# Escambo: Um Modelo de Comportamento e Reputação para Sistemas Peer-to-Peer

**Rafael da Rosa Righi, Felipe Rolim Pellissari, Carla Merkle Westphall**

[1] Programa de Pós-Graduação em Ciência da Computação – PPGCC
Laboratório de Redes e Gerência (LRG) – Universidade Federal de Santa Catarina
Caixa Postal 476 - 88040-900, Florianópolis, SC

{rrighi,rolim,carla}@lrg.ufsc.br

***Resumo.*** *Os sistemas colaborativos Peer-to-Peer apresentam uma forma de computação colaborativa onde cada participante atua como cliente e servidor de recursos. Entre os principais desafios existentes nesse tipo de computação estão o desenvolvimento de técnicas para incentivar a colaboração dos usuários e minimizar o número de nós caronas que não auxiliam a rede e apenas sugam seus recursos. Este artigo define um modelo baseado em micropagamentos e na análise da reputação que objetiva aumentar a eficiência da rede Peer-to-Peer e diminuir o número de membros parasitas que a compõe. O protótipo desenvolvido valida o modelo e coloca em prática suas principais idéias.*

## 1. Introdução

As redes Peer-to-Peer são sistemas distribuídos sem controle centralizado ou organização hierárquica, nas quais o programa que é executado em cada elemento é equivalente em funcionalidade. Esses sistemas possibilitam que os usuários sejam, além de consumidores de recursos, os próprios responsáveis por disponibilizá-los. Por minimizar o papel dos elementos centralizadores, os sistemas P2P tendem a ser imunes à censura, monopólios, regulamentos e outros exercícios atribuídos às autoridades centralizadoras [Agre, 2003].

O sucesso de uma rede Peer-to-Peer depende de fatores como o protocolo de comunicação utilizado, arquitetura de distribuição empregada (totalmente descentralizada ou não), tempo decorrido desde uma solicitação até o recebimento de respostas e o número de usuários participantes do sistema. Essa última característica é especialmente importante, pois é ela quem determina o tamanho da comunidade virtual e o volume de recursos presente na rede Peer-to-Peer.

Um dos problemas que os sistemas colaborativos enfrentam é a existência de usuários caronas (*free riders*), também chamados de parasitas ou sanguessugas, os quais não agregam nenhum valor à rede Peer-to-Peer, servindo somente para aumentar o congestionamento dos enlaces e concentrar as conexões sob aqueles nós que dispõem recursos no sistema [Strulo, 2004]. Os impactos dos caronas são diferentes nas várias arquiteturas Peer-to-Peer existentes. Por exemplo, na rede P2P Gnutella, além dos problemas citados, os caronas também contribuem para ao aumento do tempo de roteamento das solicitações, pois como nunca irão responder positivamente a um chamado, sempre passarão para seus vizinhos os pedidos por informações que recebem.

Os pesquisadores Adar e Huberman [Adar e Huberman, 2000] descobriram em seus estudos que quase 70 por cento dos usuários não compartilham recursos em uma rede Peer-to-Peer e aproximadamente 50 por cento de todas as respostas são retornadas por 1 por cento dos hospedeiros compartilhadores. Assim, eles confirmam a necessidade de haver mecanismos que incentivam a colaboração nas redes Peer-to-Peer e, conseqüentemente, as tornem mais justas e igualitárias.

O modelo Escambo exposto neste artigo define medidas que incentivam os usuários a disponibilizarem recursos na rede Peer-to-Peer e, como conseqüência, ele auxilia para atenuar o transtorno dos nós parasitas. Para chegar nesse objetivo o Escambo utiliza técnicas de micropagamentos (atribui um "preço" às comunicações) e reputação, juntamente com a seguinte premissa: "quem deseja informações da rede deve necessariamente também disponibilizar recursos". O artigo apresenta também as técnicas utilizadas para proteger o modelo Escambo de usuários mal-intencionados (aqueles que desejam subverter o protocolo em benefício próprio) e o protótipo P2P desenvolvido durante a pesquisa.

O artigo está organizado em 4 seções. A seção 2 é responsável por exibir o modelo Escambo, como ele se protege de usuários maliciosos no ambiente Peer-to-Peer e os principais trabalhos relacionados com o tema pesquisado. A seção 3 descreve a aplicação construída para legitimar o modelo desenvolvido e aborda a maneira como as arquiteturas P2P podem se beneficiar do Escambo. O artigo encerra na seção 4 com a conclusão, a qual reúne as principais idéias e resultados da pesquisa, além de citar os possíveis complementos sobre ela, a cargo de trabalhos futuros.

## 2. Modelo Escambo

O modelo Escambo é responsável por controlar o fluxo de recursos entre os participantes da rede Peer-to-Peer. Ele baseia-se na idéia de troca de recursos, onde um nó apenas adquire acesso aos recursos que deseja caso possua outros recursos para disponibilizar no ambiente colaborativo. Dessa forma, participantes que são parasitas - aqueles que não colaboram com os demais - têm acesso restrito às vantagens que a rede proporciona e, então, são encorajados a saírem da condição de caronas para desfrutarem integralmente da comunidade Peer-to-Peer. O modelo Escambo modifica a estrutura normal das redes Peer-to-Peer para alcançar os seus objetivos. Nele, um nó que recebe uma solicitação por um recurso que detém deve, antes de permitir o acesso, verificar se o nó requisitor também dispõe recursos na rede P2P. O Escambo oferece uma sistemática que possibilita reconhecer quais são os nós caronas e quais não são.

O desenvolvimento de métodos para incentivar a cooperação entre os usuários da rede Peer-to-Peer está em constante pesquisa pela comunidade científica. Entre as técnicas existentes para solucionar o problema está a atribuição de preços aos recursos – utilizada no protocolo Mojo Nation [McCoy, 2002]. Nesse cenário, os nós que colaboram com o sistema P2P ganham mais dinheiro virtual; fato que estimula o compartilhamento de recursos[1]. Outro trabalho relacionado é o *middleware* desenvolvido por Strulo [Strulo, 2004]. Ele divide os participantes da rede P2P em grupos e, nesse grupos, cada líder é responsável por definir regras de comportamento a serem seguidas pelos demais

[1]O maior problema de utilizar dinheiro virtual é quantificar com clareza quanto vale cada recurso.

integrantes. O modelo Escambo une as principais vantagens dos dois métodos anteriores, além de acrescentar suas próprias idéias para a solução do problema dos nós caronas e da falta de colaboração nas redes Peer-to-Peer.

Para apresentar o funcionamento do Escambo, este artigo simula a procura de uma informação em uma rede Peer-to-Peer totalmente descentralizada. O nó cliente faz uma requisição por determinado dado e esse pedido é repassado para os seus vizinhos. Se o vizinho não possuir o dado, ele re-envia o pedido para frente. Caso contrário, ele deve informar uma resposta positiva (ela pode acontecer através do roteamento normal da internet ou através do caminho inverso percorrido pela solicitação). O Escambo define que junto com a resposta, o nó "servidor" deve também comunicar a sua **política de permissão aos recursos**.

A política de permissão aos recursos informa quais as condições que o nó cliente deve suprir para acessar os recursos deste nó servidor. Ela se divide em três categorias: *(i)* tamanho total dos recursos compartilhados (medido em bytes); *(ii)* número de arquivos oferecidos; *(iii)* tipo de recursos disponibilizados. Um exemplo de política de permissão é a seguinte: "os usuários que desejam acesso aos meus recursos devem compartilhar na rede no mínimo 1 Megabyte e 4 arquivos".

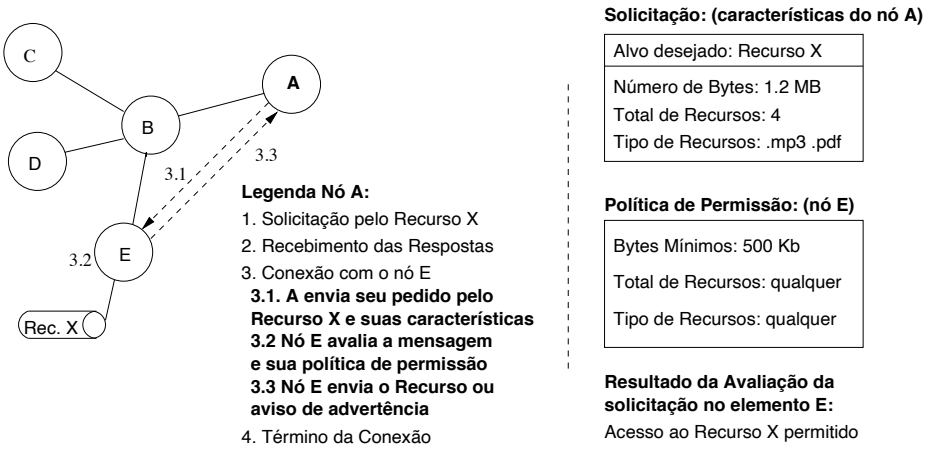


**Figura 1: Rede Peer-to-Peer e o Modelo Escambo**

O participante cliente recebe todas as respostas e analisa qual lhe parece a melhor (verifica as políticas que se encaixam em suas características) e abre uma conexão direta com o outro ponto - computação Peer-to-Peer - passando o identificador do recurso que almeja e as características dos recursos que oferece para o sistema colaborativo, assinalando o processo de reputação. O ponto servidor, ao receber a chamada por recursos, verifica a reputação do cliente avaliando suas categorias e, logo após, permite ou não o acesso aos seus recursos. Se as características dos recursos que o cliente compartilha não foram suficientes para lhe permitir o direito de acesso, ele pode tentar uma conexão a outro nó da rede com uma política menos restritiva ou disponibilizar mais recursos - fato que aumenta a sua reputação e favorece a qualidade da rede Peer-to-Peer. A Figura 1 apresenta a utilização do modelo Escambo em uma rede Peer-to-Peer. Nela estão presentes os identificadores da etapa de acesso ao recurso na rede. Os passos da procura por informações no sistema Peer-to-Peer encontram-se somente na legenda.

Para evitar que participantes maliciosos deturpem o modelo Escambo, é determi-

nado um nível máximo e outro mínimo para a política de permissão de acesso aos recursos. O grau mínimo não estabelece verificação e nele o sistema P2P se comporta como se não existisse o Escambo. O grau máximo é definido para prevenir que os usuários que administram os pontos P2P coloquem níveis "impossíveis" ou incomuns de exigências para a distribuição de seus recursos (ex: estabelecer uma política que requer que o cliente disponibilize 10 Gigabytes para a rede Peer-to-Peer). Uma política de permissão exemplo e o resultado de uma avaliação de reputação também estão presentes na Figura 1.

O Escambo utiliza um modo simplificado de micropagamento [Yang e Garcia-Molina, 2003]. O micropagamento introduz o conceito de pagamento pelo acesso a um recurso ou pedido de atividade. Esse pagamento pode ser de dois tipos: *(i)* aquele em que o nó servidor não recebe nenhum valor e o cliente paga-o geralmente com trabalho (cálculo de uma tarefa computacional complexa); *(ii)* o cliente utiliza algum sistema de pagamento (ex: dinheiro virtual) para pagar o detentor dos recursos, o qual tem acesso ao montante recebido. No caso específico do Escambo, o nó cliente paga o servidor através da oferta de recursos na rede Peer-to-Peer.

A reputação nos sistemas colaborativos Peer-to-Peer tradicionais informam quais participantes da rede são honestos ou bom servidores de recursos. A reputação dos nós é adquirida através das experiências dos próprios membros da rede e das trocas de informações de reputação entre os pares que confiam um no outro [Marti e Garcia-Molina, 2003]. O conceito de reputação encontrado no Escambo distancia-se do mencionado anteriormente. Nele, a reputação de cada nó está associada à quantidade e qualidade do material que ele disponibiliza na rede Peer-to-Peer e não depende da opinião de outros participantes do sistema. Um nó da rede Peer-to-Peer é o único responsável por sua reputação.

Além da verificação de **políticas de permissão** impróprias nos elementos da rede Peer-to-Peer, o modelo Escambo deve também evitar a falsificação das informações de reputação. O Escambo deve estar precavido contra usuários que alteram as mensagens passadas entre os nós em benefício próprio (um usuário não deve se passar por grande compartilhador de recursos quando na verdade não é). As seguintes medidas podem ser adotadas para colocar segurança no modelo definido: *(i)* ao solicitar um recurso, o cliente P2P passa, junto com a sua reputação, a lista de todos os recursos que oferece no ambiente; *(ii)* o servidor, além de aplicar sua política de permissão, escolhe um recurso aleatório na lista passada pelo cliente e tenta encontrá-lo na rede. Se ele encontrar há bons indícios que esse cliente seja honesto e a operação pode prosseguir (a anonimidade da busca na rede é essencial nesse processo). Essas ações auxiliam para a robustez do modelo Escambo e desencorajam o "atacante" a alterar os dados sobre seus recursos - sua reputação -, já que essa atitude apenas irá prejudicá-lo.

## 3. Aplicação Escambo

Esta seção apresenta o desenvolvimento do protótipo Escambo, o qual baseia sua operação no modelo de mesmo nome descrito na seção 2. O programa construído foi escrito na linguagem Java, é composto por seis classes e sua estrutura principal é semelhante àquela encontrada na aplicação P2P-Role [Righi et al., 2004], a qual define uma arquitetura de controle de acesso para redes Peer-to-Peer. As classes `ControlClient` e

`ControlServer` representam os módulos cliente e servidor existentes em cada nó P2P e estendem a classe `Thread`, ou seja, elas se comportam como fluxos de execução independentes. A classe `Resource` é responsável por duas tarefas: *(i)* a comparação da política de permissão do próprio nó com as características dos recursos do cliente P2P; *(ii)* capturar, para cada comunicação por busca de informações, a quantidade de bytes compartilhados, o número de recursos e seus tipos. Como mencionado no modelo conceitual, esses três itens acompanham a mensagem de solicitação enviada ao nó servidor.

A Figura 2 apresenta as classes que compõe um elemento na aplicação Escambo e um exemplo de conexões entre seus participantes (observe o sentido das conexões). O fluxo fornecedor de recursos abre um soquete do tipo servidor e espera por conexões na porta declarada na classe `Configuration`. Já o fluxo cliente conecta-se ao fluxo servidor do nó alvo e pede para o usuário digitar o nome do recurso (ou seu identificador) que procura. Logo após, o fluxo cliente chama a classe `Resource` para obter as informações que caracterizam o material oferecido pelo nó cliente à rede colaborativa. A mensagem enviada ao fluxo servidor é composta pelos itens mencionados anteriormente. A partir desse instante, o fluxo cliente permanece na espera por uma resposta do fluxo servidor. A resposta pode ser uma mensagem de advertência ou o recurso propriamente.

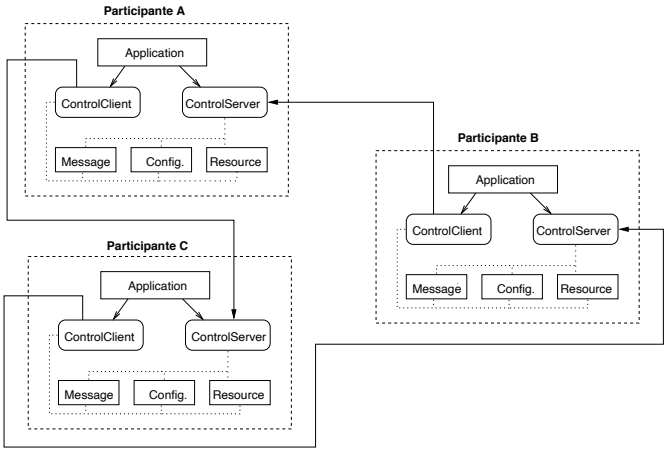


**Figura 2: Classes Java existentes nos elementos da rede Peer-to-Peer**

O fluxo servidor recebe a mensagem de solicitação da outra ponta da conexão e aciona sua classe `Resource`, a qual determina se ele permite ou não o acesso a seu recurso. Nesse ponto o nó servidor verifica se o cliente se parece com um participante carona ou não. Caso a decisão seja de conceder o recurso, o mesmo é transportado até o participante cliente. Se o parecer for de negação, é comunicado o motivo de tal atitude. O motivo do bloqueio de acesso geralmente está associado ao não cumprimento das exigências mínimas da **política de permissão** adotada pelo servidor.

Cada membro da rede virtual possui sua própria política de permissão de recursos. Essa peculiaridade possibilita a existência de nós mais rígidos e outros mais permissivos. O Escambo trabalha com um limite inferior e outro superior para a política de permissão. Nesta implementação, o nível mínimo define que o fluxo servidor aceita todas as solicitações que chegam até ele (a ação é sempre permitir). No nível máximo a regra é permitir downloads dos clientes que tenham no mínimo 600 kilobytes de informações e 5 recursos (arquivos texto).

## 4. Conclusão

As redes Peer-to-Peer possibilitam a colaboração entre os elementos da rede e seu potencial é imenso, desde o compartilhamento de recursos até o comércio eletrônico entre organizações. O sucesso dessa classe de sistemas distribuídos está associado à responsabilidade e ao comportamento de seus membros. O modelo Escambo exposto nesse artigo colabora para a otimização do ambiente colaborativo através da redução no número de nós caronas da rede. E, conseqüentemente, auxilia para o aumento do volume de recursos no sistema e para a construção de uma comunidade de usuários comprometidos em colaborar com os demais.

A idéia principal adotada pelo Escambo baseou-se nos requisitos necessários para a troca de recursos. Nesse modelo os usuários que não compartilham recursos possuem acesso restrito às vantagens da rede Peer-to-Peer. Para acessar integralmente os recursos dispostos no sistema é necessário primeiro a colaboração com mais recursos. O Escambo definiu um esquema para o controle de participantes "parasitas" que se apóia nas arquiteturas de micropagamentos e reputação em aplicações P2P. Ele preocupou-se sobretudo com a segurança nas transações de reputação, especialmente em não permitir que usuários mal intencionados forjem as mensagens do modelo em benefício próprio.

O protótipo desenvolvido ajudou no entendimento dos conceitos existentes no modelo Escambo. Seu conjunto de classes e métodos podem servir para nortear a escrita de outras aplicações P2P, principalmente no âmbito acadêmico. Finalmente, como sugestão para trabalhos futuros indica-se a realização de comparações entre ambientes P2P com e sem o modelo Escambo. A diminuição no número de mensagens trocadas no Escambo e a avaliação de seu desempenho também apresentam-se como pesquisas futuras.

## Referências

Adar, E. e Huberman, B. (2000). Free Riding on Gnutella. Technical report, Xerox Palo Alto Research Center. Available: http://citeseer.ist.psu.edu/adar00free.html.

Agre, P. E. (2003). P2P and the Promise of Internet Equality. *Communications of the ACM*, 46(2):39–42.

Marti, S. e Garcia-Molina, H. (2003). Identity Crisis: Anonymity vs. Reputation in P2P Systems. *In: Proceedings of the Third International Conference on Peer-to-Peer Computing (P2P'03)*, pages 134–141. Linkoping, Sweden.

McCoy, J. (2002). Mojo Nation Responds. Available on-line: http://www.openp2p.com/pub/a/p2p/2001/01/11/mojo.html.

Righi, R., Pellissari, F. e Westphall, C. (2004). P2P-Role: Uma arquitetura de Controle de Acesso Baseada em Papéis para Sistemas Colaborativos Peer-to-Peer. *In: IV Workshop de Segurança de Sistemas Computacionais (WSeg / SBRC)*, pages 285–296. Gramado, RS. ISBN: 85-88442-84-1.

Strulo, B. (2004). Middleware to Motivate Co-operation in Peer-to-Peer Systems. *Peer-to-Peer Journal (P2PJ)*, 1(5):1–12. http://www.p2pjournal.com.

Yang, B. e Garcia-Molina, H. (2003). PPay: micropayments for peer-to-peer systems. *In: Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS)*, pages 300–310. Washington D.C., USA.