade por poder desfrutar dos arquivos o mais cedo possível, de forma geral, é apenas após a conclusão da transferência integral do arquivo que o usuário verá o filme ou vídeo, escutará a música ou assistirá o programa, de acordo com seu ritmo ou tempo livre. Dependendo de várias condições, esse processo de transferência pode exigir horas ou dias para ser concluído.

Por outro lado, vem crescendo o escopo de aplicações nas quais o usuário tem interesse em programas "ao vivo". Situações tais como eventos esportivos, debates

políticos, conferências ou palestras seguidas de perguntas/respostas são exemplos dessas aplicações, denominadas na literatura como *live streaming* (difusão ao vivo). Nesse caso, as informações são geradas exatamente antes da sua transmissão (não estão disponíveis previamente) e disseminadas em tempo real. Para que se mantenham o interesse e a satisfação dos usuários, é necessário que elas sejam recebidas por eles com atraso mínimo e de forma regular (compassada) para manter a continuidade de exibição.

A tecnologia *peer-to-peer* (P2P) aparece como um suporte interessante para este tipo de transmissão: os participantes colaboram na redistribuição de conteúdos, aproveitando recursos disponíveis na rede e multiplicando a capacidade de difusão à medida que se multiplicam os usuários interessados, contribuindo na escalabilidade. Assim, a multiplicação dessas aplicações de *live streaming* tem ocorrido de forma rápida em países onde a Internet foi implantada recentemente, com moderna tecnologia, como na China: lá, canais de televisão vêm sendo transmitidos a milhares de usuários através dessa tecnologia (http://www.pplive.com). Em outros lugares, como nos EUA, vem crescendo com a migração maciça de usuários que abandonam a rede discada e filiam-se a provedores de conexões em banda larga.

Entretanto, as características abertas da Internet fazem com que algumas dificuldades surjam nesses tipos de aplicações: a liberdade de reunir-se à programação ou desvincular-se a qualquer momento – por perda de conexão ou de interesse – são exemplos. Eles causam impactos sobre parte dos demais nodos (*peers*). Embora o paradigma P2P favoreça a escalabilidade dos sistemas com o crescimento do número de usuários, ele também os deixa vulneráveis a comportamentos oportunísticos. Nodos oportunistas tentam receber o fluxo de dados sem retribuir de forma correspondente, reduzindo assim a capacidade total de *upload* do sistema [Haridasan, Jansch-Pôrto e van Renesse 2008]. Isso pode ocorrer, por exemplo, quando eles não contribuem com a propagação de pacotes – recebem-nos, mas não os retransmitem ou retransmitem preguiçosamente (aquém de sua capacidade ou do que é prescrito pelo protocolo de operação). Além disso, a anonimidade encoraja parte dos usuários a tentar fraudar regras de participação. E ainda o próprio meio de comunicação é sucetível a ruídos, os quais causam corrupção de pacotes, atrasos e desconexões. Essas e outras situações causam problemas nos sistemas de *live streaming* que empregam a Internet como suporte natural para a difusão de informações em tempo real. Logo, resiliência é um requisito-chave para *live streaming* em arquiteturas *peer-to-peer* [Fodor e Dán 2007].

A partir do contexto descrito, o objetivo do presente artigo é o de caracterizar comportamentos anômalos durante o período operacional nesse tipo de aplicações. Vários termos referentes ao comportamento dos diversos perfis de usuários aparecem na literatura: nodos corretos [Castro et al. 2002] [Singh et al. 2004], altruístas [DaSilva e Srivastava 2004], egoístas (do inglês: *selfish* [Hales 2004]), *freeloaders* [Ge et al. 2003], racionais [Shneidman e Parkes 2003], bizantinos [Awerbuch et al. 2002] [Aiyer et al. 2005] [Haridasan e van Renesse 2006] – eles serão estudados aqui, em conjunto com as formas mais conhecidas de burla aos sistemas. Ao longo dessa apresentação, serão feitas algumas reflexões sobre como lidar com esses problemas ou referentes aos desafios que eles apresentam em face do contexto de trabalho.

Logo após esta introdução, seguem informações referentes às aplicações de *live streaming* para fornecer subsídios aos leitores não iniciados na área (Seção 2). Em seguida, é revisada a terminologia usada na área de falhas (Seção 3). Propõe-se então

uma taxonomia para as falhas que refletem o comportamento dos usuários (Subseção 3.2). A Seção 4 explica como são vistas falhas num contexto de *live streaming*, e apresentam-se os perfis de desvios básicos de usuários (não intencionais na Subseção 4.1), com ênfase nas ocorrências intencionais (Subseções 4.2 e 4.3). Comentários sobre a modelagem de falhas completam o conteúdo do artigo (Seção 5), seguido apenas pelo fechamento na Seção 6, de conclusões.

2. Características das aplicações *live streaming*

Nas aplicações de *live streaming*, os conteúdos são gerados "ao vivo" e são então distribuídos para os usuários. Em geral, estes conteúdos são subdivididos em pequenos pacotes com identificação de ordem e codificação, o que permite recuperação de erros limitada. Os usuários vão coletando os pacotes e exibem-nos à medida em que a seqüência de pacotes vai se completando (*playback*). Pacotes excessivamente atrasados não fazem mais sentido aos usuários, pois a seqüência na qual eles seriam inseridos provavelmente já foi exibida – assim, são descartáveis. A quantidade de pacotes recebidos com relação ao número de pacotes enviados, que é dado por um percentual, é dito **índice de continuidade** (*continuity index*). A partir do valor deste percentual pode-se avaliar a qualidade das informações recebidas pelos usuários; entretanto, é necessário ressaltar que este percentual pode variar significativamente entre diferentes usuários em uma rede P2P.

Essas aplicações (*live streaming multicast*), através das quais conteúdos ao vivo são difundidos através de Internet, podem ser baseadas em uma infraestrutura de equipamentos e serviços oferecida pelo provedor do serviço ou em redes P2P. No primeiro (infraestrutura), existe a necessidade de posicionar, em locais estratégicos na Internet, servidores de vídeo e nodos de difusão no nível da aplicação, de tal forma que o vídeo seja transmitido pelos servidores aos nodos especiais e, então, aos clientes. Além de ser cara e exigir considerável esforço de manutenção, esta opção dificilmente permite atender um grupo potencialmente grande (na ordem de milhares) de usuários simultâneos, em virtude da enorme demanda de capacidade de processamento, armazenamento e comunicação exigida de poucos nodos de difusão. Aplicações de difusão que adotam tal estratégia, como as populares YouTube e Yahoo! Video, lidam com tal dificuldade, limitando drasticamente o tamanho dos conteúdos disseminados.

Por outro lado, nas redes *peer-to-peer*, onde os nodos estão conectados através de uma rede lógica (*overlay*), a distribuição não se apoia sobre nodos dedicados: cada nodo atua no recebimento da informação e na sua redistribuição a outros, através da exploração cooperativa da capacidade de *upload* dos nodos. É importante ressaltar que a escolha de uma solução centralizada ou distribuída requer dos projetistas dos sistemas uma avaliação cuidadosa da expectativa de demanda a fim de que possam prover uma aplicação que satisfaça a aspectos como qualidade da informação recebida pelo usuário e desempenho, com baixos atrasos. A quantidade de nodos que participam do *overlay* pode mudar rapidamente; os pacotes precisam ser transmitidos com atrasos fim-a-fim aceitáveis para aplicações "ao vivo", que é em torno de dezenas de segundos; e ainda, para manter aceitável a qualidade do vídeo percebida, a taxa de perda de pacotes precisa ser baixa [Fodor e Dán, 2007].

As duas formas predominantes de organização dos *overlays* são: a) em árvores ou *push-based streaming*; b) organizadas randômicamente, também referidas como *mesh*, *pull-based streaming* ou *data-driven randomized*. Encontram-se ainda

combinações das anteriores: árvores múltiplas ou árvores combinadas com *mesh*, por exemplo. Observe-se que não há como empregar uma única árvore para organizar os nodos pensando em assegurar qualquer nível de resiliência.

Com o uso de árvores, os dados do *streaming* são repassados de pais para filhos, tendo o servidor como raiz. A alternativa de múltiplas árvores tem sido usada: a) para resolver o desbalanceamento de contribuição de nodos internos à árvore e os nodos-folhas; b) para garantir a continuidade de distribuição de pacotes quando nodos internos abandonam a rede; c) para aproveitar a disponibilidade de largura de banda de nodos internos. Dependendo dos critérios usados na escolha dos nodos para a composição das múltiplas árvores, a manutenção pode não ser simples. Além disso, a exploração de uma estrutura definida deixa esta topologia mais suscetível a ataques.

Abordagens que exploram estruturas randômicas, definidas ao longo de sua construção principalmente com base no número médio de vizinhos, distribuem os pacotes através de um método *pull* (ou *swarming*). Os nodos trocam mensagens de controle com seus vizinhos para divulgar os conteúdos disponíveis e receber requisições desses; esse protocolo evita o recebimento de pacotes duplicados de vizinhos diferentes, mas introduz algum atraso (embora ele afete de forma quase regular a todo o conteúdo). Devido à multiplicidade de vizinhos, a estrutura tende a ser resiliente ao comportamento dinâmico dos nodos, pois mantém-se a troca de pacotes enquanto ocorre a manutenção do *overlay*. Sua característica randômica também a torna mais robusta a ataques.

Hoje, há diversos sistemas práticos que permitem o acesso a um grande número de usuários interessados em receber fluxo de dados em tempo real, sem requisitarem quantidade extensiva de recursos. Sistemas recentes tais como Chainsaw [Pai, Kumar, Kamilmani, Sambamurthy e Mohr 2005] e Coolstreaming [Zhang, Liu, Li e Yum 2005] mostraram que o uso de nodos organizados através de um *overlay* de composição randômica (*mesh*) e disseminação de dados *pull-based* pode proporcionar uma boa resiliência a falhas e *churn* [Haridasan e van Renesse 2006], [Magharei e Rejaie 2007]. ***Churn*** é o termo usado para expressar situações nas quais ocorrem múltiplas saídas de nodos participantes simultaneamente.

3. Tipos de falhas

O sistema aqui considerado é composto por um conjunto numeroso de máquinas, ou nodos, que correspondem a usuários interessados nos serviços disponíveis, conectadas à Internet. A tecnologia de conexão é baseada no paradigma *peer-to-peer* (P2P): os nodos estão interessados em receber conteúdos e por isso se dispõem também a disseminá-los entre os demais participantes, cooperando na distribuição e, portanto, reduzindo a quantidade de trabalho do servidor principal ou *source* (fonte de dados, único, dedicado, em geral; também denominado *seed* ou *root*). A comunicação entre participantes é definida através de uma rede *overlay*, que pode explorar diferentes formas de conexão (e.g., árvore, *mesh* ou combinações dessas). A escolha do paradigma P2P, assim como as características da Internet, fazem com que diferentes cenários de falhas produzam variados defeitos nessas aplicações.

3.1 Terminologia empregada na caracterização de falhas

Para a definição dos termos referentes à classificação de falhas, é tomado por base a taxonomia empregada por Avizienis et al. (2004) e repete-se a definição dos essenciais,

a seguir, para facilitar ao leitor. Está sendo empregado aqui o termo falha em correspondência ao que figura como *fault* (no inglês), naquela referência. Falhas **operacionais** aplicam-se às anomalias quanto à fase de ocorrência: o termo é usado para caracterizar aquelas que ocorrem durante o fornecimento do serviço, na fase de uso. Quanto à causa fenomenológica, as falhas podem ser **naturais**, quando são causadas por fenômenos naturais, sem a participação de pessoas, ou **humanas,** quando resultam de ações praticadas pelos seres humanos. Quanto ao objetivo, as falhas podem ser **maliciosas**, quando são introduzidas por humanos com o objetivo doloso, ou seja, de causar prejuízo ao sistema; ou **não-maliciosas**, as quais são introduzidas sem objetivo de prejudicar o sistema. As falhas ainda podem ser caracterizadas como **deliberadas** (**intencionais**), se resultam de uma decisão nociva; ou **não-deliberadas** (**não-intencionais**), quando são introduzidas de forma inconsciente ou inadvertida.

O escopo do presente artigo restringe-se ao tempo em que o sistema está em operação – de tal forma que todas as falhas podem ser enquadradas como operacionais. Não serão tratados aqui problemas que ocorrem durante a fase de projeto dos sistemas, que se contrapõem às falhas operacionais, na classificação quanto à fase de criação ou ocorrência.

Nodos que abandonam o sistema durante a transmissão (antes do seu encerramento) podem fazê-lo por perda de interesse ou por uma desconexão, por exemplo. No primeiro caso, pode-se falar em falha humana, não maliciosa e não deliberada: o usuário decide desvincular-se, mas, na maior parte das vezes, não percebe o seu papel no contexto da distribuição. No segundo caso, trata-se de falha natural. Em ambos casos, o comportamento pode ser representado através de colapso (*crash*). Cabe observar ainda que, nos casos de desconexão, é bastante provável que o usuário decida retornar ao sistema; dependendo de como o sistema tratar estes retornos, pode-se falar em colapso com recuperação (*crash-recover*). A corrupção de pacotes devido a ruídos no meio físico é outro exemplo de falha natural.

Falhas humanas maliciosas e deliberadas (ou intencionais) podem ser exemplificadas por nodos que retransmitem conteúdos inválidos (“lixo”) com o intuito de dissimular baixos níveis de contribuição; nodos que se associam a outros, privilegiando os “amigos” na redistribuição de pacotes; ou nodos que saem do sistema e retornam sob nova identidade para se desvincularem de má reputação obtida depois de terem exibido comportamentos inadequados, tais como os descritos na seção 4, subseções 4.2 e 4.3. Nesses casos, o comportamento é bizantino e complexo quanto à modelagem. *Softwares* mal configurados também correspondem a situações de comportamento bizantino, mas em boa parte dos casos são caracterizados como falhas humanas, não-maliciosas e não-deliberadas, pelo menos nos casos em que as deficiências de configuração devem-se à falta de conhecimento do usuário ao instalar o *software*.

3.2 Taxonomia comportamental dos usuários

No contexto de *live streaming*, as situações de falhas têm sido associadas majoritariamente ao comportamento dos usuários; é atribuída pouca atenção a anomalias nos programas de aplicações que lhes dão suporte. Este enfoque é mantido ao longo deste artigo. Um olhar possível sobre os participantes da rede de difusão de conteúdos pode subdividí-los quanto ao seu comportamento nos grupos citados e explicados a seguir.

Quanto à forma de participação – ou quanto ao comportamento cooperativo – os nodos podem ser caracterizados como corretos (incluem os altruístas), oportunistas (incluem os *freeloaders*, racionais, ou egoístas, que são todas denominações que exploram relaxamento nos mecanismos de controle do sistema) ou bizantinos.

Nodos **corretos** são aqueles que cumprem fielmente o protocolo definido para sua atividade – basicamente, eles solicitam dados na medida das necessidades e enviam dados de acordo com as requisições que recebem. Os nodos **altruístas** podem ser vistos como um subgrupo dos nodos corretos, os quais, nesse caso, estão dispostos a fornecer mais dados do que lhes é requisitado (contribuições espontâneas). Aiyer et al. (2005) sugerem que os nodos altruístas refletiriam apenas a existência de "bons samaritanos" e nodos fonte (*source*) em sistemas reais, mas não os permitem contribuir acima do especificado no protocolo.

O termo **oportunista** foi usado por Haridasan, Jansch-Pôrto e van Renesse (2008) para identificar nodos que tentam fornecer menos dados que eles forneceriam se exibissem um comportamento de nodos corretos, com a intenção de maximizar a relação entre a quantidade de dados obtida e o custo unitário destes. Essa relação pode ser maximizada quando eles buscam acesso aos dados que são distribuídos na rede, mas ignoram o atendimento às requisições recebidas. Não havendo mecanismos de controle, eles podem permanecer apenas desfrutando dos benefícios, enquanto o sistema sobreviver, já que o crescimento de usuários deste tipo condena o sistema à inanição. Outras caracterizações encontradas na literatura e que podem ser enquadrados no contexto de "oportunistas" aparecem sob as denominações: *freeloaders*, racionais, ou egoístas (*selfish*). Talvez seja possível agrupar o uso dos termos *freeloader* e *selfish*, citados na literatura, como sendo associados a um uso totalmente irresponsável dos recursos com o consumo de dados sem qualquer retribuição, se possível. O termo **racional** (tal como usado em BAR Gossip [Li, et al. 2006]) têm sido associado a nodos que seguem estritamente as regras de uso do sistema, se o seu desrespeito significar punição ou algum tipo de medida que implique em prejuízo na sua atividade de trocas. Logo, eles se desviam das regras apenas se com isso puderem maximizar seus ganhos.

Os nodos racionais têm por objetivo maximizar os seus benefícios de acordo com uma função-utilidade conhecida. Em economia, uma função-utilidade mede o nível de satisfação auferida por um consumidor a partir do consumo de um dado bem (ou um conjunto de bens). Em difusão de conteúdos, a função-utilidade está relacionada a custos que o nodo enfrenta com a sua participação; pode ser avaliada em ciclos de computação, área de armazenamento, largura de banda empregada, *overhead* associado ao envio e recebimento de mensagens, consumo de potência, sanções financeiras, ou vantagens decorrentes de sua participação no sistema, tais como armazenamento remoto, serviços de rede ou ciclos computacionais. Desvios com relação ao protocolo só ocorrem se isso acarretar benefício ao nodo racional, isto é, se o descumprimento fizer com que ele aumente a sua função-utilidade. Os nodos racionais também podem ser enquadrados como um subgrupo dos bizantinos pois, ao se desviar do protocolo definido, sua forma de atuação não faz parte do modelo do sistema.

Nodos **bizantinos** são aqueles que se comportam de uma forma completamente arbitrária, inclusive atuando em seu próprio prejuízo; logo o seu modelo de atuação é ignorado *a priori*. Possuem funções de utilidade arbitrárias e desconhecidas, decorrentes de configuração inadequada, mau funcionamento, problemas de programação, ou como

resultado de comportamento malicioso. Observe-se que o comportamento bizantino não pressupõe benefícios obtidos a partir do descumprimento do protocolo: é possível inclusive que ele siga uma estratégia que resulte em perdas incluindo ataques de negação de serviço (*Denial-of-Service*, DoS).

Em BAR Gossip [Li, et al. 2006], o primeiro artigo a propor um modelo que reúne nodos altruístas, racionais e bizantinos, os altruístas foram restringidos ao "cumprimento rígido do protocolo", sem poder contribuir de forma extra. Lá, eles diferenciam-se dos racionais apenas porque não se desviam do protocolo, nem com objetivo de ampliar benefícios do conjunto de participantes. Contribuições espontâneas iriam perturbar completamente o protocolo proposto. A convivência de nodos altruístas com oportunistas iria fazer com que os oportunistas explorassem, a seu favor, a "boa vontade" dos altruístas. Assim, com a existência destes, os nodos racionais não seriam obrigados a fazer trocas justas, tendo boas razões para desviar-se do seu comportamento definido pelo protocolo do sistema, já que a "exploração" dos altruístas aumentaria a função-utilidade dos racionais na obtenção de informações. Logo, protocolos que prevejam a convivência de nodos altruístas com racionais precisam ter características de adaptação dos níveis de contribuição dos nodos em função dos perfis de composição de participantes. Como é difícil conhecer esta composição *a priori*, apenas o monitoramento das condições da rede – ou da qualidade das informações recebidas – pode ser usado para esta adaptação, através de mecanismos de auditoria, por exemplo.

Quanto ao estado da conexão, pode-se falar em nodos ativos ou inativos. Os primeiros estão fisicamente conectados, participam das atividades recebendo pacotes e redistribuindo (de acordo com a sua forma de participação), e respondem a mensagens de controle. Os que se apresentam inativos, não respondem a qualquer tentativa de comunicação. Portanto, não consomem recursos mas tampouco contribuem na difusão de conteúdos. Precisam ser identificados e removidos já que distorcem os parâmetros relacionados à composição do *overlay*.

Quanto ao momento de conexão, os nodos podem solicitar participação no *overlay* a partir do início da transmissão, fazê-lo de forma tardia (durante a transmissão, após o seu início), podem retirar-se de forma prematura (quando a transmissão ainda está em andamento), ou ao final da transmissão. Os nodos que vêm e vão, respectivamente, no início da transmissão e ao seu final, não apresentam problemas ao sistema já que (se cumprirem o protocolo de difusão) participam de todas as fases, exceto quando um grande número deles chega simultaneamente (***flash crowd***). Os desafios estão relacionados aos procedimentos de manutenção do *overlay* que são necessários para incluir e atualizar os nodos que chegam tardiamente ao sistema, e para manter em nível aceitável o índice de continuidade nos nodos vizinhos ou dependentes dos que saíram prematuramente do sistema, principalmente quando isso ocorre em grupos (*churn*).

4. Falhas no contexto de *live streaming* (conceitos e técnicas usadas)

As instabilidades em conexões efetuadas através da Internet, o desinteresse dos usuários nas aplicações, e erros dos aplicativos ou no *software* podem determinar a desconexão dos usuários, resultando em comportamentos semelhantes ao que tradicionalmente é classificado como colapso ou falha de conexão (*link*). Por outro lado, o espírito "aproveitador" de usuários, que esperam apenas benefícios ao baixar pacotes e não distribuí-los em reciprocidade também vai causar problemas ao princípio cooperativo

proposto. Adicionalmente, participantes que tentam se aproveitar do interesse dos usuários para modificar pacotes e difundem, por exemplo, propaganda ou simplesmente lixo, também acarretam problemas às aplicações.

Assim, quando examinados quanto à forma de participação (ou espírito cooperativo), encontrar-se-á a possibilidade de que os nodos exibam comportamentos corretos (incluindo altruístas), oportunistas ou bizantinos. Mas não é possível identificar inequivocamente estes comportamentos em associação com os nodos, ou seja, "rotulá-los". Então avaliar a capacidade funcional do sistema diantes de diversas relações entre estes grupos, com estimativas quanto à sua composição percentual, é um enfoque possível. Os desvios de comportamento podem se dar por falhas humanas maliciosas ou não – mas a existência do interesse em prejudicar o sistema não é explícita; logo não pode ser alvo de análise. Assim, emprega-se nesse artigo apenas a divisão em falhas deliberadas (ou intencionais) ou não-deliberadas (não-intencionais).

Uma outra abordagem possível é quanto ao momento de conexão. Neste caso, embora as desconexões possam ocorrer voluntariamente, é difícil vincular este motivo ao modelo. Pode-se inferir motivação para a saída quando a qualidade é baixa, mas não há como confirmar as suspeitas. Após a conexão, e até que haja a desvinculação, os nodos são associados ao estado de conexão ativo.

4.1. Caracterização dos perfis básicos de falhas não intencionais

Os tipos de falhas não intencionais que se manifestam no contexto em estudo, em sua maioria, são decorrentes de: ruídos e congestionamentos no meio de comunicação, que causam erros no conteúdo dos pacotes recebidos ou perda (não recebimento) desses; ou fraca vinculação dos usuários, que faz com que haja uma dinâmica bastante intensa na composição do *overlay*. As entradas e saídas extemporâneas são tratadas como eventos indesejados e randômicos – portanto, enquadrados como falhas também. Esses aspectos são abordados a seguir.

Devido à natureza dos conteúdos multimídia, sua transmissão é bastante suscetível a erros [Meddour, Mushtag e Ahmed 2006]. Por outro lado, o grande volume de dados e a tolerância do usuário a um baixo nível de distorção fazem com que não se justifique incorporar codificação extensa a essa informação. Além disso, para que a recepção seja adequada, é necessário empregar um esquema bem planejado de codificação de vídeo confiável, de tal forma que a transmissão seja suficientemente flexível para adequar-se à dinâmica das redes P2P e sua heterogeneidade [Yang, et al. 2006]. Yang et al. dividem os conteúdos em dois níveis hierárquicos: enquanto as informações fluem adequadamente, ambos níveis são transmitidos. À medida que são identificados congestionamentos e possíveis atrasos decorrentes desses, apenas as informações de maior hierarquia são enviadas, reduzindo a qualidade do vídeo conforme percebido pelo usuário final. Os pacotes transmitidos precisam ainda incorporar codificação suficiente que permita a percepção da perda de pacotes ou sua alteração, a fim de que o protocolo possa tratar erros ou solicitar a retransmissão.

O comportamento de usuários finais da Internet é completamente imprevisível. Como participantes interessados em uma transmissão em curso, pode-se imaginar que a maior parte associa-se à difusão em seu horário inicial e desvincula-se ao seu final. Entretanto, não há observação suficiente sobre esse comportamento – e alguns estudos publicados não confirmam plenamente essa intuição. Adicionalmente, tomando-se por

base aplicações que envolvam programação de televisão, por exemplo, um bom percentual de usuários apenas se conecta para verificar se há algo de interesse ou se o programa alvo é “bom”, o que é julgado a partir de uma amostra. O terceiro aspecto é uma suspeita de que a desvinculação prematura de usuários pode ocorrer devido à insatisfação com a qualidade das informações recebidas, no que se refere a índice de continuidade, e atrasos no *playback*. Esses usuários podem tentar retornar novamente ao sistema e, dependendo dos critérios de composição do *overlay*, eles observam alguma melhora (ou não, piorando a qualidade de recepção), ou podem simplesmente desistir, abandonando definitivamente a rede. Mais tarde (seção 4.3), será visto que ainda existem outras razões para saída prematura causadas por falhas bizantinas.

Devido a essa natureza dinâmica dos usuários de redes P2P e à liberdade dos usuários quanto aos momentos de ingresso e abandono da rede (e, por conseqüência, da transmissão e redistribuição), sem notificação prévia aos demais, a gerência desse tipo de sistemas necessita de características que os façam reagir adequadamente às demandas provocadas por esse comportamento. As descontinuidades locais na distribuição dos pacotes não devem afetar a percepção daquilo que é recebido pelos demais usuários, ou seja, a regularidade no fluxo de pacotes deve ser mantida em nível suficiente para atenuar os impactos sobre a taxa de *playback* durante a sessão correspondente. Há necessidade de empregar mecanismos que sejam simultaneamente robustos e adaptativos para lidarem com essa dinâmica da rede. Alguns trabalhos mencionam esses cuidados, mas talvez um dos maiores problemas seja o de que ainda não se dispõe de uma modelagem efetiva associada a este comportamento que possa ser usada para comprovar a eficiência das técnicas propostas.

Os dados referentes ao comportamento dos usuários ainda são bastante limitados, já que a maior parte das aplicações de *live streaming* ainda opera em níveis experimentais. Assim, a obtenção de dados ainda pode estar contaminada por tendências, motivação da população para associar-se à transmissão, entre outras.

Liao et al. (2006) apresentam alguns dados relacionados a experimentos conduzidos com o AnySee, um sistema desenvolvido para distribuição de pacotes em *live streaming* que busca ter como características básicas eficiência e escalabilidade. Este sistema vem sendo usado na China e, de acordo com a referência citada, mais de 60 mil usuários têm tido acesso a programas de televisão, filmes e conferências acadêmicas. Segundo eles, não há uma relação comprovada entre o interesse dos usuários (e conseqüente permanência no sistema) e atrasos na distribuição de informações. Entretanto, estes dados podem ser questionados diante dos aspectos explicados a seguir: a) as amostragens são pequenas e talvez com um certo componente de tendência: foram realizadas em sete momentos diferentes (*hot periods*) sobre três programas selecionados. Não há informações sobre o conjunto de usuários observados e em que condições foram colhidas as amostras, por exemplo. Mas há menção a 7200 usuários de mais de 40 universidades em 14 cidades da China - ou seja, não se tratavam de usuários domésticos comuns; b) os atrasos considerados para tirar conclusões sobre o comportamento dos usuários estão na ordem de dezena de segundos. São valores médios, sem qualquer informação adicional sobre o desvio padrão e intervalo de confiança - portanto, são dados estatisticamente muito pobres. Assim, os cerca de 10% de usuários que abandonam o sistema não causam um impacto significativo sobre as demais características do sistema e ajudam a compor os gráficos apresentados como resultados experimentais.

Liu, Rao e Zhang (2008) apresentam um ponto de vista diferente de Liao et al. (2006). Eles afirmam que, se a qualidade do vídeo não é adequada durante ao período inicial de distribuição, é bastante provável que o usuário abandone o sistema, sendo possível inclusive a ocorrência de *churn*. Esse abandono maciço tende ainda a realimentar os problemas de distribuição e incentivar mais usuários a se desvincularem. Além deste comentário, eles ainda fazem algumas suposições estatísticas referentes ao ingresso de usuários no início de uma transmissão: se um milhão de interessados se reunirem ao sistema no início da transmissão – nos primeiros 100 segundos – a taxa de pico de chegada será de 10.000 nodos por segundo. Trata-se de um problema real de escalabilidade para associar eficientemente à rede os nodos interessados.

4.2. Um ambiente para falhas intencionais

Matteo Dell'Amico (2006) comenta alguns problemas decorrentes das características das redes P2P. Um deles é a ausência de conhecimento global sobre a rede: em ambientes grandes, além de ser provavelmente desprovido de interesse, é impossível aos participantes manterem conhecimento sobre cada interação que ocorre no sistema. Enquanto isso simplifica a operação, abre um campo expressivo para problemas de segurança. Problemas apontados por ele são ataques do tipo *whitewashing* e conluio (*collusion*), que serão vistos nesta seção (subseção 4.3).

Em ambientes distribuídos abertos, tal como ocorre com os sistemas construídos sobre a Internet, e principalmente naqueles que cujos participantes são conjuntos de nodos altamente dinâmicos, abre-se a possibilidade a uma entidade qualquer aparecer sob diferentes identidades. Isso se constitui em ameaça à segurança e precisa se tratada por mecanismos próprios. É preciso lembrar que boa parte das hipóteses empregadas tradicionalmente em dependabilidade repousam sobre a premissa de que os participantes são independentes e detêm identidades diversas. Entretanto, será visto que alguns cenários resultantes de ataques não se enquadram nesse tipo de hipótese [Androutsellis-Theotokis e Spinellis 2004].

Adicionalmente, pode-se dizer que as falhas intencionais constituem a classe mais rica em função das possibilidades de comportamento. Não se pode antecipar todas as variantes que a imaginação humana irá produzir. Nessa seção, serão caracterizados as formas de comportamento mais conhecidas, tipos de impacto que elas podem causar e algumas abordagens que têm sido usadas para conter ou minimizar os prejuízos decorrentes destes tipos de ataques.

Enquanto seguem estritamente o protocolo, os nodos racionais (subseção 3.2) não deveriam oferecer problemas ao sistema, já que um protocolo bem construído assegura que as ações mantenham um balanço equilibrado entre contribuição e obtenção de conteúdos. Entretanto, eles seguem as regras apenas se correrem riscos no descumprimento e enquanto não descobrirem desvios admissíveis. Mecanismos para restringir as ações oportunistas incluem o uso de auditores, que controlam os níveis de contribuição dos participantes, e o enfoque *tit-for-tat*, no qual um nodo apenas envia dados a outro nodo se recebe um montante em retorno ou pagamento. Mas uma rede aberta e dinâmica (que oferece a possibilidade de retorno a participantes, o que inclui ex-infratores) dificulta o controle dos indivíduos e o emprego de mecanismos disciplinadores. Por consequência, não estimula a manutenção do papel correto, sem desvios. Até o momento, não se tem conhecimento de uma solução adequada substitutiva ao *tit-for-tat* porque, em atividades de baixíssimo valor financeiro por

unidade de transferência (remuneradas através de *micropayments*) como é o caso dos pacotes em *live streaming*, a manutenção dos mecanismos é muito cara frente à aplicação. Técnicas de auditoria ativadas apenas quando a qualidade dos índices de continuidade estão descendo a patamares perigosos (próximos dos níveis mínimos aceitáveis) foram sugeridos por Haridasan, Jansch-Pôrto e van Renesse (2008). Os resultados apresentados são promissores e a estimativa de impacto no custo do sistema mostra níveis adequados. Ainda é importante ressaltar que qualquer desvio no comportamento de um nodo racional o desloca para um comportamento bizantino – sendo que assim a antecipação do modelo de comportamento fica bastante complexa.

4.3. Caracterização de perfis básicos de falhas intencionais (bizantinos)

Uma das razões para usuários terem interesse em exibir identidades múltiplas é livrar-se de ações inadequadas cometidas no passado. Essas ações podem ter sido, por exemplo, a omissão em contribuir na distribuição de conteúdos (referidos como *omission attacks*, [Haridasan e Van Renesse 2006]) e serem flagrados pelos mecanismos de incentivos empregados no sistema. Ou pode ser que ações indevidas e o descumprimento de promessas, medidos por mecanismos de avaliação, os classifique mal através de parâmetros de reputação utilizados. O retorno ao sistema sob nova identidade poderia ser uma alternativa de voltar a desfrutar dos benefícios; outra é o uso simultâneo de múltiplas identidades que sirvam para atuação sob perfis diversos.

Quando há liberdade na criação de identidades, e essas podem ser usadas de forma proveitosa por quem as detêm, alguns usuários podem valer-se dessa fragilidade do sistema em benefício próprio criando múltiplas identidades. Esse tipo de ação foi definida por Douceur (2002), sob a denominação de ***Sybil attack***. Hipoteticamente, se uma única entidade defeituosa pode atuar apresentando-se através de diversas identidades, ela pode controlar uma parte significativa do sistema, minando os meios de redundância usados para sua proteção. Uma forma de prevenir esses ataques é manter identidades certificadas através de uma agência confiável, o que só é obtido em cenários reais através de uma autoridade lógica centralizada.

Infraestruturas centralizadas ou de gerência de identidade podem, portanto, minorar o problema; entretanto são soluções difíceis de implementar na prática [Piatek, Anderson e Krishnamurthy 2007]. Por consequência, esses autores propõem que à simples obtenção de identidades não sejam atribuídos quaisquer dados ou elementos de valor (como forma de *bootstrapping*), de tal forma que o usuário não obtenha vantagem dessa ação. Eles propõem o uso de mecanismos de incentivo, mas resta ainda em aberto a forma de inicialização de novos participantes. Num contexto de *live streaming*, o usuário pode obter vantagem de múltiplas identidades se, ao entrar no sistema, ele receber imediatamente conteúdos de atualização de forma que possa integrar-se às demais atividades. Por outro lado, sem dados, um nodo ingressante tampouco pode contribuir com os seus vizinhos.

Uma outra alternativa seria o uso de técnicas de identificação que consumam muitos recursos – de tal forma que não sejam atrativas para uso prático pelos atacantes [Androutsellis-Theotokis e Spinellis 2004]. Entretanto, há necessidade de considerar os custos envolvidos aos usuários regulares do sistema (usuários P2P comuns), e não menosprezar a capacidade daqueles que desejam servir-se maliciosamente dele.

Para que seja mantida a operação correta do *overlay*, é necessário que os nodos corretos mantenham seu potencial de comunicação e repasse de mensagens através dos *links*. Esta capacidade é o alvo de participantes maliciosos que isolam nodos corretos, ou os "eclipsam" (***eclipse attacks***) através do preenchimento da tabela de vizinhos de um membro correto com endereços de participantes maliciosos. Assim, se o atacante controlar uma fração significativa de conjuntos de vizinhos de nodos corretos, ele impede este nodo de receber mensagens endereçadas a ele. A expansão exagerada deste controle poderia resultar inclusive no controle integral do tráfego no *overlay* pelo atacante [Singh, et al. 2004]. Este ataque pode ser iniciado a partir de um Sybil *attack*, seguido do preenchimento da tabela de vizinhos de nodos corretos com identificação de nodos aparentemente distintos. Se combinado com o protocolo de manutenção para a substituição de nodos defeituosos, pouco a pouco os maliciosos vão dominando a rede.

Defesas contra este tipo de ataques incluem a proposta de Castro et al. (2002), voltada para *overlays* estruturados, que impõem o uso de restrições estruturais fortes em sua composição. Uma desvantagem é que estas restrições impedem a implantação de otimizações visando melhorar o desempenho. Singh et al. (2004) propuseram uma outra forma para evitar este tipo de ataque pelo estabelecimento de limites (*thresholds*) conjuntos na análise dos graus de entrada e saída dos membros da comunidade P2P. Juntamente com a implementação deste mecanismo, é necessário um sistema de auditoria que impeça os nodos maliciosos de mentirem sobre os valores dos seus graus de entrada e saída. De acordo com os autores, a técnica não é particular a qualquer tipo de estrutura, além de permitir o uso de otimizações baseadas em métricas tais como proximidade física, necessária para a eficiência do *overlay*.

Um outro tipo de ataque – ***whitewashing*** – consiste da obtenção de nova identidade na vinculação (ou retorno) à rede, simulando ser um neófito ao desfazer-se do histórico anterior. Esse procedimento faz com que nodos possam desvincular-se de má reputação obtida a partir de "mau comportamento". Isso tem sido uma operação cujo custo (tipicamente) é baixo, o que acaba sendo do interesse de nodos maliciosos que apresentam histórico de não-contribuição ou de ações indevidas. É desincentivado, entretanto, quando nodos recentes não recebem privilégios de ingresso, mas precisam prestar serviços ou pagamentos para receber benefícios [Friedman e Resnick 2001]. Procedimentos simplificados e rápidos na saída e entrada de nodos funcionam como convite a esse tipo de procedimento. Portanto, buscar uma relação de compromisso na qual as facilidades não estimulem atacantes mas apresentem exigências adequadas a usuários regulares (honestos) é um desafio.

Na classe de ataques por falsificação (*forgery*), citado por Haridasan e van Renesse (2006) estão os ataques que envolvem a fabricação e adulteração de dados que estão sendo difundidos através do sistema. Os mecanismos de contenção deste tipo de ataques operam com base em uma infraestrutura de chave pública. O problema é o custo deste mecanismo de assinaturas, muitas vezes proibitivo numa aplicação de *streaming*, sendo reduzidos a protocolos mais simples para autenticação de dados.

Ataques por **conluio** (***collusion attacks***) ocorrem como resultado da conspiração de um grupo de participantes maliciosos; eles realizam, de forma combinada, uma ação, ou conjunto dessas, de forma a obterem benefícios para si ou para participantes do grupo. Essas ações podem ser de diferentes naturezas: por exemplo, os nodos podem introduzir informações incorretas em seu histórico, de forma a criar ataques que visam

aumentar ou diminuir artificialmente a reputação de alguns nodos. Um reforço para a resiliência com relação a este tipo de ataques é obtido pela associação de maior peso aos votos gerados por nodos de maior reputação no sistema [Dell'Amico 2006]. Na difusão de arquivos ou de *streaming*, a atuação de um grupo em conluio tipicamente se dá pelo repasse de conteúdos ou informações apenas a participantes que fazem parte do grupo, deixando à míngua os demais.

Os ataques por conluio não precisam ser necessariamente efetivados por participantes diversos, mas podem resultar da criação de múltiplas identidades espúrias relacionadas a um participante – e neste caso enquadram-se no conceito de *Sybil Attack*.

5. Comentários em aspectos de modelagem de falhas

Estabelecer modelos correspondentes adequados para a representação dos diferentes tipos de falhas não é tarefa fácil, devido à imprevisibilidade de comportamento, do tipo de mecanismo que será alvo de ataque e do próprio objetivo dos atacantes (por exemplo, nodos bizantinos podem "decidir" atuar em seu próprio prejuízo). Por esse motivo, autores têm estimado algumas situações particulares a fim de estudarem o impacto de falhas sobre os sistemas de *live streaming*.

Uma outra dificuldade é estimar *a priori* a distribuição dos perfis de desvio em diversos sistemas – por exemplo, estabelecendo a composição entre nodos corretos, racionais e bizantinos numa rede aberta. De acordo com os autores de BAR Gossip [Li, et al. 2006], os participantes racionais corresponderiam à maioria dos participantes em um sistema P2P através de múltiplos domínios administrativos. Entretanto, esta afirmativa não é sustentada por qualquer tipo de avaliação. Pode-se imaginar que seja resultado do protocolo estabelecido inicialmente, e que a maioria dos usuários instala em sua configuração básica (*default*); mesmo assim, não há como antecipar desvios sobre este quadro.

Assim, na tentativa de estudar sistemas cujos perfis de composição sejam variados, alguns trabalhos mais recentes modelam as interações entre os diferentes perfis de usuários através da teoria conhecida como "Equilíbrio de Nash" [Nash 1950] e/ou de modelos originados na Teoria de Jogos. Uma das desvantagens das propostas baseadas no trabalho de Nash é que os seus fundamentos repousam sobre um ambiente limitado (ou fechado) e conjuntos de regras que são conhecidos por todos os participantes. Assim, conluios (nos quais existe coordenação de nodos através de regras "extra-sistema" e válidas apenas para sub-grupos) não se enquadram nesse modelo. A teoria de jogos parece ser promissora já que vem sendo ampliada com inspiração em atividades conduzidas através da Internet, e portanto num cenário bastante semelhante aos de difusão de conteúdos, sejam eles ao vivo ou não. Mas a modelagem de aplicações de rede e de difusão de arquivos, através desta teoria, ainda é incipiente.

Outras alternativas mais simplificadas têm sido encontradas em trabalhos que buscam estudar o efeito do comportamento malicioso em ambientes de difusão de *live streaming*. Num exemplo usado para simulações de comportamentos maliciosos, Haridasan e van Renesse (2006) consideram quatro tipos de ataques: a) os nodos agem como totalmente falhos, não requisitando pacotes nem atendendo solicitações; ou b) solicitam pacotes mas não os repassam; ou c) eles sobrecarregam os vizinhos com a solicitação de grande quantidade de pacotes (tantos quantos forem possíveis); ou ainda d) eles sobrecarregam os vizinhos com a solicitação de grande quantidade de pacotes e

não os repassam. Portanto, a última opção é a que mais prejudica o sistema. Cada um dos cenários usado separadamente é estudado com a variação percentual dos participantes maliciosos.

Em BAR Gossip, Li, et al. (2006) modelaram nodos maliciosos para estudar um cenário de conluio perfeito, no qual todos nodos participantes do ataque difundem as atualizações, de forma imediata ao recebimento, apenas ao seu grupo. Isso coloca em risco a distribuição de informações aos nodos não participantes do grupo, pois não existe mais a reciprocidade nas trocas. No cenário lá apresentado, os nodos participantes do conluio são considerados racionais, enquanto os demais são altruístas. Isso significa que os conspiradores apenas recebem pacotes (enquanto for do seu interesse, seguindo o protocolo racional) quando interagem com nodos não-conspiradores, enquanto que os externos ao grupo seguem fielmente o protocolo. Os resultados ali apresentados mostram que o sistema torna-se inutilizável apenas quando os nodos conspiradores atingem 50% da população. Ao negar trocas com os não envolvidos na trama, os nodos em conluio vão minando a distribuição de dados: num caso limite, eles terão eliminado todos os nodos não envolvidos e terão que atuar em trocas de forma completa para continuar a sobreviver.

Os próprios autores [Li, et al. 2006] constataram problemas associados a grupos muito grandes, os quais necessitam de maior largura de banda e geram maior latência na difusão das informações a todos os membros do grupo. Além disso, uma análise da modelagem proposta àquele sistema permite inferir que ela favorece o cenário de conluio na medida em que os nodos externos ao grupo continuam repassando pacotes apesar de não obterem qualquer vantagem nas trocas ou mesmo usufruírem de sua realização (uma vez que recebem apenas lixo). Um cenário com nodos apenas racionais (com um subgrupo envolvido no conluio) não permitiria tal expansão, pois o grupo rapidamente perderia seus “alimentadores”. Um aspecto estranho na análise apresentada é que os participantes do conluio são classificados como racionais; entretanto, na medida em que difundem dados aos participantes do grupo de forma “gratuita”, eles não estão maximizando o seu benefício individual, o que é de certa forma contraditório no modelo (racional) considerado. Um nodo participante do conluio “esforça-se” para obter dados dos externos ao grupo mas atua como “um bom samaritano” frente ao seu grupo, doando dados.

Ao modelar nodos bizantinos para avaliar seu impacto sobre os sistemas, Li et al. (2006) pressupõem que o objetivo desses é inverso ao de qualquer participante racional, fazendo com que eles aumentem o custo e diminuam seus benefícios com relação ao perfil racional. Certamente, trata-se de um modelo bastante simplificado frente às possibilidades que um nodo bizantino pode “criar”, mas é um ponto de partida.

6. Conclusões

Quando comparados aos sistemas tradicionais de difusão de arquivos via Internet, as aplicações de *live streaming* agregam exigências por suas condições de tempo real e escalabilidade: os pacotes enviados precisam chegar ao grande número de usuários com regularidade e pequenos atrasos. Assim as soluções de gerência do sistemas e os mecanismos usados para conter os efeitos das falhas precisam ser eficientes e leves, de forma a não prejudicar o sistema.

Foram discutidos os principais tipos de falhas que afetam as aplicações de *live streaming*, incluindo um enfoque comportamental e outro temporal, além de caracterizar as principais modalidades de ataques que são usadas de forma intencional. Também foram enfocados os problemas de modelagem de falhas nestes ambientes, quanto às abordagens e falta de dados reais (ainda) neste escopo de aplicações.

Há vários problemas que restam em aberto no tratamento de falhas deste grupo de aplicações e tratam-se ainda de desafios bastante interessantes, embora novas propostas estejam surgindo rapidamente numa área de pesquisa que se apresenta altamente dinâmica.

Referências

Androutsellis-Theotokis, S. and Spinellis D. (2006) "A Survey of *Peer-to-peer* Content Distribution Technologies." *ACM Computing Surveys* v. 36, n. 4, December, pp. 335-371.

Avizienis, A., Laprie, J.-C., Randell, B. and Landwehr, C. (2004) "Basic Concepts and Taxonomy of Dependable and Secure Computing." *IEEE Transactions on Dependable and Secure Computing*, v. 1, n. 1, pp. 11-33.

Awerbuch, B., Holmer, D., Nita-Rotaru C., and H. Rubens (2002) "An On-demand Secure Routing Protocol Resilient to Byzantine Failures". *Proceedings of the 1st ACM Workshop on Wireless Security*. Atlanta, GA. pp. 21-30.

Ayer, A. S., Alvisi, L., Clement, A., Dahlin, M. Martin, J. P. and Porth, C. (2005) "BAR Fault Tolerance for Cooperative Services." *SIGOPS Oper. Syst. Rev.*, v.39, n. 5, October, pp. 45-58.

Castro, M., Druschel, P., Ganesh, A., Rowstron, A. and Wallach, D. S. (2002) "Secure Routing for Structured P*eer-to-Peer* O*verlay* Networks." *Proc. of the 5th Symposium on Operating Systems Design and Implementation (OSDI)*. Boston, MA. pp. 299-314.

DaSilva, L. A. and Srivastava, V. (2004) "Node Participation in Ad Hoc and Peer-to-Peer Networks: A Game-Theoretic Formulation". *Proceedings of the First Workshop on Games and Emergent Behaviors in Distributed Computing Environments*. Birmingham, UK.

Dell'Amico, M. (2006) "Neighbourhood Maps: Decentralised Ranking in Small-World P2P Networks." *Proceedings of the Hot Topics in Peer-to-peer Systems (HoTP2P2006)*.

Douceur, R. (2002) "The Sybil *attack*." *Proceedings of the First International Workshop on Peer-to-peer Systems (IPTPS)*. Springer Berlin / Heidelberg, Cambridge, MA, USA, pp. 251-260.

Fodor, V., and Dán, G. (2007). "Resilience in Live *Peer-to-peer* Streaming." *IEEE Communications Magazine*, v. 45, n. 6, June, pp. 116-123.

Friedman, E. J., and Resnick, P. (2001) "The Social Cost of Cheap Pseudonyms." *Journal of Economics & Management Strategy* v.10, n.2, August, pp. 173-199.

Ge, Z., Figueiredo, D. R., Jaiswal, S., Kurose, J., Towsley, D. (2003) "Modeling Peer-Peer File Sharing Systems". *Proceedings of the Twenty-Second Annual Joint*

Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), vol 3, pp. 2188-2198.

Hales, D. (2004) "From Selfish Nodes to Cooperative Networks - Emergent Link-Based Incentives in Peer-to-Peer Networks". *Proceedings of the Fourth International Conference on Peer-to-Peer Computing*, pp. 151-158.

Haridasan, M., Jansch-Pôrto, I., and van Renesse, R. (2008) "Enforcing Fairness in a Live-Streaming System." *Proceedings of SPIE: Multimedia Computing and Networking*. v. 6818. San Jose, CA.

Haridasan, M., and van Renesse, R. (2006) "Defense Against Intrusion in a *Live streaming* Multicast System." *Proceedings of the 6th IEEE International Conference on Peer-to-peer Computing (P2P)*. Cambridge, UK, pp. 185-192.

Li, H. C., et al. (2006) "BAR Gossip." *Proceedings of the 7th Symposium on Operating System Design and Implementation (OSDI '06)*. Seattle, WA, pp. 191-204.

Liao, X., Jin, H., Liu, Y., Ni, L. M., and Deng, D. (2006) "Anysee: *Peer-to-Peer Live Streaming*." *25th IEEE Intl. Conf. on Computer Commun (INFOCOM)* pp. 1-10.

Liu, J., Rao, S. G. and Zhang, H. (2008) "Opportunities and Challenges of *Peer-to-peer* Internet Video Broadcast." *Proceedings of the IEEE*, v. 96, n. 1, Jan., pp. 11-24.

Magharei, N., and Rejaie, R. (2007) "PRIME: *Peer-to-peer* Receiver-drIven *Mesh*-based Streaming." *Proceedings of the 26th Conference on Computer Communications (INFOCOM)*. Anchorage, Alaska, pp. 1415-1423

Meddour, D.-E., Mushtag, M. and Ahmed, T. (2006) "Open Issues in P2P Multimedia Streaming." *Proc. IEEE ICC: Multimedia Commun. Workshop (MultiCom)*.

Nash, John (1950) "Equilibrium Points in n-person Games." *Proceedings of the National Academy of Sciences* v. 36, n. 1, pp. 48-49.

Pai, V., Kumar, K., Kamilmani, K., Sambamurthy, V. and Mohr, E. (2005) "Chainsaw: Eliminating Trees from *Overlay* Multicast." *Proceedings of the 4th International Workshop on Peer-to-peer Systems (IPTPS)*. Ithaca, NY, pp. 127-140.

Piatek, M., Anderson, T. and Krishnamurthy, A. (2007) "A Case for Holistic Incentive Design." *Proc. Workshop Future Directions in Distr. Computing (FuDiCo III)*.

Shneidman, J., Parkes, D. C. (2003) "Rationality and Self-Interest in Peer to Peer Networks". *Proceedings of the 2nd International Workshop on Peer-to-Peer Systems (IPTPS'03)*. Berkeley, CA, USA, pp. 139-148

Singh, A., Castro, M., Rowstron, A. and Druschel P. (2004) "Defending against Eclipse *attacks* on *overlay* networks." *Proceedings of the 11th ACM SIGOPS European Workshop*. Leuven, Belgium.

Yang, G.-H., Shen, D., Yang, D. and Li, V. O. K. (2006) "Adaptive Video Streaming over Multi-channel Ad Hoc Networks." *Global Telecommunications Conference IEEE (GLOBECOM'*06). pp. 1-5.

Zhang, X., Liu, J., Li, B. and Yum, T.-S P. (2005) "CoolStreaming/DONet: A Data-Driven *Overlay* Network for Efficient Live Media Streaming." *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)* v. 3. Miami, FL, USA, pp. 2102-2111.