Um Sistema P2P Adaptável a Diferentes Contextos de Utilização

Bruno Bompastor
Dept. de Informática
Universidade do Minho
Braga, Portugal
b.bompastor@gmail.com

Pedro Sousa
Dept. de Informática
Universidade do Minho
Braga, Portugal
pns@di.uminho.pt

***Resumo*—No mundo actual em que vivemos tudo e todos estão conectados por uma rede global denominada Internet, onde as aplicações P2P proliferam. Com a crescente evolução da Internet tem-se vindo a observar um aumento na utilização de soluções P2P, que devido à sua imprevisibilidade trazem fortes problemas para os fornecedores de serviços (e.g. ISPs). Este artigo apresentará um sistema P2P baseado no protocolo BitTorrent de fácil integração na rede Internet através da sua capacidade de adaptação a diferentes contextos de utilização. Esta integração será alcançada recorrendo a vários mecanismos e estratégias implementadas no sistema desenvolvido. A arquitectura a desenvolver será avaliada e testada com o auxilio da ferramenta de simulação NS-2, com o objectivo de testar os mecanismos propostos e analisar os resultados obtidos.**

***Keywords*-Peer-to-peer (P2P); BitTorrent; Trackers P2P; Engenharia de Tráfego.**

I. Introdução

Actualmente existem diferentes tipos de aplicações P2P [1] apresentando diferentes mecanismos de configuração, estratégias de operação e objectivos particulares. O paradigma P2P tem várias vantagens na distribuição rápida de elevadas quantidades de informação em relação ao modelo tradicional cliente-servidor. Em particular, e a título de exemplo, o protocolo BitTorrent [2], [3] é uma das soluções mais populares, existindo estudos que o apontam como sendo já responsável por mais de um terço de todo o tráfego da rede Internet [4]. É desta forma inegável a influência que este tipo de aplicações tem na Internet colocando novos desafios à comunidade científica.

Neste contexto, a crescente utilização de aplicações P2P tem resultado no facto dos ISPs terem de enfrentar sérios problemas, tais como a alta variabilidade e alteração de perfis de tráfego na rede, a excessiva carga em links críticos, a geração de tráfego inter-domínio desnecessário e diversas dificuldades na utilização de técnicas clássicas de Engenharia de Tráfego [5], [6]. Neste sentido, várias soluções foram adoptadas pelos ISPs de modo a aumentar o desempenho da rede, como por exemplo o uso de estratégias de *caching* [7] para reduzir o consumo de largura de banda e vários mecanismos de detecção e controlo de tráfego P2P [8]. Neste sentido, existem vantagens no desenvolvimento de mecanismos de selecção de *peers* mais flexíveis [9] que, caso sejam bem integrados nas soluções P2P actuais, podem facilitar a integração e coexistência destas aplicações na rede de Internet.

O sistema proposto estará focalizado na integração de aplicações P2P baseadas no protocolo BitTorrent na Internet actual possibilitando o desenvolvimento de soluções que possam permitir o desenvolvimento de esforços colaborativos, estratégias de diferenciação, bem como a possibilidade de levar em consideração alguns requisitos impostos por entidades externas como ISPs, prestadores de serviços, etc. A título exemplificativo, no caso específico dos interesses particulares dos ISPs, destaca-se a maximização do desempenho da sua rede minimizando os custos de operação. Como um outro exemplo pode-se referir que muitas entidades poderão também beneficiar com este sistema P2P mais adaptável na medida em que permitirá desenvolver perfis de diferenciação entre os utilizadores do sistema, criando oportunidades para explorar novos modelos de negócio por parte das empresas prestadoras de serviços. Para atingir estas metas foi pensada numa forma de introduzir as melhorias necessárias na arquitectura BitTorrent tendo em conta as alternativas já apresentadas pela comunidade cientifica e os meios disponíveis para o desenvolvimento do sistema. A solução encontrada passa pela reformulação e desenvolvimento de um *tracker* BitTorrent que possua as características necessárias para atingir os objectivos traçados.

Este artigo está assim organizado: a Secção II descreve a arquitectura do sistema desenvolvido; a Secção III apresenta possíveis contextos de utilização para a solução proposta; a Secção IV enumera algumas das estratégias idealizadas; a Secção V descreve o ambiente utilizado para testar as experiências efectuadas; a Secção VI mostra as experiências e os resultados obtidos e, finalmente; a Secção VII traça as conclusões.

II. Arquitectura do Sistema

A arquitectura do *tracker* BitTorrent[1] idealizado será apresentada sobe a forma de cinco principais módulos que representam cada um deles um conjunto de funcionalidades específicas. A Figura 1 mostra a arquitectura do *tracker*

[1]Detalhes adicionais sobre o funcionamento do protocolo BitTorrent podem ser consultados em [2], [3].

desenvolvido e a sua interacção com os diversos participantes do sistema.

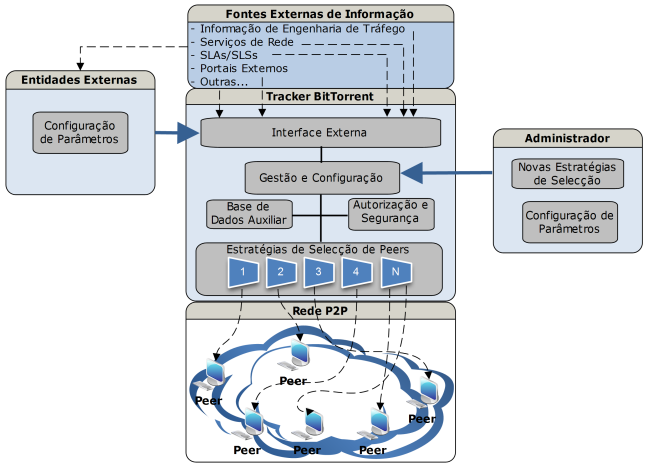

Figura 1. Arquitectura do *tracker* P2P desenvolvido.

Gestão e Configuração: Este módulo é dedicado à gestão e configuração do *tracker* BitTorrent e será usado pelos administradores do sistema e eventuais entidades externas, devidamente autorizadas, para alterar o modo de operação do mesmo. Do conjunto de funcionalidades presentes neste módulo destacam-se as seguintes: activação da estratégia de selecção de *peers*, adicionar novas estratégias de selecção de *peers*, adicionar novas entidades externas de informação e configuração do *tracker* em modo manual/automático e estático/dinâmico.

Autorização e Segurança: Aqui serão estabelecidas todas directivas referentes à autorização e segurança do *tracker* BitTorrent. O administrador terá a possibilidade de criar diferentes perfis de configuração para o *tracker*, detalhando as permissões de cada um para que diferentes entidades tenham a possibilidade de aceder ao sistema sem comprometer a sua estabilidade.

Estratégias de Selecção de *Peers*: Este é o principal módulo do sistema, pois aqui estarão definidas as estratégias de selecção de *peers*. Aqui serão definidas as características e parâmetros de todas as estratégias activas ou inactivas do sistema. Exemplos de mecanismos e estratégias de selecção de *peers* pensadas serão apresentados na secção IV.

Base de Dados Auxiliar: Este módulo será responsável por armazenar informação necessária ao funcionamento do *tracker*, nomeadamente dados que caracterizem os *peers* activos na *swarm*. A grande parte da informação retida neste modulo será usada pelo *tracker* para suportar os procedimentos de selecção de *peers*. Armazenará também informação fornecida pelas entidades externas, informação essa que será usada para desencadear futuras acções no sistema.

Interface Externa: Aqui serão definidos os métodos de interacção entre o *tracker* e as fontes externas de informação. A informação disponibilizada pelas entidades será sobretudo utilizada para alimentar as estratégias de selecção, e por isso será principalmente informação de estado da rede e dados relacionados com engenharia de tráfego. Outras possíveis fontes de informação vão desde portais externos [10], passando por serviços contratuais (SLAs - Service Level Agreements), até base de dados externas disponibilizadas pelos ISPs.

III. Contextos de Utilização

Como anteriormente mencionado, a principal motivação da arquitectura proposta é adicionar flexibilidade às decisões que as aplicações P2P podem tomar em relação aos diferentes contextos de utilização escolhidos. De uma forma resumida é possível apontar alguns objectivos que se podem alcançar com a solução proposta:

Esforços colaborativos: A arquitectura desenvolvida pode ser usada para criar aplicações P2P com capacidades colaborativas adicionais permitindo que as entidades externas forneçam informação valiosa que, se correctamente utilizada, possa ajudar a mitigar os problemas tradicionais que as aplicações P2P causam aos ISPs.

Diferenciação na qualidade dos *peers*: Outro possível uso para este *tracker* adaptável é a introdução de estratégias que permitam a diferenciação na qualidade aplicacional que os diferentes *peers* obtêm. Tais mecanismos permitem o desenvolvimento de soluções capazes de beneficiar ou penalizar *peers* de acordo com um conjunto de regras pré-definidas tendo em conta objectivos específicos.

Engenharia de tráfego: Dada a flexibilidade e a natureza adaptável do *tracker* proposto, será possível configurar determinados parâmetros aplicacionais (e.g., estratégias de selecção de *peers*, comportamentos reactivos a eventos externos, etc) de modo a precaver e planear melhor a maneira como o tráfego P2P irá influenciar a rede do fornecedor e, desta forma, alcançar uma melhor utilização da infra-estrutura.

A utilização deste sistema poderá trazer grandes vantagens para as entidades prestadoras de serviço mas também para os seus clientes que, como compensação pelo uso desta solução, poderão beneficiar por parte dos ISPs de determinadas regalias. Por exemplo, os utilizadores que usem o cliente BitTorrent (e respectivo *tracker*) que implementa a solução proposta neste trabalho poderão ser compensados por parte do ISP com um tratamento preferencial por forma terem uma qualidade de serviço superior aos utilizadores de outra qualquer aplicação P2P, que normalmente são condicionadas por estratégias de *throttling* e/ou *shapping* adoptadas pelo ISP. Esta possibilidade de obter um melhor desempenho na obtenção do conteúdo pretendido tornará este sistema aliciante para os clientes dos prestadores de serviços disponíveis para implementar esta solução.

IV. Estratégias Propostas

Uma das principais características do *tracker* idealizado será a possibilidade de configurar a estratégia de selecção de *peers* activa. De seguida serão apresentados, a título meramente exemplificativo, alguns exemplos de estratégias possíveis de serem programadas no *tracker* proposto.

A. Redução de Tráfego Inter-Domínio

A implementação inicial do protocolo BitTorrent abstrai-se da topologia e dos custos dos links da rede onde assenta. Ao tomar decisões sem ter em conta estes factores, o protocolo pode aumentar significativamente os custos operacionais dos ISPs, particularmente em termos de tráfego inter-domínio. Por isso este mecanismo introduz no *tracker* BitTorrent uma estratégia de selecção baseada na localidade para poder distinguir quais os *peers* pertencentes a um determinado domínio ou ISP. Para poder aplicar esta estratégia é necessário que as fontes externas (e.g. ISPs) forneçam informação de localidade dos *peers*. Isso poderá ser feito de várias formas, como por exemplo, usar mapas da topologia da rede ou mapear os ASs [11], [12] utilizados pelo ISP. Os ISPs que pretendam preservar a localidade do seu tráfego podem também fornecer a sua gama de endereçamento ao *tracker*. Outra forma será aproveitar o facto de a interacção *peer-tracker* ser feita sobre HTTP e utilizar as *proxies* dos ISPs para adicionar aos *headers* HTTP uma tag especifica de localidade [13]. Todos os *peers* com a mesma tag de localidade são identificados como pertencentes ao mesmo ISP.

Depois de obter a informação de localidade necessária, o *tracker* está habilitado a aplicar a estratégia de selecção de *peers* orientada para a redução do tráfego inter-domínio. Numa primeira fase o mecanismo desenvolvido permite que a rede P2P inicie a sua operação normalmente sem que fique limitada pelo reduzido número de *peers* com a mesma localização, ou seja, é retornada uma amostra aleatória[2] de *peers* existentes na *swarm*. A partir deste momento, os novos *peers* terão acesso principalmente a vizinhos locais para efectuar a transferência pretendida.

B. Protecção de Pontos Críticos

Os ISPs usualmente recorrem a técnicas de engenharia de tráfego para controlar a sua rede e dimensiona-la de acordo com as necessidades dos utilizadores. Um dos possíveis objectivos para a aplicação das técnicas de engenharia de tráfego poderá ser proteger pontos críticos da rede tais como domínios, links ou nós. Por isso foi também definido um mecanismo específico capaz de suportar essas características típicas da engenharia de tráfego.

Para que esta estratégia de selecção de *peers* seja bem sucedida é necessário que os fornecedores de serviços de Internet cooperem com o *tracker* e indiquem exactamente quais os pontos da sua rede que pretendem proteger. Esta informação fornecida pelas fontes externas terá que repercutir à partida alguma forma de mapeamento entre a topologia da rede e os *peers* activos na rede P2P, porque o *tracker* apenas tem conhecimento dos *peers* presentes na *swarm*. O cruzamento da informação topológica com a informação de *routing* da rede em causa permitirá definir quais os *peers* que não devem estabelecer relações que possam sobrecarregar os pontos críticos da rede.

[2]Comportamento usualmente assumido pelos trackers P2P BitTorrent.

Uma solução seria o *tracker* ser alimentado com esta informação e automaticamente escolher quais os *peers* conectáveis, ou seja, os que podem estabelecer relações adequadas à estratégia de protecção de pontos críticos definida. Outra alternativa seria as fontes externas indicarem quais os *peers*, que segundo a suas decisões de engenharia de tráfego, não se podem conectar entre si para que o *tracker* os possa excluir das amostras que irá divulgar. A Figura 2 demonstra um exemplo ilustrativo de uma topologia que pode beneficiar com esta estratégia de protecção de pontos críticos. Por exemplo, caso assim se pretenda, o *link* R0<->R2 pode ser facilmente protegido se o *tracker* deixar de fornecer contactos de *peers* do domínio 3 para o 1 e vice-versa[3].

C. Estratégias de Agendamento

Por vezes certos fornecedores de serviço optam por libertar ou reservar recursos da sua rede segundo horários pré-escalonados para que possam garantir uma constante qualidade de serviço ao longo do tempo. Normalmente durante o dia os ISPs tentam reservar recursos essenciais para que a qualidade do seu serviço não seja degradada à custa de utilizadores que esgotam a sua largura de banda com aplicações menos prioritárias. As aplicações P2P estão invariavelmente incluídas nesse grupo de aplicações indesejadas, por isso este mecanismo de selecção permitirá ao nível aplicacional ter diferentes comportamentos segundo os agendamentos efectuados pelos fornecedores de serviços.

Previamente será definido, pelas fontes externas de informação, o horário em que o serviço prestado deverá ter uma qualidade aceitável e ao mesmo tempo serão definidos horários onde não haverá limitações para o utilizador da rede (e.g. *Happy Hour*). Depois de escolhido o intervalo horário mais restritivo para a rede, será indicado ao *tracker* os vários mecanismos que deve executar para atingir esse objectivo. Ou seja, durante um determinado horário o *tracker* é obrigado a fornecer uma lista de *peers* não muito favorável aos participantes da rede, isto é, uma lista que inclua um menor número de *peers*, ou *peers* com menor largura de banda ou mesmo restringir a lista a *peers* locais, por forma a limitar a quantidade de tráfego gerado pelas aplicações.

D. Estratégias de Diferenciação

Estas estratégias vocacionadas para promover novos modelos de diferenciação serão, por exemplo, capazes de punir *peers*: que não obedeçam a algumas regras pré-estabelecidas ao nível da aplicação P2P; ou que tenham um comportamento que degrade o desempenho global do sistema; ou mesmo que não tenham acesso a níveis de serviço de elevada prioridade. Quando o *tracker* desenvolvido opera neste modo está também habilitado a fornecer incentivos a *peers* específicos numa dada *swarm*. Este mecanismo pode então também ser utilizado para beneficiar os clientes que cumpram os acordos pré-estabelecidos, ou que sejam considerados de alta prioridade.

Em relação à penalização exclusiva de *peers*, este mecanismo

[3]Assumindo que a estratrégia de routing utilizada selecciona caminhos com o menor número de saltos.

de selecção baseia-se num *tracker* programado para restringir o número de *peers* que fornece a clientes específicos. Espera-se que esta simples técnica de diferenciação origine diferentes níveis de qualidade de serviço já que os *peers* com menor prioridade terão menor oportunidade de descobrir e comunicar com outros *peers* da *swarm*.

No que diz respeito à valorização de determinados utilizadores, todos os incentivos serão fornecidos através de uma selecção cuidada dos *peers* a incluir nas amostras enviadas pelo *tracker*. Um conjunto de *peers* de uma dada *swarm* pode beneficiar deste mecanismo de selecção se o *tracker* fornecer informação privilegiada acerca de *seeds* com maior capacidade de upload, ou até mesmo *seeds* de elevada qualidade que sejam escondidas dos outros participantes menos prioritários. Como consequência, esse conjunto de *peers* irá formar uma espécie de *sub-swarm* mais prioritária que é expectável que obtenha um melhor serviço aplicacional.

E. Estratégias Híbridas

Estas estratégias híbridas ajudarão o protocolo BitTorrent a suportar simultaneamente várias estratégias de selecção. A título de exemplo, a estratégia pode ser configurada para reduzir o tráfego inter-domínio e combinada com mecanismos de protecção de links críticos internos para que a carga excessiva em recursos internos não comprometa a qualidade do serviço global. Outras possibilidades será a criação de estratégias híbridas que combinem as técnicas de engenharia de tráfego e modelos de diferenciação.

V. Ambiente de Simulação

Através de um *patch* para o ns-2 [14] que implementa o protocolo BitTorrent [15] foi possível desenvolver e testar a arquitectura proposta na Secção II. Este *patch* sofreu as devidas alterações de modo a implementar os vários modulos da arquitectura do *tracker* anteriormente definida.

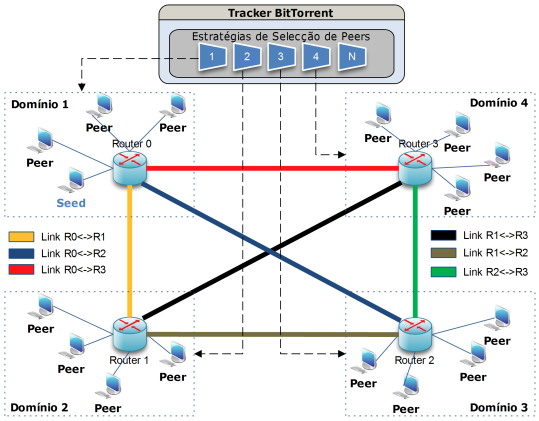

Figura 2. Topologia da rede simulada usada para testar o *tracker*.

A Figura 2 ilustra uma das topologias de rede usadas para apresentar alguns resultados ilustrativos do *tracker* adaptável a diferentes contextos de utilização proposto. Administrativamente a rede está dividida em quatro domínios distintos inter-conectados por *links* inter-domínio (R0<->R1, R1<->R3, etc.). A maior parte dos parâmetros que controlam o protocolo baseado no BitTorrent podem ser configurados, incluindo parâmetros como o número de *seeds* e *leechers* por domínio, configurações relacionadas com o *tracker*, tamanho do *chunk*, tamanho do ficheiro, capacidade de upload dos *peers*, vários tempos e intervalos específicos do protocolo BitTorrent, entre outros. O *tracker* adaptável a diferentes contextos de utilização proposto foi testado recorrendo a um elevado número de experiências de simulação e cada um dos cenários foi testado várias vezes usando sementes distintas que controlam parâmetros como os atrasos de propagação dos *links*, os tempos de chegada dos *leechers* à *swarm*, padrões de distribuição dos *peers*, etc.

Na secção seguinte será apresentado um conjunto de resultados ilustrativos dos cenários simulados. Dos exemplos seleccionados a maior parte dos resultados foram testados assumindo o cenário de simulação onde existem 100 *peers* por domínio, resultando no número total de 400 *peers*. O tamanho do ficheiro é de 50 MB e o tamanho do *chunk* é de 256 kB. O número máximo de *peers* fornecido pelo *tracker* é 25, no entanto dependendo do mecanismo seleccionado o *tracker* pode manipular este valor para *peers* específicos. A maior parte dos resultados seleccionados assumem o pior caso para a disseminação do ficheiro, isto é, inicialmente apenas existe uma *seed* e alguns *leechers* na rede (i.e. efeito *flash crowd*). Ao nível de rede os *peers* têm, em média, uma capacidade de *upload* de 1 Mbps e uma capacidade de *download* que é considerada oito vezes superior a este valor (i.e. para simular *links* de acesso assimétricos, como os ADSL dos utilizadores residenciais). De modo a melhorar a heterogeneidade de cada domínio, os atrasos de propagação dos *links* de acesso são gerados aleatoriamente segundo um intervalo de 1-50 ms. Considera-se que os *links* inter-domínio podem comportar tráfego P2P até 10 Mbps e os seus atrasos de propagação são pelo menos duas vezes superiores do que o máximo valor considerado para os links intra-domínio. O desempenho dos *peers* é medido tendo em conta o tempo de *download* necessário para completar a transferência do ficheiro. Para simplificar a visualização dos resultados, a cada *peer* foi atribuído um ID de identificação, neste caso no intervalo de [0, 400].

VI. Cenários Simulados e Resultados Obtidos

Redução de Tráfego Inter-Domínio: Como explicado anteriormente, neste exemplo o *tracker* foi programado para se comportar de forma colaborativa, recebendo informação de localização dos *peers* com o objectivo de reduzir o tráfego inter-domínio gerado pela aplicação P2P. A Figura 3 mostra os resultados comparativos do *tracker* configurado com a selecção padrão e quando programado com o mecanismo baseado na localização, neste caso considera-se que apenas existe uma *seed* inicialmente no domínio um da rede. Como observado, quando o *tracker* é programado para realizar uma selecção de *peers* baseada na localização o tráfego inter-domínio gerado é pelo menos dez vezes inferior ao observado na selecção

padrão (ver a Figura 3 b) que mostra o tráfego inter-domínio total gerado com a selecção baseada na localização). Para além do mais, e mesmo tendo em conta que as decisões de selecção de *peers* são agora restritivas e os *peers* locais têm maior probabilidade de serem escolhidos, o tempo médio de download dos *peers* manteve-se ao mesmo nível (ver tempo de *download* dos *peers* na Figura 3 a)).

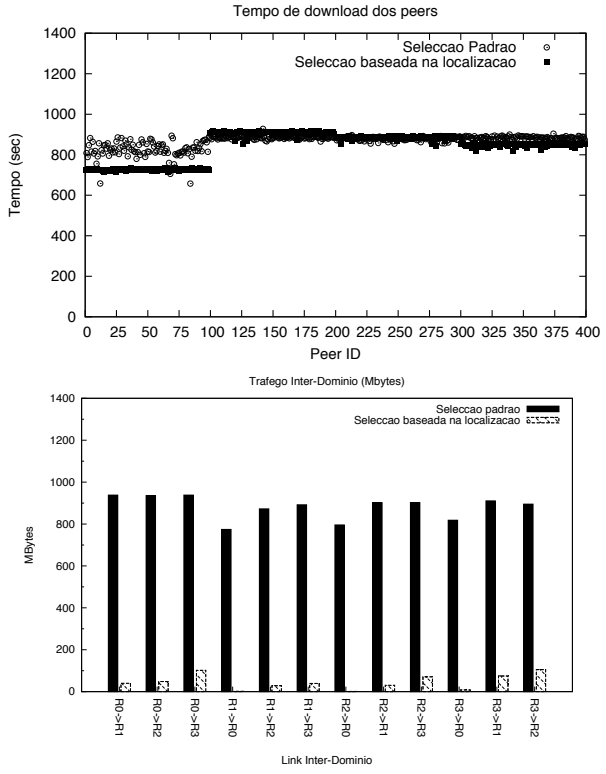

Figura 3. Redução de tráfego inter-domínio: a) tempo de download; b) tráfego inter-domínio.

Protecção de Pontos Críticos: Este cenário de simulação pretende demonstrar o funcionamento da estratégia de selecção de *peers* focada na protecção de pontos críticos da rede. Neste caso especifico, foi utilizada a topologia da Figura 2 e decidiu-se que o *link* R0<->R2 teria uma atenção especial por parte do *tracker* proposto. Os resultados apresentados na Figura 4 demonstram que o tráfego que atravessou esse link foi substancialmente inferior quando comparado com os demais. Esta protecção foi facilmente induzida pelo tracker visto que foi alimentado de antemão com a topologia da rede e com informação do *routing* aplicado à mesma.

Estratégias de Agendamento: Nesta experiência vai ser testada a hipótese de aplicar uma estratégia agendada para um determinado horário e a consequente estratégia aplicada fora desse horário. Os dois horários serão encarados como duas simulações distintas em intervalos temporários distintos. O ambiente de simulação foi alterado para aumentar a heterogeneidade da rede com o auxilio de *peers* de alta, média e baixa capacidade. Os primeiros 25 *peers* de cada domínio são considerados de baixa capacidade (256 Kbps), os seguintes 25 *peers* são de alta capacidade (3 Mbps) e os restantes são de média capacidade (1 Mbps).

Assim, durante o horário mais restritivo os *peers* apenas recebem contactos para *peers* de baixa capacidade do seu próprio domínio. Esta estratégia irá permitir ao administrador de rede limitar a largura de banda utilizada pela aplicação P2P e ao mesmo tempo reduzir o tráfego inter-domínio. Como demonstra a Figura 5 a) uma consequência desta técnica de selecção foi aumento significativo do tempo de *download* quando comparado com o horário não restritivo. Em contraste, durante a *happy hour* é visível na Figura 5 a) que a globalidade dos *peers* obteve tempos de download significativamente mais baixos.

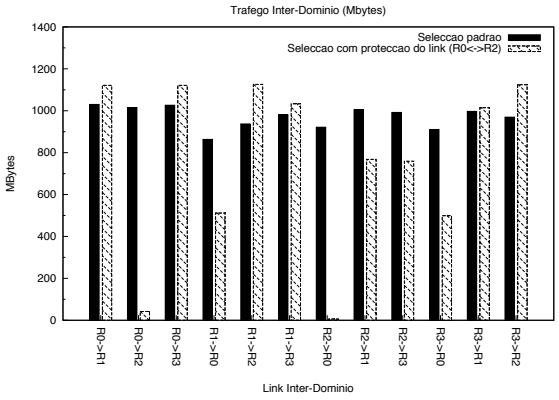

Figura 4. Protecção de pontos críticos: tráfego inter-domínio.

Estratégias Híbridas: O último exemplo seleccionado usa o *tracker* configurado em modo de diferenciação híbrido. Os resultados da Figura 5 b) foram obtidos com o *tracker* programado para beneficiar um grupo específico de *peers* no domínio dois, neste caso os *peers* no intervalo [150, 160], e para punir um grupo de *peers* no domínio um da rede, neste caso os *peers* no intervalo [20, 30]. Como observado na Figura 5 b), os resultados mostram claramente a actuação do modo híbrido, evidenciando que as configurações mistas e híbridas são possíveis de serem implementadas usando este *tracker* adaptável a diferentes contextos de utilização.

VII. Conclusão

Este trabalho apresentou a arquitectura de um sistema P2P adaptável as diferentes contextos, e mostrou exemplos ilustrativos de possíveis estratégias de selecção de *peers* que poderão utilizar informações adicionais fornecidas por entidades externas. A solução do *tracker* proposto foi implementada recorrendo à simulação e, como corroborado pelos resultados apresentados, comportamentos colaborativos e diferenciações semânticas são possíveis de serem alcançados ao nível P2P utilizando a solução proposta. Desta forma, a abordagem proposta irá beneficiar o desenvolvimento de aplicações P2P avançadas, e também apoiar o desenvolvimento de métodos inteligentes de colaboração entre os ISPs e as aplicações P2P. Além disso, devido à maior diferenciação semântica que pode

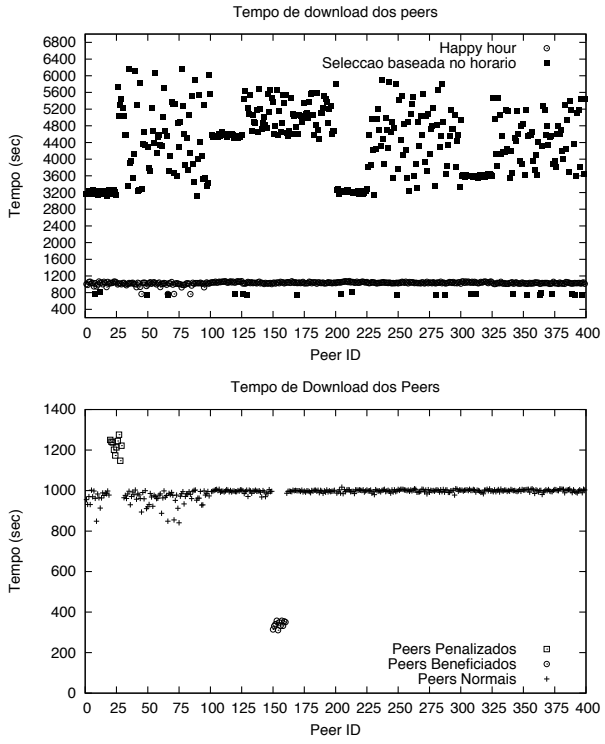

Figura 5. a) Estratégias de agendamento: tempo de download. b) Estratégia híbrida de Diferenciação: tempo de download.

ser obtida usando o *tracker* sensível ao contexto proposto, novos serviços de Internet e modelos de negócio baseados no paradigma P2P poderão também tirar partido da arquitectura definida neste trabalho.

REFERÊNCIAS

[1] K. Lua and et al., "A Survey and Comparison of Peer-to-peer Overlay Network Schemes," *Communications Surveys & Tutorials, IEEE*, pp. 72–93, 2005.

[2] B. Cohen, "Incentives Build Robustness in BitTorrent," in *Proc. 1st Workshop on Economics of Peer-to-Peer Systems*, June 2003.

[3] J. Pouwelse, P. Garbacki, D. Epema, and H. Sips, "An Introduction to the BitTorrent Peer-to-Peer File-Sharing System," 2004.

[4] H. Schulze and K. Mochalski, "Internet Study 2008/2009," Tech. Report, 2009.

[5] R. Keralapura, N. Taft, C. Chuah, and G. Iannaccone, "Can ISPs Take the Heat from Overlay Networks?" in *Proc. of HotNets-III*, November 2004.

[6] L. Qiu and et al., "On Selfish Routing in Internet-like Environments," in *Proceedings of the 2003 Conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '03)*, New York, NY, USA, 2003, pp. 151–162.

[7] G. Shen, Y. Wang, and Y. Zhao, "HPTP: Relieving the Tension between ISPs and P2P," in *Proc. of Sixth International Workshop on Peer-to-Peer Systems (IPTPS'07)*, 2003. [Online]. Available: http://www.cs.ucsb.edu/ ravenben/publications/abstracts/hptp-iptps07.html

[8] A. Spognardi, A. Lucarelli, and R. Pietro, "A Methodology for P2P File-Sharing Traffic Detection," in *HOT-P2P '05: Proceedings of the Second International Workshop on Hot Topics in Peer-to-Peer Systems*, USA, 2005, pp. 52–61.

[9] P. Sousa, "Flexible Peer Selection Mechanisms for Future Internet Applications," in *Proc. of Sixth International ICST Conference on Broadband Communications*, 2009.

[10] H. Xie, Y. R. Yang, A. Krishnamurthy, Y. G. Liu, and A. Silberschatz, "P4p: provider portal for applications," in *SIGCOMM '08: Proceedings of the ACM SIGCOMM 2008 conference on Data communication*. New York, NY, USA: ACM, 2008, pp. 351–362.

[11] J. Li and K. Sollins, "Exploiting autonomous system information in structured peer-to-peer networks," in *In ICCCN*. IEEE CS Press, 2004, pp. 403–408.

[12] A. Nakao, L. Peterson, and A. Bavier, "A routing underlay for overlay networks," in *Proceedings of the 2003 ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '03)*. New York, NY, USA: ACM Press, 2003, pp. 11–18.

[13] R. Bindal and et al., "Improving traffic locality in bittorrent via biased neighbor selection," in *26th IEEE International Conference on Distributed Computing Systems, 2006. ICDCS 2006*, July 2006, pp. 66–77.

[14] "The Network Simulator NS-2," http://www.isi.edu/nsnam/ns/, Last visited: Feb 2010.

[15] "Simulation of BitTorrent Peer-to-Peer (P2P) Networks in ns-2 ," http://www.tu-harburg.de/et6/research/bittorrentsim/index.html, Last visited: Feb 2010.