RBRP: Protocolo de Reputação Baseado em Papéis para Redes Peer-to-Peer

Felipe Rolim Pellissari[1], Rafael da Rosa Righi[1], Carla Merkle Westphall[1]

[1]Programa de Pós-Graduação em Ciência da Computação
Laboratório de Redes e Gerência (LRG) – Universidade Federal de Santa Catarina (UFSC)
Caixa Postal 476 – 88.040-900 – Florianópolis – SC – Brazil

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

Abstract. *Most of Internet data traffic belongs to peer-to-peer file-sharing applications. One major concern of these application users is to find the safest source of a resource. Reputation protocols intend to solve this problem using nodes past experiences to find the best source of a resource. This article defines and evaluates the Role-Based Reputation Protocol (RBRP), a reputation protocol for peer-to-peer networks based on roles for a peer-to-peer system reputation values definition, classifying the nodes of a network based on these nodes behavior.*

Resumo. *Grande parte do tráfego de dados existente na Internet pertence a aplicações peer-to-peer para troca de arquivos. Uma das maiores preocupações dos usuários dessas aplicações é encontrar a fonte mais segura de um recurso desejado. Os protocolos de reputação se propõem a resolver esse problema usando experiências passadas pelos nós para encontrar a melhor fonte de um determinado recurso. Este artigo define e desenvolve um protótipo do Role-Based Reputation Protocol (RBRP), um protocolo de reputação para redes peer-to-peer baseado em papéis para definição de valores de reputação de um sistema peer-to-peer, classificando os nós de uma rede de acordo com o comportamento exercido por cada um.*

1. Introdução

Os protocolos de reputação em redes peer-to-peer têm um papel importante no provimento de segurança da rede. Esses protocolos são responsáveis para auxiliar os nós a encontrar a fonte mais confiável de um determinado recurso que desejem utilizar. Normalmente os protocolos baseiam-se em experiências anteriores para calcular um valor numérico que represente um valor de confiança com relação a um determinado nó possuidor do recurso ou mesmo ao próprio recurso.

Para seres humanos é difícil atribuir um valor numérico que represente um valor de confiança com relação a outro ser humano. Seres humanos costumam usar rótulos que indicam confiança como: “amigo“, “colega”, “vizinho” ou “aluno”. No mundo real, quando um ser humano deseja saber se outro é confiável, pergunta a um terceiro conhecido de ambos e recebe uma resposta do tipo “ele é amigo“. Nota-se que esses rótulos reproduzem papéis que outros seres humanos representam. Portanto, os protocolos de reputação que seguirem essa idéia estarão mais próximos da realidade dos seres humanos e terão melhor aceitação em uma rede peer-to-peer cujos nós representam seres humanos.

Este artigo define o protocolo Role-Based Reputation Protocol (RBRP), um protocolo baseado em papéis para cálculo de reputação e valores de confiança para nós de uma rede peer-to-peer. O documento apresenta o funcionamento do protocolo, incluindo: a especificação formal, os dados armazenados pelas bases de dados, as mensagens trafegadas, as delegações do usuário e a implementação do protocolo. A principal característica desse protocolo está na forma como ele reconhece um valor de confiança. Enquanto os demais protocolos pesquisados [Kamvar et al., 2003, Singh and Liu, 2003, Damiani et al., 2002, Cornelli et al., 2002, Gupta et al., 2003] procuram quantificar em números os valores de confiança, o RBRP atribui nomes relacionados com papéis aos valores de confiança. Isso, além de organizar os valores de confiança em grupos reproduzidos por papéis, auxilia os usuários na atribuição de confiança a outros nós. O RBRP também se preocupa em separar os valores de confiança com relação ao tipo de dado desejado. Isso é importante porque, por exemplo, uma boa fonte de arquivos MP3 não é necessariamente uma boa fonte de arquivos-texto.

Outro detalhe importante com relação ao RBRP e a outros protocolos de reputação é a largura de banda utilizada. Alguns autores se preocupam em comprovar que a carga gerada pelas mensagens desses protocolos não gera um aumento significativo na largura de banda utilizada pelo sistema. Esse trabalho comprova matematicamente que o uso do RBRP contribui para um uso mais eficiente da largura de banda através de uma redução do tráfego gerado pelas redes p2p, já que com a utilização desse protocolo a quantidade de trocas de recursos inválidas diminui significativamente.

O artigo está dividido da seguinte forma: A seção 2 mostra os trabalhos relacionados. Na seção 3 o protocolo RBRP é especificado. A seção 4 mostra o desenvolvimento matemático sobre a redução na largura de banda consumida por redes p2p que usam o RBRP. A seção 5 apresenta a implementação realizada e o trabalho encerra na seção 6 com a conclusão.

2. Trabalhos Relacionados

Para os nós p2p, ou *servents*, trocarem informações e recursos, são necessários alguns mecanismos de segurança para garantir a funcionalidade e proteção do sistema contra o mau uso por parte de participantes ou entidades externas. Dois pontos importantes nas redes p2p são a segurança na troca de recursos e o estabelecimento de níveis de confiança entre os *servents* [Bailes, J. E. e Templeton, G. F. ,2004]..

Os dois tipos básicos de confiança que podem ser estabelecidos em redes p2p são os baseados em micropagamento e os baseados em reputação. Os modelos de reputação têm em comum o fato de utilizarem experiências passadas pelos nós para atribuir níveis de confiança a recursos ou a outros nós [Kamvar et al., 2003, Singh and Liu, 2003, Damiani et al., 2002, Cornelli et al., 2002, Gupta et al., 2003]. Para que isso funcione, os nós precisam ser persistentes no sentido de manterem o mesmo identificador durante todo o período de tempo que estiverem dentro do sistema. Caso um nó deixe a rede e retorne com outro identificador, as informações anteriores sobre esse nó não são utilizadas.

Os primeiros trabalhos nesse tema são os seguintes: [Damiani et al., 2002], chamado de XRep, e [Cornelli et al., 2002], chamado de P2PRep. A principal diferença entre os dois protocolos é que P2PRep se preocupa em guardar informações apenas

sobre os *servents* que fazem parte da rede p2p, enquanto que o XRep armazena, além disso, informações sobre os recursos disponíveis pelo sistema.

A idéia desses trabalhos começa com os nós guardando informações sobre transações feitas por eles em uma base de reputação. Quando algum nó deseja receber um recurso desconhecido oferecido por um nó também desconhecido, ele requisita a opinião de alguns nós para verificar a reputação do detentor do recurso, além da reputação que o recurso desejado possui entre eles (somente no caso do XRep). Se o nível de reputação de, tanto o recurso quanto o nó que o oferece forem satisfatórios, a operação deve ser realizada.

Outro trabalho relacionado é o de [Singh e Liu, 2003]. Esse artigo também descreve um modelo de segurança em redes p2p baseado em reputação. Nesse modelo, chamado de TrustMe, quando um nó entra na rede, o nó *bootstrap*[1] seleciona um conjunto de nós (chamados de THA[2] peers) para atuarem como controladores da reputação desse novo nó. Quando um nó requisita e utiliza-se de um recurso de um outro nó, ele deve avaliar a atuação desse nó que ofereceu o recurso. Ele deve enviar um relatório de comportamento aos THA peers desse nó.

Todos os trabalhos citados até aqui têm algo em comum. Quando um nó deseja saber a reputação de um outro nó desconhecido, esse nó pergunta aos seus nós vizinhos sobre a reputação de tal nó. A resposta tem relação com a opinião dos nós que trocaram recursos com o nó desconhecido, e nada tem com as próprias experiências do nó que requisita a informação. Contra esse enfoque, existe o trabalho de [Kamvar et al., 2003]. O protocolo EigenTrust, detalhado no documento citado, utiliza as notas pessoais de reputação dadas pelo nó requisitante aos nós que ele conhece para calcular a reputação de um nó desconhecido, ou seja, a reputação de um nó desconhecido vai variar de acordo com as experiências anteriores passadas pelo nó requisitante.

Quando os nós deixam o sistema normalmente não avisam a outros nós sobre essa ação. Poucos trabalhos tratam dessa questão que pode gerar alguns problemas de segurança. Por exemplo, no trabalho de [Singh e Liu, 2003], se existe para um nó qualquer um único nó THA e este nó THA deixa o sistema sem qualquer aviso por ocasião de uma falha ou um acidente, ele não realiza as operações de delegação de suas obrigações e o valor de confiança do nó pelo qual ele era responsável é perdido e o nó perde o que conquistou através de um bom-uso contínuo do sistema.

Um problema relacionado com esse caso é o exemplo de nós que saem da rede depois de várias transações e retorna com outro identificador sem avisar outros nós. Outros nós não têm como saber que o nó recém-chegado é o mesmo que se relacionaram há algum tempo antes. O problema se agrava pois, em algumas arquiteturas propostas como [Cornelli et al., 2002] e [Kamvar et al., 2003], não existe um tempo definido para abandonar as informações armazenadas pertinentes a identificadores não-presentes na rede. Se esses nós abandonarem os dados no momento em que percebem que o identificador está ativo, corre o risco de o nó apenas ter saído por algum tempo do sistema e quando este volta os outros nós apagaram as informações que possuíam sobre ele. Mas se os nós nunca descartarem esse tipo de informação, as bases se tornarão repletas de informações sobre identificadores abandonados.

---

[1] Um nó *bootstrap* é o nó responsável pela conexão com um nó recém-chegado ao sistema.

[2] *Trust Holding Agent*

3. Role-Based Reputation Protocol

O protocolo Role-Based Reputation Protocol (RBRP) é um protocolo de reputação baseado em papéis para redes peer-to-peer. Esse protocolo contribui com alguns pontos significativos no estado-da-arte sobre segurança em redes peer-to-peer [Pellissari, F. R., 2005].

O ponto principal é distinguir em papéis os nós presentes nas redes, aproximando-se do modelo de controle de acesso RBAC[3]. O segundo ponto é usar nomes ao invés de números para valores de reputação, facilitando a classificação em papéis pelo usuário do sistema. A distinção em papéis auxilia na classificação de reputação dos nós. Nos trabalhos relacionados, um nó é considerado confiável ou não independente do tipo de recurso que é buscado no sistema. O uso de papéis, portanto, iguala em reputação diversos nós que, por algumas afinidades, se comportam de maneira parecida.

Outra contribuição deste protocolo é a utilização dos papéis no processo da classificação da reputação de um determinado nó da rede de acordo com o tipo de dado desejado numa troca. Nós que usam uma rede p2p para, por exemplo, trocar apenas arquivos-texto serão considerados nós com boa reputação para troca de arquivos-texto somente. Se um usuário buscar a reputação de um destes nós para obter um arquivo texto o valor de reputação não será o mesmo caso opte por um arquivo MP3.

Uma outra vantagem desse protocolo está no emprego do certificado de nomes SPKI/SDSI[4] [Mello, R., 2003] para informar um valor de reputação. Esse uso aproxima o RBRP de um padrão internacional e permite que um controle de acesso usando SPKI/SDSI seja anexado ao protocolo sem maiores dificuldades. Outra possibilidade é desenvolver uma cadeia de confiança através da rede.

Outra característica importante nesse protocolo é atribuir um campo validade ao valor de reputação. Isso é importante porque os nós podem abandonar um identificador; então os dados presentes nas bases de dados relacionados com tal nó também devem expirar, tornando as bases de dados mais atualizadas e menores.

O RBRP não é uma extensão de um protocolo, já que pode ser implementado em qualquer sistema p2p, isto é, é independente do protocolo de rede p2p utilizado. Também não pode ser considerado apenas um serviço, já que as mensagens usadas na comunicação são definidas formalmente.

3.1. Seres Humanos e Redes Peer-to-Peer

A aplicação Napster foi, sem dúvida, a principal responsável pela disseminação do conceito de redes p2p pelo mundo de tecnologia da informação. Assim como o Napster, outros sistemas que desempenham a mesma função, a troca de informações ponto-aponto, são nomes comumente relacionados com p2p. Aplicações como KaZaA, Gnutella ou Emule são bons exemplos desse fato.

Essas aplicações têm diversos pontos em comum. Um desses pontos é a funcionalidade do sistema: a troca de arquivos pela Internet. Mas o ponto a ser

---

[3] *Role-Based Access Control*

[4] *Simple Public Key Infraestructure/ Simple Distributed Security Infraestructure*

ressaltado aqui é a presença humana atrás de cada nó do sistema. Em todos esses sistemas, cada nó representa um ser humano buscando recursos na Internet.

Seres humanos possuem diversas diferenças de raciocínio se comparados com máquinas. Essas diferenças alteram o modo como o ser humano encara a confiança. Para máquinas, é simples quantificar em valores numéricos um valor de confiança, mas para seres humanos não. Seres humanos, por outro lado, são mais capazes de associar um valor de confiança a um nome, como amigo ou colega .

3.2. Nomear Segurança X Quantificar Segurança

Considerando que os nós das principais redes p2p são controlados por seres humanos e estes têm melhor capacidade para associar a confiança a nomes, o uso de nomes de confiança para valores de reputação em redes p2p parece, num primeiro momento, mais correto. Entretanto, é preciso tomar alguns cuidados.

Um ponto em aberto com relação aos nomes relacionados com confiança é o idioma em que são apresentados. Um usuário português pode não entender, por exemplo, os nomes usados por um inglês, e vice-versa. Para solucionar esse problema, podem ser adotadas duas ações. A primeira é regulamentar uma língua oficial dentro da rede. Então os nós só podem usar nomes de confiança escritos nessa língua. Outra solução, bem mais complexa, é manter uma base de dados para traduções.

Outro ponto é a forma como os seres humanos encaram os nomes de confiança. É possível que exista uma pessoa que tenha vários amigos, mas não confie muito neles. Outra pessoa pode possuir poucos amigos, mas confiar muito neles. Essas pessoas usam o nome amigo para um valor de confiança diferente. Uma solução para isso é acompanhar sempre do nome amigo um outro nome que quantificaria a confiança, como alto ou muito alto . Tais valores podem representar valores numéricos, como, por exemplo, o nome muito alto representa valor numérico 10 e valor baixo representa valor 3.

3.3. Papéis de Confiança

Os nomes a serem usados em protocolos de reputação não devem ser escolhidos a esmo. Essa escolha deve ser feita de acordo com funções desempenhadas pelos nós no sistema. Embora todos os nós possuam as mesmas funcionalidades na rede, os nós tendem a concentrar suas atividades nas que mais desejam realizar. Por exemplo, em um sistema como o Emule é permitida a troca de arquivos dos tipos: MP3, Vídeo, Executáveis e texto. No Emule usuários que buscam recursos de leitura certamente vão concentrar suas buscas e seu repositório de dados em arquivos texto e usuários que buscam músicas tendem a possuir mais arquivos MP3 que arquivos-texto.

Essa separação de atividades em redes p2p gera uma separação de funcionalidades realizadas pelos nós. Um determinado nó pode separar, portanto, os outros nós de acordo com as funções que estes representam no sistema. Essas funções podem ser representadas por papéis, como os papéis usados no modelo RBAC. Um exemplo é que um nó de uma rede p2p pode definir, usando o conceito de papéis, um grupo de nós que representam um papel “usuário de arquivos MP3”. Então esse nó atribui maior valor de confiança aos nós que pertencem a esse grupo e representam esse papel.

3.4. Bases de dados do RBRP

Cada nó do protocolo RBRP possui as bases mostradas na Figura 1. Pode-se observar nessa figura duas bases. A primeira é a base de nomes, a qual lista os nomes conhecidos pelo nó que a possui. Nessa base existem três campos principais. O primeiro campo, nome, lista os nomes indicando os papéis conhecidos pelo nó. O segundo, valor de confiança, mostra quanto o nó confia no papel relacionado. Finalmente, o terceiro campo indica os tipos de dados válidos para a confiança. Inicialmente é proposto separar os dados pelos tipos diferentes, mas o protocolo pode ser avançado de modo que suporte outros tipos mais elaborados de distinção de dados.

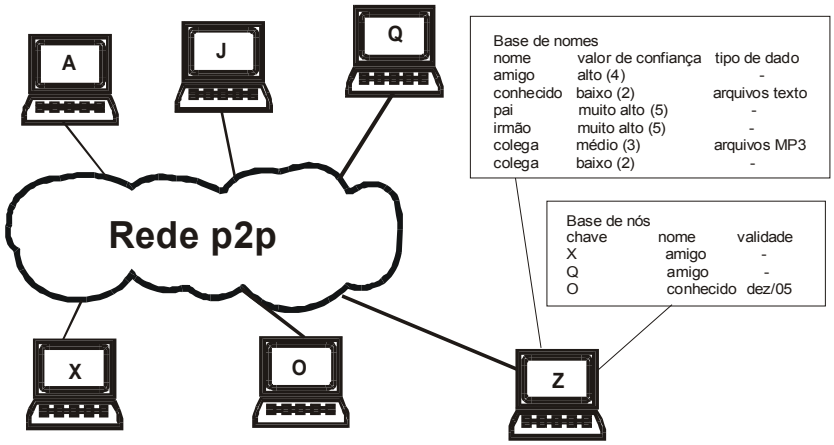

Figura 1. Bases de dados do RBRP

A segunda base lista as chaves que representam outros nós do sistema. As chaves servem para construir um relacionamento com os nomes listados na primeira base. Além disso, existe um campo opcional de validade, pois esse relacionamento pode expirar. A partir dessas duas bases os nós são capazes de armazenar suas experiências passadas e classificar os nós conhecidos por papéis desempenhados no sistema.

3.5. Busca por Recursos

O protocolo RBRP não influi no resultado das buscas por conteúdo em uma rede p2p. Essa busca depende exclusivamente do tipo de rede na qual esse protocolo seja utilizado. Se, por exemplo, o RBRP for aplicado à rede Napster, a busca é centralizada. Por outro lado, se for aplicado ao Gnutella a busca é descentralizada e desestruturada.

Busca por: "u2"
Tipo de dado: MP3

Reputação: alta — baixa

Nome	Origem
u2 - vertigo.mp3	conhecido (ver detalhes da origem)
u2 - one.mp3	desconhecido(procurar reputação)
u2 - vertigo.mp3	amigo (ver detalhes da origem)
u2 - vertigo.mp3	desconhecido(procurar reputação)
u2 - sunday bloody sunday.mp3	amigo (ver detalhes da origem)
u2 - with or without you.mp3	amigo (ver detalhes da origem)
u2 - vertigo.mp3	desconhecido(procurar reputação)

Figura 2. Exemplo de resultado de busca com o RBRP

Apesar da busca não ser alterada pelo RBRP, o protocolo realiza uma ação de classificação dos resultados de acordo com o nível de confiança indicado em suas bases. Na listagem dos resultados são mostrados os resultados advindos dos nós que estão presentes na base de nós desse nó requisitante. Assim, a aplicação indica a preferência

por usar recursos dos nós com maiores valores de reputação. A Figura 2 apresenta um exemplo dessa questão.

A Figura 2 ilustra um exemplo de um resultado busca numa rede p2p que usa o protocolo RBRP. Por exemplo, considerando que um determinado usuário resolve buscar uma MP3 da banda "U2". Ele então faz uma pesquisa por "U2" pelo sistema. O resultado que ele recebe está marcado na Figura 2. O protocolo RBRP deve, então, sinalizar através de cores ou outro esquema quais as melhores fontes para a obtenção do recurso. No caso do exemplo, foram encontrados três arquivos diferentes com a mesma reputação. O usuário então deve escolher qual dos três arquivos lhe interessa mais.

Um detalhe importante é que o RBRP não força o usuário a escolher nenhum arquivo, nem realiza uma troca automática a partir da pesquisa. Essa troca automática não é viável, pois em alguns casos é possível que a busca retorne centenas de recursos com a mesma reputação, todos altos. Outro detalhe é que a aplicação deve habilitar que o usuário faça uma pesquisa por um valor de reputação de um nó desconhecido. Essa pesquisa é feita caso o usuário deseje conhecer a opinião dos seus nós conhecidos sobre um nó desconhecido.

3.6. Cálculo de Reputação de Nós Desconhecidos

Um nó que deseja um recurso de outro usuário desconhecido por ele precisa do valor de reputação para decidir se requisita ou não um determinado recurso a esse usuário. Essa verificação da reputação é mostrada na Figura 3. Primeiro, o nó que deseja conhecer o valor de reputação do outro nó envia uma mensagem aos nós que estão presentes em sua base de nós. Essa mensagem contém uma requisição sobre a reputação do nó que deseja conhecer.

Em seguida, os nós que conhecem esse nó descrito na requisição respondem com um certificado de nomes SPKI/SDSI. O certificado é usado para associar uma chave a um nome. O nome no certificado corresponde ao papel que o nó da requisição pertence na tabela do nó que recebeu a requisição. Por exemplo, na Figura 3, o nó que envia a requisição é o nó Q, o nó que responde é o Z e o nó requisitado é o X. Pode-se ver, no exemplo, que o nó Z indica que o nó X é um nó definido com papel "amigo". Portanto, Q conclui que o nó X é um amigo de seu amigo. A partir desse ponto, o servent Q pode decidir se deseja ou não iniciar a troca de recursos.

Deve-se notar que a política seguida pelo usuário do sistema para definir sua base de nomes fica totalmente a cargo do usuário, fato também visto nos outros trabalhos sobre reputação descritos neste documento. Nada impede, porém, que um usuário ou um grupo deles usem scripts ou algum modelo para designar automaticamente os papéis aos outros nós do sistema. Um exemplo seria se, depois de uma troca de recursos com sucesso com um determinado nó, tal nó recebesse um papel chamado "conhecido" automaticamente.

Apesar da distribuição de papéis existente no RBRP não ser utilizada em nenhum dos outros trabalhos sobre reputação, alguns conceitos empregados no RBRP são provenientes desses trabalhos citados no seção 2, principalmente em [Kamvar et al., 2003, Damiani et al., 2002, Cornelli, 2002, Singh e Lui, 2003, Gupta et al., 2003]. O conceito reaproveitado mais importante é a descentralização dos valores de reputação usado por [Kamvar et al., 2003]. Diferentemente de [Damiani et al., 2002] e [Singh e Liu, 2003], o protocolo RBRP obtém diferentes valores de reputação dependendo do nó

que requisita um valor de reputação de um determinado nó. Isso acontece pois o nó que faz a requisição leva em conta sua própria base de nós para verificar a reputação que deseja.

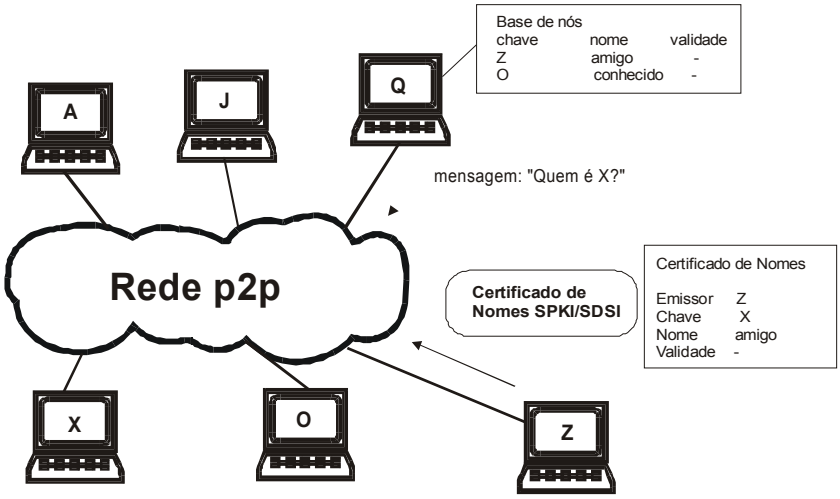

Figura 3. Requisição de reputação

Outro ponto em comum com os outros trabalhos é deixar a decisão sobre se um valor de reputação é suficientemente alto ou não aos usuários. Nenhum dos trabalhos, inclusive este, define valores mínimos ou máximos para aceitar ou recusar uma troca de recursos. Isso porque esses valores dependem da política adotada pelo requisitante do recurso.

O protocolo RBRP não traz nenhum benefício aos nós que acabam de entrar no sistema. Essa restrição é necessária para que usuários maliciosos não troquem de identificador a todo momento para ganhar benefícios. Quando usuários entram no sistema, possuem suas bases de dados sem nenhum valor, portanto devem confiar inicialmente em alguns nós para poderem utilizar, mais adiante, das vantagens do protocolo de reputação. Isso é o significado de reputação: aproveitar-se de experiências anteriores para conseguir segurança.

3.7. Justificativa Sobre o Uso do SPKI/SDSI

O protocolo PRBP, mesmo sem concentrar seu foco no controle de acesso, adota um certificado de nomes para identificar um nó associado a um papel durante um cálculo de reputação. Embora esse uso possa ser trocado por uma outra estrutura parecida, o uso do certificado de nomes SPKI/SDSI, além de satisfazer todas as necessidades do protocolo, traz algumas vantagens ao modelo.

A principal vantagem é agregar ao modelo um protocolo padrão da Internet. Com o uso do certificado de nomes SPKI/SDSI a aplicação de um modelo SPKI de controle de acesso torna-se mais simples, já que parte da estrutura já deve estar implementada no sistema.

O SPKI é uma infra-estrutura de chaves públicas que se enquadra muito bem dentro do protocolo, pois não utiliza um centro de distribuição de chaves, o que também deve ocorrer em redes peer-to-peer puras. Além disso, a associação de chaves com nomes locais tem a mesma função da base de nomes usada no protocolo RBRP.

Entretanto, o SPKI limita de certo modo o anonimato na rede, pois insere rótulos aos usuários do sistema. Entretanto, isso não traz, de modo geral, danos graves ao anonimato da rede p2p, pois esses rótulos correspondem apenas ao comportamento do nó, não a identificação do usuário do sistema.

3.8. Limitações do RBRP

O RBRP, apesar de atender certos problemas encontrados em protocolos de reputação, possui algumas limitações. Como o RBRP é baseado no uso de papéis para o cálculo de reputação, seu uso é mais indicado em redes p2p cujos nós representam seres humanos, como a Gnutella ou o KaZaA.

Outro ponto é a falta de uma política pré-estabelecida para a definição de um valor padrão de confiança em pesquisas por confiança de nós desconhecidos. Em outros protocolos como [Kamvar et al., 2003], os valores de reputação de nós desconhecidos são calculados automaticamente quando ocorre uma requisição de reputação. Entretanto, isso pode ser útil no sentido de deixar o usuário mais livre para definir o valor de reputação que deseja.

Apesar do uso do certificado de nomes SPKI/SDSI para o cálculo de reputação, não é enfoque do protocolo realizar qualquer tipo de controle de acesso no sistema. Entretanto, esse uso possibilita uma implementação de um mecanismo de controle de acesso baseado em SPKI/SDSI com certa facilidade, já que a estrutura do SPKI/SDSI já deve estar implementada no sistema para que ele funcione usando certificados de nomes SPKI/SDSI.

4. Redução do Valor Médio de Tentativas por Download de Recurso Válido

Em sistemas p2p, podem existir diversos recursos inválidos ou impróprios dentro das redes. Exemplos são arquivos incompletos e conteúdo pornográfico, que podem ser requisitados devido a falsas informações nos metadados dos recursos. Portanto, os usuários desses sistemas podem realizar mais de um download para conseguir um recurso de boa qualidade.

Em redes p2p sem protocolos de reputação, o valor médio de tentativas de download varia exclusivamente de acordo com a proporção de usuários maliciosos presentes no sistema. Numa rede p2p cuja porcentagem de usuários maliciosos chega a 60% do total do sistema e cada tentativa de troca de recursos com tais nós é falha, cada usuário necessita de 2,5 tentativas para cada download com sucesso. Isso gera uma sobrecarga de 125% no tráfego de recursos dentro da rede[5]. Entretanto, o uso de protocolos de reputação auxilia na diminuição desse valor. Como os nós armazenam as boas experiências, futuras trocas de recurso realizadas entre nós com boa reputação têm menor probabilidade de encontrarem recursos inválidos. Se um nó designa corretamente outro nó como confiável, uma troca de recursos entre eles dificilmente trará um recurso impróprio.

Para visualizar melhor o cenário, o modelo matemático para cálculo de largura de banda extra utilizada numa rede p2p é proposto a seguir. Considerando que uma rede p2p possui *n* nós, sendo que desse total *m* são maliciosos, a probabilidade de encontrar-se um recurso inválido é mostrada na fórmula 4.1:

[5] Tais conclusões podem ser tiradas a partir das fórmulas descritas nesta seção.

$P(i) = (m / n) * Im$, para $n>1$, $m \geq 0$ e $0<Im\leq 1$ (4.1)

Na fórmula 4.1, *Im* indica o valor médio de recursos inválidos de um usuário malicioso. Portanto, para um sistema com 10.000 nós, sendo 2.000 maliciosos e com um índice de recursos inválidos de 0,8, a probabilidade de se obter um recurso inválido é 0,16, ou seja 16%.

Essa probabilidade de se obter um recurso inválido aumenta o número de tentativas médio para se obter um recurso válido com sucesso. Esse número de tentativas t é ilustrado pela fórmula 4.2:

$t = 1 / (1 - P(i))$, para $P(i) \neq 1$ (4.2)

Considerando um valor de $P(i) = 0,16$, o valor de $t \approx 1,19$. Isso significa que em uma rede com as especificações detalhadas, cada download com sucesso requer 1,19 tentativas de download. Isso gera um tráfego extra *e* no sistema, mostrado na fórmula 4.3:

$e = t - 1$ (4.3)

Como no exemplo usado o valor de *t* é de aproximadamente 1,19, o valor de *e* é 19%, ou seja, os nós maliciosos do sistema geram um tráfego inútil de 19% sobre o total necessário.

Esse excesso de tráfego pode ser diminuído com o uso do RBRP. Através do uso do RBRP os usuários são capazes de identificar nós amigos e nós maliciosos. Se um determinado usuário identificar uma quantidade suficiente de nós amigos e maliciosos, o número médio de tentativas de download irá diminuir e, portanto, o excesso de tráfego irá diminuir também.

Um usuário usando o RBRP é capaz de identificar *q* nós maliciosos. Sendo assim, a probabilidade de obter-se um recurso inválido é dada pela fórmula 4.4:

$P_r(i) = ((m - q) / n) * Im$, para $n>1$, $m \geq 0$, $0<Im\leq 1$ e $q \geq 0$ (4.4)

Usando o exemplo em questão, caso um usuário identifique 50 nós maliciosos, ou seja, $q = 50$, a probabilidade é $P_r(i) \approx 0,16$. Pode-se notar que a probabilidade praticamente não muda, então apenas identificando nós maliciosos no sistema pouco ajuda na redução das tentativas de download.

Entretanto, um usuário RBRP também é capaz de identificar nós confiáveis. Esses nós confiáveis tanto possuem recursos válidos quanto podem informar sobre nós maliciosos que conhecem. Então, na fórmula 4.5, *r* é o número de nós confiáveis identificados e *s* é o valor médio de usuários maliciosos conhecidos por tais nós:

$P_{rb}(i) = ((m - q - (r * s)) / n) * Im$, para $n>1$, $m \geq 0$, $0<Im\leq 1$, $q \geq 0$, $r \geq 0$ e $s \geq 0$ (4.5)

Na fórmula 4.5, usando o já citado exemplo, com $r = 50$ e $s = 25$, o valor de $P_{rb}(i) \approx 0,05$. Portanto, nota-se uma mudança significativa no número médio de tentativas de download *t*, sendo $t \approx 1,005$, eliminando assim o tráfego inútil no sistema pois nesse caso $e = 0,005$.

5. Implementação

O protocolo RBRP é possível de ser implantado dentro de qualquer sistema peer-to-peer, já que cada usuário, independente dos demais, é capaz de classificar de acordo

com papéis os outros nós do sistema. Basta adicionar a um nó as tabelas citadas na seção 3, alguns procedimentos para manipular essas tabelas e um suporte para manipular a infra-estrutura de chaves públicas SPKI/SDSI, que esse nó torna-se capaz de realizar a classificação dos outros nós do sistema. Entretanto, se os outros nós do sistema não forem adaptados ao uso do RBRP, as pesquisas de reputação não terão efeito, já que devem ter as respostas armazenadas nas bases de dados para responder às pesquisas.

Na arquitetura apresentada na seção 3, o sistema peer-to-peer usa uma chave pública para identificar um nó. O uso de uma chave pública de 1024 bits garante um identificador único e seguro para os nós, já que a quebra de uma chave de 1024 bits é computacionalmente inviável [Stallings, 2003]. Porém, nada impede que o RBRP seja implementado em um sistema que use pseudônimos para identificar os nós. O problema nesse caso é garantir a identificação única dos nós, já que os pseudônimos não garantem autenticidade.

5.1. DNet

A implementação realizada neste trabalho é como o modelo de implementação de (Damiani et al., 2002), que altera o código-fonte do Gnutella para que este funcione em conjunto com o protocolo de reputação, no caso deste trabalho o RBRP. O código-fonte do Gnutella pode ser encontrado nas linguagens C++ e Java na Internet, como a aplicação DNet (DNet, 2004). Essa é uma aplicação de código-fonte aberto que funciona sobre o protocolo do Gnutella. O modelo de conexão usado na aplicação está representado na Figura 5.

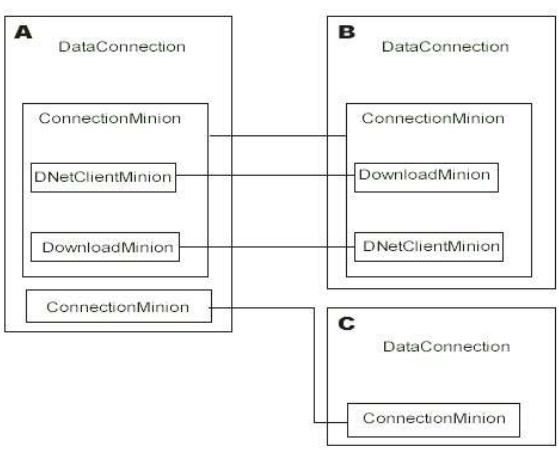

Figura 5: Exemplo de conexões entre nós DNet

Cada nó possui uma classe principal chamada DataConnection. Cada nó pode criar subclasses ConnectionMinion para que estas se conectem com outros nós. Na figura 6.1 o nó A está conectado com o nó B e o nó C, porém B e C não estão conectados diretamente. Cada ConnectionMinion pode usar as subclasses DownloadMinion para gerenciar um download e a DNetClientMinion para gerenciar uploads. No exemplo da figura o nó A está realizando um download de B e B realiza um download de A. Além disso, a classe ConnectionMinion permite que os nós enviem consultas para seus peers.

Para que o protocolo RBRP fosse adicionado nesse sistema, foram realizadas algumas modificações no protocolo Gnutella. O ponto mais importante é a interação do protocolo Gnutella com as bases de dados do RBRP. Para que o RBRP funcione, ao menos localmente, as duas bases – a base de nós e a base de nomes – são adicionadas ao sistema e devem ser preenchidas de acordo com as necessidades do usuário. O usuário deve ter a oportunidade de adicionar ou remover *servents* e papéis sempre que desejar. Além disso, depois que os nós estiverem cadastrados no sistema, a aplicação deve informar o usuário sobre os dados das bases sempre que ele deseje se comunicar com um nó conhecido.

5.2. Formato das Mensagens

O protocolo RBRP possui basicamente 2 mensagens, a mensagem de requisição de reputação (*RepRequest*) e a de resposta (*RepResponse*), compostas por um cabeçalho (Figura 6) seguido de algumas informações (Figura 7). Uma mensagem de requisição pode ser gerada a qualquer momento por qualquer nó do sistema. Já a mensagem de resposta pode surgir a partir de uma mensagem de requisição recebida.

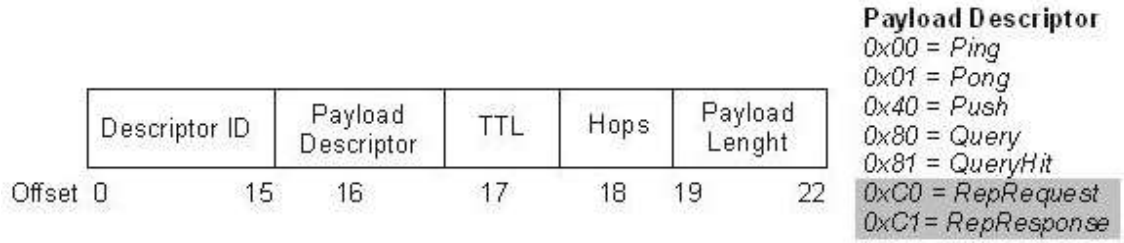

Figura 6: Formato do cabeçalho Gnutella estendido pelo RBRP.

As mensagens seguem o cabeçalho do protocolo Gnutella, porém com uma alteração no campo *Payload Descriptor*, como mostra a Figura 6. Esse campo deve aceitar dois valores novos, para as mensagens *RepRequest* e *RepResponse*. Esse formato similar ao Gnutella permite uma melhor adaptação do protocolo de reputação nas aplicações Gnutella existentes [Clip2 2004].

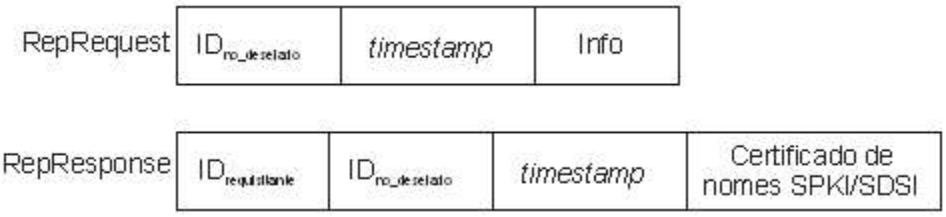

Figura 7: Formato da carga útil das mensagens RBRP

A Figura 7 apresenta o formato de uma mensagem de requisição de reputação (*RepRequest*). O primeiro campo, chamado de $ID_{no\_desejado}$, corresponde ao *servent* que se deseja conhecer o valor de reputação. O segundo campo corresponde a um valor de *timestamp* para proteger o protocolo de ataques de repetição. O terceiro campo (*Info*) mostra algumas informações que podem ser passadas para auxiliar os nós no cálculo de reputação.

A mensagem *RepResponse*, apresentada na Figura 7, possui 4 campos. Os três primeiros campos ($ID_{requisitante}$, $ID_{no\_desejado}$ e *timestamp*), assim como a mensagem *RepRequest*, apresentam respectivamente os mesmos significados da *RepRequest*. O

quarto campo carrega um Certificado de nomes SPKI/SDSI, cuja funcionalidade já está explicada na seção 4.

6. Conclusão

Este artigo descreveu o Role-Based Reputation Protocol (RBRP), um protocolo de reputação que, diferente dos demais pesquisados, usa nomes ao invés de valores numéricos para avaliar um patamar de reputação. Essa diferença auxilia o sistema a realizar uma classificação dos nós com relação à reputação que cada ponto do sistema possui.

Outra importante contribuição desse protocolo é abstrair os valores numéricos presentes nos demais trabalhos, auxiliando na aceitação do uso do protocolo pelos usuários do sistema. Essa aceitação é importante porque o uso do protocolo deve ser feito por uma parte significativa da rede para que o protocolo produza efeitos aceitáveis com relação à segurança do sistema.

Uma terceira contribuição do protocolo é separar os valores de reputação por tipos de dados. Isso é importante, pois uma fonte de dados pode ser confiável apenas para um tipo, como arquivos-texto. Do mesmo modo um nó pode ser considerado malicioso apenas para um tipo de dado, apesar de ficar a cargo do usuário tomar essa decisão.

Além das contribuições já citadas, o protocolo usa uma opção de atribuir validade aos valores de reputação. Essa atribuição permite tabelas de reputação mais atualizadas, pois em redes p2p sempre é possível que nós abandonem o sistema. Quando isso ocorre, as descrições desse nó não devem ficar indefinidamente nas bases de dados dos outros nós.

Outro ponto importante do trabalho é aproximar o protocolo RBRP da infra-estrutura de chaves SPKI/SDSI. Essa aproximação permite uma futura aplicação de um modelo de controle de acesso com menores dificuldades. Além disso, o uso do SPKI/SDSI é importante pelo fato de tratar-se de um padrão internacional.

Por fim, o trabalho provou matematicamente que o uso pleno do protocolo pode trazer, além do benefício da segurança, benefícios com relação à largura de banda consumida pelo sistema. Isso ocorre porque o protocolo de reputação, quando corretamente utilizado, ajuda a diminuir as trocas de recursos inválidas pela rede.

Embora possua diversas contribuições, o RBRP possui uma limitação com relação ao seu uso. Como o protocolo é baseado em nomes para o cálculo de reputação, o RBRP torna-se mais apropriado para sistemas cujos nós representam seres humanos. Redes peer-to-peer independentes de seres humanos, como a SETI@Home, não são capazes, a princípio, de tratar com nomes de reputação. Outra limitação do RBRP é não atribuir valores de reputação padrões. Esses valores são úteis quando os usuários da rede não estão devidamente preocupados com a segurança do sistema. Entretanto, tais valores padrões podem não refletir as reais preocupações dos usuários.

Um terceiro ponto que o protocolo não trata com clareza é a troca de recursos compartilhados. Alguns sistemas p2p mais recentes, como o Emule, permitem que um usuário requisite um único recurso e obtenha o recurso de várias origens, transferindo uma parte de cada fonte. Caso tal recurso seja ruim, o protocolo RBRP deixa a cargo do

usuário a decisão de quem diminuir o valor de reputação, se de apenas uma ou de todas as fontes usadas.

Essas limitações podem ser pesquisadas em trabalhos futuros. Além dessas duas questões, outras são válidas para estudo. Uma questão importante não tratada na pesquisa realizada foi o uso do SPKI/SDSI para controle de acesso no sistema, aumentando ainda mais a segurança das redes peer-to-peer que utilizassem a arquitetura descrita aqui. Outro ponto a cargo de trabalhos futuros é a evolução dos filtros de tipos de dados pesquisados pelos sistemas p2p e pelos protocolos de reputação. O RBRP classifica os dados apenas com relação ao formato do arquivo (MP3, arquivo-texto). Uma idéia é, no caso dos arquivos MP3, por exemplo, classificá-los de acordo com o ritmo da música ou autor.

Referências

Bailes, J. E. e Templeton, G. F. (2004). Managing P2P Security. Communications of the ACM, 47(9):95-98.

Clip2 (2004). "The Gnutella Protocol Specification v0.4". Document Revision. http://www9.limewire.com/developer/gnutella_protocol_0.4.pdf

Cornelli, F., Damiani, E., Vimercati,S. C., Paraboschi, S. and Samarati, P. (2002). "Choosing Reputable Servents in a P2P Network". In: 11th International World Wide Web Conference (WWW'02), May 7-11, Honolulu, Hawaii, USA.

Damiani, E., Vimercati, S. C., Paraboschi, S., Samarati, P. and Violante, F. (2002). "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks". In: Computer and Communications Security (CCS'02), November 18-22, Washington DC, USA.

Dnet (2004). Website. http://schnarff.com/gnutelladev/source/dnet/dnet/Gnutella/

Pellissari, F. R. (2005). "RBRP: Protocolo de Reputação Baseado em Papéis". Dissertação de Mestrado, UFSC, Florianópolis.

Gupta, M., Judge, P. and Ammar, M. (2003). "A Reputation System for Peer-to-Peer Networks". In: 13th International Workshop on Network and Operating Systems Suport for Digital Audio and Video (NOSSDAV' 03), June 1-3, Monterrey, California, USA.

Kamvar, S., Schlosse, M. T. and Garcia-Molina, H. (2003). "The EigenTrust Algorithm for Reputation Management in P2P Networks". In: 12th International World Wide Web Conference (WWW'2003), May 20-24, Budapest, Hungary.

Mello, E. R. (2003). "Redes de confiança em sistemas de objetos CORBA". Dissertação de mestrado, UFSC, Florianópolis.

Singh, A. and Liu, L. (2003). "TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems". In: 3rd IEEE International Conference on Peer-to-Peer Computing, September 1-3, Linköping, Sweden.

Stallings, W. (2003). "Cryptography and Network Security". 3rd Ed., Prentice Hall.