A Token-based Reputation Framework

Ricardo Godinho[1], Carlos Ribeiro[1]

[1] Instituto Superior Técnico – Taguspark
Av. Prof. Dr. Cavaco Silva, 2744-016 Porto Salvo, Portugal
{ricardo.godinho, carlos.ribeiro}@tagus.ist.utl.pt

Resumo

Num ambiente distribuído, os nós da rede apresentam a necessidade de obter recomendações dos seus pares, no sentido de inferir uma avaliação acerca da reputação de uma determinada entidade. Genericamente, o modo como estes nós recolhem informação de *feedback* conduz a um elevado número de interrogações na rede. No seguimento da investigação efectuada, este artigo introduz um modelo bidireccional, utilizando o conceito de lista de recomendação inversa, que está habilitado a determinar valores de confiança, através de uma quantidade mínima de requisições na rede. Após a concepção deste modelo, adoptou-se uma noção designada de confiança diversificada, com o intuito de evitar as intenções maliciosas de alguns dos pares da rede. Utilizando esta noção, cada par é julgado de acordo com a sua capacidade de recomendação e habilidade no fornecimento de serviços ou recursos. Os resultados experimentais permitem obter conclusões em relação ao modelo bidireccional e à noção de confiança diversificada. Primeiramente, são evidenciadas as vantagens significativas, em termos de nós interrogados, daquele modelo. Seguidamente, a noção de confiança diversificada é confrontada perante um conjunto de ameaças onde se demonstra que em determinados cenários a rede não é significativamente perturbada pelo mau comportamento dos seus constituintes.

1 Introdução

As redes P2P são sistemas distribuídos descentralizados onde cada participante possui responsabilidades equivalentes. Nomeadamente, permitem que determinado utilizador actue simultaneamente como cliente e servidor. Neste sentido, é intuitiva a percepção de que a viabilidade de uma rede P2P depende essencialmente do nível de colaboração de cada um dos seus constituintes.

Com o intuito de evitar a degradação da rede através do funcionamento malicioso de algumas das suas entidades, a adopção de um esquema de reputação e confiança é essencial. Estes esquemas, tendem a punir as entidades que operam de uma forma prejudicial para a rede ou visam a incentivar os nós ao comportamento cooperativo, fazendo uso das noções de reputação e confiança. A reputação de uma entidade resulta da confiança que os vários pares têm nessa entidade. No sentido de averiguar se determinado agente é digno de confiança, cada nó deverá obter a reputação desse mesmo agente através de requisições efectuadas aos seus nós conhecidos.

Os esquemas de reputação e confiança actualmente mais relevantes, apesar de garantirem uma melhoria no funcionamento dos sistemas distribuídos, apresentam-se reféns de algumas condicionantes, como é o caso da arquitectura de rede. Concretamente, a maioria dos sistemas de reputação e confiança apenas se direcciona para situações onde existe o recurso a mecanismos centralizados ou onde a organização de rede é do tipo estruturada. Por outro lado, os sistemas vocacionados a operar em redes descentralizadas e não estruturadas, como é o caso da Gnutella [10], deparam-se com dificuldades acrescidas aquando da obtenção de um recurso ou de um valor de confiança para determinado nó. Nessa rede, a informação é recolhida dos seus pares através de técnicas de inundação. Tal situação pode conduzir a uma elevada sobrecarga em termos de quantidade de tráfego que circula na rede. Além disso, este ambiente ao fazer uso de um TTL (*Time To Live*) para evitar a propagação infinita de requisições, pode levar a que em situações de baixa densidade de partilha, o nó solicitador não obtenha a informação que desejaria.

Assim, o primeiro objectivo deste artigo passa por conseguir obter um valor de reputação de uma entidade através de uma solução que minimize o número de nós interrogados, conseguindo obter um maior número de caminhos entre a origem e o destino, através de um menor número de *hops*. Para esse efeito, começou-se por

desenvolver soluções de cálculo baseadas em recomendações de nós conhecidos. Numa primeira fase, apenas foram consideradas recomendações no sentido directo. De seguida, o valor de reputação é calculado recorrendo somente a recomendações inversas. Por último, ao se agregar ambos os tipos de recomendações, desenvolveu-se um modelo bidireccional que considera recomendações directas e inversas na mesma solução.

Foi primordial utilizar um sistema que permitisse avaliar as várias soluções desenvolvidas com o intuito de determinar aquela que se aproxima de uma situação óptima. Por permitir soluções centralizadas e descentralizadas, optou-se pela utilização do EigenTrust [1]. Considerando este sistema como meio de comparação, os resultados demonstram a vantagem significativa, em termos de nós interrogados, de uma solução que utilize simultaneamente ambos os modos de recomendação.

No modelo de procura bidireccional, a rede torna-se mais sensível aos nós que de forma maliciosa submetem *feedback* desonesto ou incorrecto. Nesta linha, o segundo objectivo deste trabalho passa por redefinir a noção de confiança, considerando um valor associado à capacidade de estabelecer recomendações e outro destinado à capacidade no fornecimento de recursos ou serviços. É esta delimitação do alcance de confiança que permite enfraquecer o impacto de recomendações mal intencionadas de nós maliciosos. Com base nesta noção de confiança diversificada, os resultados demonstram que a rede se pode tornar praticamente indiferente às recomendações de índole maliciosa.

No presente artigo, começa-se por descrever os ataques e fragilidades, bem como as propriedades e componentes dos sistemas de reputação e confiança (secção 2). A secção 3 corresponde à descrição e caracterização dos sistemas de reputação actualmente mais relevantes, onde se dá ênfase ao EigenTrust. A quarta secção descreve os algoritmos desenvolvidos, partindo da contextualização do modelo bidireccional e da noção de confiança diversificada. A quinta secção apresenta os resultados experimentais obtidos, antes de se proceder à conclusão do artigo na secção 6.

Sendo este artigo resultante de uma dissertação de mestrado, considerações ou resultados adicionais podem ser obtidos através da consulta do documento integral da mesma.

2 Sistemas de Reputação e Confiança

As pessoas interagem diariamente entre elas. Comunicam com familiares, amigos, vizinhos ou outros contactos. Este tipo de relação constitui uma rede, designada de rede social. Nas redes sociais, as pessoas tendem a confiar mais em amigos do que em pessoas totalmente desconhecidas. Neste âmbito, é importante introduzir os conceitos de reputação e confiança. A confiança é por vezes baseada na reputação. Uma pessoa que apresente boa reputação é mais digna de confiança do que outra pessoa cuja reputação seja negativa. Nas redes de computadores, construir um esquema semelhante, baseado na reputação e confiança, é estimulante. O maior desafio prende-se com o anonimato. Ao contrário das redes sociais, os utilizadores das redes de computadores não se observam mutuamente, o que pode conduzir a uma falta de confiança naquilo que terceiros possam dizer [2]. Sendo assim, é necessário um mecanismo de suporte ao estabelecimento de relações de confiança, isto é, sistemas baseados em reputação e confiança [3]. No entanto, existem inúmeras técnicas que podem ser exploradas, com o intuito de danificar o seu funcionamento, quer seja para tirar partido de alguma situação ou simplesmente comprometer o sistema.

Nos sistemas P2P os nós podem ser classificados como egoístas ou maliciosos. Um exemplo concreto de nós egoístas é o caso dos *freeriders*. Estes nós usam recursos sem oferecer nada em troca [6]. Um nó que actue de forma traiçoeira é outro tipo de comportamento indesejado. Alguns pares apresentam um funcionamento correcto durante um certo período de tempo. Após esta fase, tendem a agir de uma forma mal intencionada. Esta técnica tem especial efeito no caso em que uma reputação elevada corresponde a privilégios adicionais [4]. O *whitewashing* consiste num par que de forma voluntária abandona o sistema P2P, voltando a associar-se posteriormente, com uma identidade nova, de forma a libertar a má reputação associada à sua identidade anterior [5]. Em sistemas P2P, é possível que nós mal intencionados enviem acusações falsas, ou forneçam relatórios falsos de forma a afectar um par inocente [6].

Em muitas situações, o dano provocado por um conjunto de nós mal comportados, é significativamente maior do que se estes actuassem isoladamente. Estes nós conspiram contra um nó alvo, tendo como intenção influenciar a opinião externa acerca desse nó. Em esquemas de reputação, a actuação em conluio é extremamente difícil de ser detectada [6].

Idealmente, um sistema de reputação e confiança deve respeitar um conjunto de propriedades [6]. A primeira corresponde ao tipo de *feedback*. A confiança sobre um nó pode basear-se no *feedback* positivo ou

negativo, dos outros nós em relação a esse. É desejável que um esquema de confiança contemple vários tipos de *feedback*. A segunda propriedade corresponde à comunicação e armazenamento. Existe a necessidade que haja um *trade-off* entre o custo de trocar demasiada informação e obter um valor de confiança credível. Do mesmo modo, é fundamental um *trade-off* entre a quantidade de informação de *feedback* que deve ser armazenada para avaliar a credibilidade da transacção e as implicações desse armazenamento em termos de ocupação de memória. A última propriedade consiste no anonimato. Os sistemas de reputação e confiança tendem a proteger a identidade do nó que submete *feedback*. A propriedade de anonimato visa preservar o par que envia *feedback*, de qualquer tipo de retaliação.

Além do respeito pelas propriedades apresentadas, genericamente, a concepção de esquemas de reputação envolve três componentes principais [4]. A primeira componente consiste na recolha de informação. Para determinar o grau de confiança, é fundamental que o sistema tenha a capacidade de recolher informação acerca do histórico comportamental dos vários utilizadores. A recolha de informação pode ser efectuada individualmente por cada par ou através dos vários pares, com base no seu conjunto de experiências. A segunda componente é o *scoring* e *ranking* da reputação. Tendo a informação do histórico de transacções sido recolhida, procede-se ao cálculo de um determinado *score* para a reputação do par pretendido. Isto pode ser feito por um par, por uma entidade centralizada ou eventualmente, pelo conjunto de todos os pares pertencentes ao sistema. Geralmente o valor do *score* corresponde à reputação e é obtido através de uma função geral de *score*. A terceira e última componente do sistema consiste nas acções resultantes. Além de permitir a escolha de nós cooperativos na execução de uma transacção específica, os esquemas de reputação e confiança podem ser usados para incentivar os nós a colaborarem com a rede. Por outro lado, devem punir os nós cujo funcionamento é incorrecto.

3 Trabalho Relacionado

O sistema EigenTrust atribui a cada nó um valor único e global de confiança, com base na história de *uploads* desse nó. Um nó tem em consideração os valores globais de confiança aquando da decisão de um *download* e a rede utiliza esses valores para identificar e isolar nós maliciosos. Este sistema permite que um nó da rede esteja habilitado a calcular a reputação de qualquer entidade, de um modo totalmente descentralizado. Assim, cada nó apresenta uma visão local de confiança que se traduz pelo número de transacções satisfatórias e insatisfatórias que foram estabelecidas com as demais entidades. Essa visão traduz-se no valor s_{ij} que representa a opinião do nó *i* em relação a *j*: $sij = sat(i,j) - insat(i,j)$. Estes valores locais de confiança são normalizados de forma a evitar que um agente atribua, de forma maliciosa, um valor consideravelmente baixo ou elevado a um outro agente da rede:

$$cij = \frac{\max(sij, 0)}{\sum_j \max(sij, 0)}$$

Baseando-se na ideia de confiança transitiva, os valores c_{ij} podem ser agregados. O nó *i* de forma a obter o valor de confiança de *k*, deverá interrogar todos os seus *j* nós conhecidos. Essas opiniões são pesadas pelo valor que *i* ostenta de *j*:

$$tik = \sum_j cij\ cjk$$

Considerando como exemplo uma situação em que um nó *i* pretende obter um valor de confiança para *k*, através da opinião dos seus vizinhos *m*, *n* e *p*: $tik = cim\ cmk + cin\ cnk + cip\ cpk$. Se, segundo *i*, os nós *m*, *n* e *p* são muito reputáveis, esse facto tem repercussões nos valores cim, cin e cip, sendo que as suas opiniões serão mais consideradas. Em contrapartida, a um nó que se atribua um peso pouco relevante, implicará uma menor consideração pela sua opinião.

Paralelamente, o sistema EigenTrust sugere um algoritmo centralizado para determinar valores de reputação de qualquer constituinte da rede. Considera-se que os valores c_{ij} são representados sob a forma de uma matriz C, isto é, C corresponde à matriz $[c_{ij}]$. Por outro lado, definindo $\overrightarrow{ci}$ como o vector local de confiança que contém as opiniões c_{ij} de todos os nós com quem *i* interagiu, pode-se obter o vector de confiança $\overrightarrow{ti}$. O vector $\overrightarrow{ti}$ apresenta o valor de confiança tik: $\overrightarrow{ti} = C^T \overrightarrow{ci}$. Esta equação reflecte apenas a visão de *i* e dos seus nós conhecidos. Com o intuito de incluir um número significativamente alargado de opiniões e assumindo a matriz C como aperiódica e irredutível, é possível obter o vector $\vec{t}$ do modo seguinte: $\vec{t} = (C^T)^x \overrightarrow{ci}$. Para x iterações elevadas, a potência da matriz C tende a estabilizar num determinado valor. Além disso, se cada nó *i* executar o

cálculo apresentado, $\overrightarrow{ti}$ converge para o mesmo valor em todos esses nós. Concretamente, $\overrightarrow{ti}$ corresponde ao vector próprio esquerdo da matriz C. Por outro lado, cada elemento tj do vector $\vec{t}$ quantifica o valor total de confiança atribuído ao nó *j* por parte da rede.

No seguimento das noções enunciadas, e descartando a natureza distribuída das redes P2P, surge um algoritmo centralizado, designado de Basic EigenTrust, para o cálculo dos valores globais de confiança. Assume-se que uma determinada entidade central tem conhecimento dos valores locais de confiança de toda a rede. Esse conhecimento traduz-se pela matriz C. Por outro lado, o algoritmo propõe que é possível efectuar a substituição do vector $\overrightarrow{ci}$ por um vector $\vec{e}$, que representa uma distribuição uniforme de probabilidades sobre os nós da rede, sem colocar em causa a convergência do algoritmo.

Além do EigenTrust, foram considerados outros sistemas de reputação. Todos os esquemas de reputação e confiança analisados estão caracterizados, de acordo com a recolha de informação, *score* e *ranking* da reputação e as acções resultantes, na tabela 1.

Tabela 1 – Caracterização dos sistemas de reputação e confiança.

Sistemas de Reputação	Recolha de Informação	*Score* e *Ranking* da Reputação	Acções Resultantes
EigenTrust	Os *score managers* são responsáveis por calcular a reputação de um par. Um *score manager* é localizado com base numa DHT.	O cálculo da reputação de um nó é efectuado por um conjunto de nós (*score managers)*.	O nó, de entre aqueles que apresentam reputação mais elevada, é seleccionado de forma probabilística.
XRep [8]	A recolha da informação de reputação é efectuada através das mensagens de *Poll*, ao qual os nós respondem com *PollReply*.	Além da reputação dos pares, é atribuído um valor aos objectos. Agrupa os vários votantes pelo seu endereço IP.	O nó que apresente a maior reputação é contactado afim de obter o recurso pretendido.
Credence [9]	Um cliente consulta directamente os seus pares para obter a votação acerca de um determinado objecto.	Os clientes avaliam os votos dos seus pares com o intuito de determinar a credibilidade dos mesmos. São atribuídos pesos aos votos.	Os votos determinam a autenticidade de um objecto. Um objecto é seleccionado dependendo da votação recolhida.
PeerTrust [11]	A informação de reputação é recolhida através da componente *Data Locator*.	O modelo de confiança do PeerTrust baseia-se em transacções recentes para o cálculo do nível de confiança de um par.	A selecção é feita de forma descentralizada. Cada nó decide, através do *Trust Manager*, se um determinado par é confiável.
P2PRep [12]	Tal como os outros sistemas, o P2PRep interroga os seus pares, através de esquemas de *flooding*.	Interroga os seus pares para obter a reputação de um determinado nó. Pode atribuir pesos à opinião desses pares.	Selecciona interagir com o par que tenha sido alvo de uma opinião mais favorável.
TrustGuard [13]	Recolhe informação acerca da reputação de um par, através do *Trust Evaluation Engine*.	O *Trust Evaluation Engine* reúne *feedback* através do protocolo de *overlay*. Engloba um mecanismo de provas de transacção, para se basear somente em transacções efectuadas.	O utilizador solicita a execução de uma acção e o sistema determina se a transacção deve ser efectuada ou não, de acordo com a reputação calculada.

4 Trabalho Desenvolvido

A extensão de uma relação de confiança para fora das partes para as quais foi criada é possível através do conceito de confiança transitiva. Genericamente, a confiança transitiva pode ser descrita do seguinte modo: se a entidade A confia em B, e B confia em C, então A pode obter uma opinião de C através da recomendação exercida por B. A recomendação de B em relação a C designa-se de recomendação directa.

Por outro lado, é possível que uma entidade estabeleça uma relação de confiança com uma outra entidade, igualmente baseada em recomendações, porém sistematicamente diferente. Considere-se que cada nó apresenta não só a lista de todos os agentes que conhece, mas igualmente a lista de todos aqueles que o conhecem. Neste âmbito, o nó A, ao invés de interrogar B, poderia abordar directamente C. O nó C facultaria a A, a lista de todos os nós que apresentam uma opinião de C. Por último, o nó A decidiria confiar em C de acordo com essa recomendação recebida. A essa recomendação designa-se de recomendação inversa.

Nos exemplos apresentados, a entidade A elabora a sua opinião em relação a C através de recomendações recebidas de outras entidades. Na primeira situação a recomendação é feita pelo nó B (recomendação directa), para o qual existe uma relação de confiança directa por parte de A. Em contrapartida, na segunda abordagem é o próprio nó C que indica a A os nós sobre os quais ele se deve basear de modo a formular uma opinião acerca

de C (recomendação inversa). Em ambos os casos, é o caminho A-B-C que permite a A obter uma visão de C. Primeiramente, B é o nó interrogado enquanto que no exemplo seguinte passa a ser C.

Nas situações descritas anteriormente, a origem obtém um valor de confiança com base num caminho que é determinado pelas recomendações que vão sendo recebidas da rede, quer sejam directas ou inversas. Normalmente, a utilização isolada de apenas um destes tipos de recomendação conduz a um elevado número de interrogações na rede. Esta situação é sobretudo preocupante em redes de dimensão elevada, onde no limiar se tem a necessidade de interagir com a totalidade dos nós da rede. No sentido de limitar o número de interacções na rede na obtenção de um valor de confiança, considerou-se a utilização simultânea de ambos os modos de recomendação: directa e inversa. Este modelo bidireccional, para um mesmo *hop*, permite obter um maior número de caminhos, isto é, mais informação útil para o cálculo da reputação de um nó, interrogando uma quantidade bastante menor de nós. Esta conclusão é intuitiva se for dada relevância às seguintes considerações: numa solução directa procura-se estabelecer caminhos entre os vários nós conhecidos pela origem, ou sucessivamente conhecidos de conhecidos, e determinado destino; no caso de uma solução inversa, com base nas recomendações, nós conhecedores do destino, ou sucessivamente conhecedores de conhecedores, pretendem alcançar caminhos até à origem; na solução bidireccional a origem questiona os seus nós no sentido de obter um conjunto de recomendações directas que lhe permita calcular a reputação do destino. Caso não seja possível, passa a considerar a informação no sentido inverso. Assim, seguidamente, pretende-se encontrar caminhos entre os nós conhecidos da origem e os nós conhecedores do destino. Indefinidamente, são considerados mais nós, conhecidos de conhecidos e conhecedores de conhecedores, até se obter a reputação do destino. Neste caso, deixa de haver um ponto único em alguma das extremidades dos caminhos;

O conceito de opinião que está por base às relações de confiança merece uma análise cuidada. De uma forma simplificada, a opinião consiste num valor de entre uma escala previamente definida (ex.: [0;1]). Esse valor numérico traduz a visão externa dos demais acerca de um nó alvo. Tipicamente, um valor elevado indica que o nó é digno de confiança e um valor baixo corresponde à conclusão contrária.

A visão apresentada anteriormente engloba num valor único o grau de confiança de um nó. Neste sentido, o *score* de confiança calculado para um determinado destino representa apenas o seu nível de cooperação com a rede, tanto no fornecimento de serviços e recursos, como nas recomendações que estabelece acerca de outros nós. Contudo, se um nó é correcto a prestar serviços, não é dado adquirido que também o seja a recomendar bons prestadores de serviço. Neste sentido, considera-se relevante definir uma separação da noção de confiança em termos de confiança na recomendação e confiança na prestação de serviços ou recursos.

A delimitação da confiança é a forma encontrada no sentido de punir os nós cujo comportamento é prejudicial para a rede. Sem esta diversificação, nós que facultassem recomendações desonestas ou forjadas não seriam alvo de qualquer retaliação. É por este motivo, que a confiança diversificada é importante, especialmente em modelos que façam uso de recomendações inversas. Numa outra perspectiva, este tipo de confiança permite ainda introduzir uma visão mais realista do comportamento que as várias entidades que integram um sistema distribuído podem apresentar.

O trabalho desenvolvido apresenta-se organizado em 3 fases distintas: modelo bidireccional, confiança diversificada e algoritmos de lista de recomendação.

4.1 Modelo Bidireccional

O trabalho desenvolvido assenta na existência de uma rede composta por um conjunto de nós, aos quais está associado um identificador único. Para esse efeito é necessária a execução de um protocolo designado de IdleProtocol. Cada nó conserva uma lista de recomendação directa e uma lista de recomendação inversa. A lista de recomendação directa de um nó x apresenta os identificadores únicos dos nós conhecidos por x e o respectivo valor de confiança que lhes está associado. Em contrapartida, a lista de recomendação inversa indica os identificadores únicos de todos os nós que conhecem x bem como os valores de confiança atribuídos pelos mesmos a x.

De seguida, considera-se a existência de uma entidade, central e externa à rede, que recolhe todos os valores locais de confiança (listas de recomendação directa dos diversos nós) e executa o algoritmo Basic EigenTrust. Este algoritmo possibilita que a entidade central tome conhecimento do valor global de confiança que cada nó da rede apresenta. De forma equivalente, para obter localmente o valor global de confiança de um determinado nó alvo, cada nó deverá executar o protocolo a que se designa de TransitiveTrust. A implementação deste protocolo contempla três soluções distintas, todas baseadas na noção de confiança transitiva. Numa primeira fase foram desenvolvidas soluções que apenas recorrem a recomendações no sentido directo. Posteriormente,

passou a considerar-se soluções que calculam a reputação do destino utilizando recomendações inversas dos vários nós da rede. Ambas as soluções apresentadas requisitam um elevado número de nós de modo a obter um valor de reputação. Procedendo à união de soluções directas e inversas num único modelo, a quantidade de nós interrogados diminui substancialmente.

A natureza distribuída de um sistema P2P deve evitar a utilização de entidades centralizadas. Nesse sentido, a rede serve-se da entidade central para ganhar autonomia. Numa primeira fase calcula-se o valor global de confiança com base na entidade central como termo de comparação para detectar a convergência das várias soluções. Paralelamente, esta entidade funciona como mecanismo de validação, ao permitir registar o número de caminhos e de nós interrogados até se alcançar a tal convergência. É este registo que legítima o modelo bidireccional como a solução óptima de entre as soluções desenvolvidas.

Finda a operação centralizada, procede-se a um treino que permite descartar a presença da entidade central no exercício do cálculo. Por esse motivo, é de considerar a seguinte divisão: algoritmos de recomendação com entidade central e algoritmos de recomendação sem entidade central;

4.2 Confiança Diversificada

No caso de confiança diversificada, o valor de confiança único é substituído por um valor de confiança associado à recomendação e um valor de confiança associado ao serviço.

Revela-se importante referir que os valores de confiança são normalizados (a soma de todos esses valores, no caso do sentido directo da lista de recomendação de um nó, é igual a 1). Cada um desses valores é a visão local que determinado nó apresenta em relação aos demais. Intuitivamente, aos olhos desse nó, um valor mediano de confiança corresponde a:

$$valor\ mediano\ de\ confiança = \frac{1}{\#\ \text{total de nós conhecidos por parte do nó}}$$

Tipicamente, um nó i atribui a um conhecido j um valor superior ao valor mediano se este for digno de confiança. Por outro lado, se ao j for atribuído um valor inferior ao valor mediano é um indício de que este não merece confiança. São as diferentes combinações de atribuição de valores que traduzem o modo como determinado nó coopera com a rede.

A confiança diversificada enfatiza o comportamento heterogéneo dos vários pares constituintes da rede. Foram estabelecidos quatro tipos de nós: A, B, C e D; sendo que apenas o nó tipo A é de natureza cooperativa. Um nó do tipo A é hábil a exercer recomendações e a prestar serviços, contrastando com os nós do tipo D que são inábeis em ambas as situações. Por outro lado, um nó do tipo B recomenda mal mas presta bons serviços. Por fim, um nó do tipo C é óptimo a recomendar, mas não presta serviços de uma forma correcta. Assim, um nó do tipo A ou do tipo C mantém nas suas listas de recomendação de confiança diversificada valores correctos. Em contrapartida, um nó do tipo B ou do tipo D, ao ser mal intencionado nas suas recomendações, indica valores incorrectos de forma a sacrificar o funcionamento da rede. Os valores atribuídos por parte dos vários nós da rede são apresentados na tabela 2.

Tabela 2 – Tipos de nós: atribuição de valores.

	Valor atribuído à habilidade de recomendar				Valor atribuído à habilidade de fazer serviços			
	A	**B**	**C**	**D**	**A**	**B**	**C**	**D**
A	+	-	+	-	+	+	-	-
B	-	+	-	+	-	+	+	+
C	+	-	+	-	+	+	-	-
D	-	+	-	+	-	-	+	+

\+ valor superior ao valor mediano de confiança.
\- valor inferior ao valor mediano de confiança.

O valor concreto da atribuição feita a um nó reflecte a importância real desse mesmo nó. Isto é, se por exemplo em termos de confiança na prestação de serviços, o nó i indicar que j apresenta um valor pouco inferior ao valor mediano e se i indicar ainda que um outro nó k ostenta um valor muito inferior ao valor mediano, então conclui-se naturalmente que segundo i, o nó k é pior a prestar serviços do que j. Esta evidência serve de suporte ao conceito de valor de punição. Neste contexto, definem-se níveis de punição de acordo com a grandeza concreta dos valores atribuídos. Uma punição severa consiste em conceder valores significativamente baixos, enquanto que uma punição fraca representa a atribuição de valores não muito

inferiores ao valor mediano. De um modo complementar, e fruto da normalização das listas, os nós que não são alvo de punição vêem o seu valor de confiança aumentado.

A utilização dos conceitos de confiança diversificada é materializada através do desenvolvimento de um protocolo ao qual se designa de TrustDiversity, contemplando as três soluções de recomendação previstas neste artigo. Para a execução efectiva deste protocolo, cada nó interessado em obter a reputação do destino indica o número de caminhos que deverá estabelecer entre si e o tal nó alvo. Um caminho representa uma opinião em relação ao destino. Logicamente, um maior número de caminhos corresponde a um maior conjunto de opiniões. O nó de origem agrega as opiniões recebidas, sendo que estas são pesadas de acordo com a habilidade de recomendar dos nós que devolvem tal *feedback*. No sentido de exemplificar esta situação, considere-se uma derivação do exemplo apresentado no ponto 3. Um nó i pretende obter um valor de confiança para o serviço prestado por k, através da opinião dos seus vizinhos m, n e p: $confiança\ de\ i\ no\ serviço\ de\ k = cim\ cmk + cin\ cnk + cip\ cpk$. Os valores cmk, cnk e cpk representam a confiança que os nós m, n e p apresentam na habilidade para prestar serviços por parte de k. As recomendações dos vizinhos de i são influenciadas pela própria confiança que i deposita na capacidade que estes têm em contribuir com *feedback* (cim, cin e cip).

Após a execução do protocolo TrustDiversity, dependendo do número de caminhos definidos, o nó agrega um conjunto de opiniões, favoráveis ou desfavoráveis, em relação ao destino que pretende avaliar em termos de reputação. É nesta fase que é necessário tomar a decisão de confiar ou não confiar no serviço prestado pelo nó de destino. Para esse efeito, considera-se um bloco designado de Decision Factory. Tendo como ponto de partida as recomendações recolhidas pelo nó, esta entidade toma uma decisão de acordo com os critérios seguintes: se o número de opiniões favoráveis é superior ao número de opiniões desfavoráveis, o nó a avaliar é assumido como confiável; se pelo contrário, a maioria das opiniões indica uma baixa reputação para o destino, não se lhe deve depositar confiança; no caso do número de opiniões favoráveis ser igual ao número de opiniões desfavoráveis, deve avaliar-se o quão forte são as opiniões negativas e as opiniões positivas e optar-se por quem exerce mais influência. No sentido de determinar se a decisão tomada é efectivamente correcta, contemplou-se a existência de uma entidade de validação. Após a decisão resultante do bloco Decision Factory, tal entidade tem por objectivo averiguar se o nó de origem verá as suas expectativas defraudadas de acordo com a natureza do nó de destino.

4.3 Algoritmos de Lista de Recomendação

As noções apresentadas ao longo deste artigo culminam na concepção de um conjunto de algoritmos cujo intuito é alcançar os objectivos propostos. Na sua totalidade, foram desenvolvidos nove algoritmos, três para cada um dos tipos de recomendação: directa, inversa e bidireccional; Os algoritmos de recomendação encontram-se divididos em três secções: algoritmos centralizados de confiança única, descentralizados de confiança única e de confiança diversificada. Os algoritmos centralizados têm como condição de paragem a convergência com uma entidade central. Foram implementados três algoritmos distintos: i) algoritmo de recomendação directa de confiança única com entidade central; ii) algoritmo de recomendação inversa de confiança única com entidade central; iii) algoritmo de recomendação bidireccional de confiança única com entidade central;

Tendo como ponto de partida o registo do número de caminhos e do número de nós interrogados, provenientes da execução dos algoritmos de lista de recomendação com entidade central, é possível proceder à implementação de soluções descentralizadas para cada um dos tipos de recomendação. Para esta fase, os algoritmos centralizados foram modificados de forma a permitir um modo de operação independente da entidade central. Assim, os algoritmos de lista de recomendação sem entidade central devem ser alvo de um treino prévio resultante das soluções centralizadas. Um nó, sendo conhecedor do número de caminhos ou de nós que deverá interrogar, à medida que agrega recomendações da rede, consegue determinar, através dos algoritmos descentralizados, se a informação que dispõe é suficiente para fazer uma avaliação correcta do destino pretendido. As três soluções algorítmicas desenvolvidas para esta fase foram: i) algoritmo de recomendação directa de confiança única sem entidade central; ii) algoritmo de recomendação inversa de confiança única sem entidade central; iii) algoritmo de recomendação bidireccional de confiança única sem entidade central;

Em último lugar, os algoritmos de lista de recomendação passam a considerar a noção de confiança diversificada. O número de caminhos até ao destino é a condição de paragem dos algoritmos. Posto isto, decide-se se o destino é de confiança ou não. Desenvolveu-se um novo algoritmo para cada um dos tipos de recomendação previstos neste artigo: i) algoritmo de recomendação directa de confiança diversificada;

ii) algoritmo de recomendação inversa de confiança diversificada; iii) algoritmo de recomendação bidireccional de confiança diversificada;

5 Resultados Experimentais

Neste capítulo pretende-se apresentar os resultados provenientes da execução dos vários algoritmos desenvolvidos. Numa primeira fase demonstra-se os benefícios inerentes à utilização de soluções bidireccionais na obtenção do valor global de confiança. Seguidamente, são analisados diferentes cenários envolvendo os algoritmos de confiança diversificada.

A implementação deste trabalho foi concretizada através do recurso ao simulador PeerSim [19], tendo o Eclipse IDE como ambiente de desenvolvimento. A linguagem de programação utilizada foi o Java (versão 1.5), refém da escolha do simulador. A rede utilizada nos resultados é não estruturada e definiu-se que cada par pode apresentar um de três graus de ligação: fracamente ligado, normalmente ligado ou fortemente ligado. O conceito de grau de ligação serve de mote à ideia de densidade da rede. Esta noção traduz numericamente o número de ligações existentes na rede por tamanho total de rede (ligações/rede).

5.1 Modelo Bidireccional

5.1.1 Procedimento Experimental

Estabeleceu-se como requisito que os nós de diferentes graus de ligação deveriam coabitar numa mesma rede interligada. Nesse sentido, considerou-se uma rede de 100 nós onde se assume a existência de pelo menos um nó pertencente a cada um dos graus definidos. Com o intuito de efectuar simulações para diferentes densidades de rede, fez-se variar o número de ligações existentes de forma a alcançar densidades no intervalo de [10;100[ligações/rede. Este intervalo reflecte uma densidade mínima de 10 ligações/rede e uma densidade máxima de 99 ligações/rede (caso em que todos os nós da rede conhecem todos os outros). Considerou-se ainda um incremento de densidade correspondente a 10 ligações/rede entre cada simulação efectuada (exceptuando o incremento para a densidade máxima).

Para as várias densidades de rede, foram executados 10 ciclos de simulação sendo que em cada ciclo o valor global de confiança é obtido através das soluções algorítmicas de confiança única previstas neste trabalho. Por fim, os resultados de simulação são direccionados para um ficheiro com a finalidade de se proceder ao cálculo da sua média e à sua representação gráfica.

5.1.2 Algoritmos Centralizados e Descentralizados

Estes primeiros resultados experimentais demonstram, em termos de nós interrogados, a vantagem associada a uma solução que utilize simultaneamente recomendações bidireccionais. Numa primeira fase, foram analisados os três algoritmos centralizados de confiança única. Os resultados provenientes da sua execução são aproximados a funções no sentido de se considerar as soluções descentralizadas. Exalta-se o facto de que em ambos os casos o algoritmo Basic EigenTrust apresenta um papel primordial. Para os algoritmos centralizados, funciona como condição de paragem e para os algoritmos descentralizados permite calcular a exactidão do valor obtido pelos mesmos.

Especificamente, começa-se por registar o número de caminhos e de nós interrogados até se alcançar uma convergência com o algoritmo Basic EigenTrust. Essa convergência traduz-se pelo conceito de exactidão. Estipulou-se que cada nó apenas declara o algoritmo como finalizado, assim que obtenha um valor aproximado ao da entidade central. Para esse efeito definiram-se dois níveis que consistem numa exactidão de pelo menos: 70 % e 90 %. Tendo como ponto de partida os valores obtidos com a presença da entidade central, procede-se à sua representação em termos de funções polinomiais, através de um modelo de regressão polinomial. Assim, um nó ao saber a densidade de ligações existentes na rede, e tendo conhecimento, através da regressão polinomial, do número de caminhos a encontrar ou do número de nós que deverá interrogar, está habilitado a calcular correctamente o valor global de confiança de um qualquer nó.

Número de Caminhos O número de caminhos encontrados até se obter um valor coincidente com a entidade central depende da solução de cálculo considerada e essencialmente do *hop* no qual esse valor é obtido. Tipicamente, para um mesmo *hop*, a solução bidireccional consegue alcançar um número de caminhos significativamente superior aos que podem ser encontrados, entre a origem e o destino, em soluções puramente de recomendação inversa ou recomendação directa. No caso de uma densidade de rede elevada,

independentemente da solução algorítmica considerada, a origem tende a obter o valor global de confiança do destino com base no mesmo número de caminhos e apenas considerando o conhecimento proveniente de um único *hop*. Para densidades de rede relativamente baixas, o número de caminhos encontrados até convergência diverge. Tal como seria expectável, numa situação de mais baixa exactidão, são necessários menos caminhos para atingir um valor global de confiança coincidente com a entidade central.

Nós Interrogados Os gráficos que correspondem à aproximação por funções do número de nós interrogados até convergência com o algoritmo Basic EigenTrust estão ilustrados na figura 1.

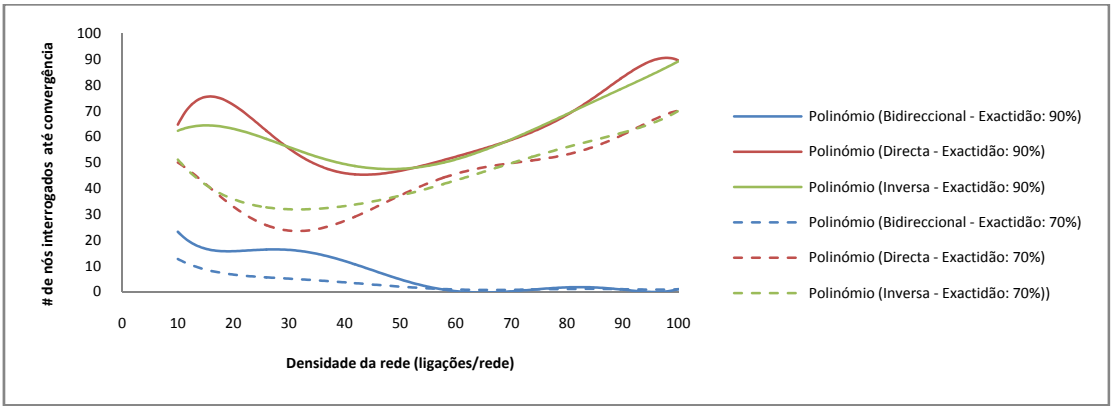

Figura 1 – Número de nós interrogados: regressão polinomial.

Os resultados obtidos para esta fase validam a solução bidireccional como a mais vantajosa para o cálculo da reputação de um determinado nó. O funcionamento dos algoritmos de recomendação directa e recomendação inversa é bastante idêntico, daí se explica a produção de resultados semelhantes. Estes algoritmos apresentam uma tendência equivalente: numa rede com poucas ligações estabelecem-se mais interrogações; numa rede de densidade elevada o número de nós interrogados tende a aumentar. No caso do algoritmo de recomendação bidireccional de confiança única, os resultados obtidos são bastante mais satisfatórios, comparativamente aos restantes algoritmos.

Para densidades de rede superiores a 50 ligações/rede, o algoritmo bidireccional apenas necessita de exercer uma única interrogação. O nó de origem, considerando a sua própria lista de recomendação directa, ao solicitar a lista de recomendação inversa a determinado destino, fica a dispor da informação necessária para proceder ao cálculo do valor global de confiança sem precisar de novas requisições. Por seu termo, os nós ao executarem os algoritmos que utilizam apenas o conhecimento em um dos sentidos, para estes níveis de densidade, apresentam um número de nós interrogados que se aproxima do seu grau de ligação.

Analogamente ao número de caminhos, independentemente da solução utilizada, quando se tolera um erro maior, o número de nós interrogados é menor. Para atingir um valor global de confiança cuja exactidão deve ser superior a 90%, o número de nós requisitados é superior.

Sintetizando, numa rede menos ligada é necessário interrogar um conjunto alargado de nós afim de se poder alcançar o valor global de confiança de determinado nó alvo, dado que apenas alguns nós conhecem o destino. Por outro lado, se o destino é conhecido por um elevado número de nós e se a origem apresenta um elevado grau de ligação, é muito provável que a generalidade dos nós interrogados pela origem consiga contribuir para a obtenção do valor de reputação do destino.

Conclusão dos Resultados do Modelo Bidireccional Os resultados evidenciam que o algoritmo bidireccional permite uma melhoria substancial em termos de interrogações efectuadas na rede. Sendo uma solução que se baseia simultaneamente em recomendações directas e inversas, permite, para densidades de rede elevadas, alcançar um valor global de confiança de elevada exactidão apenas requisitando uma única lista de recomendação. Por outro lado, considerando uma rede onde as ligações residem em menor número, a solução bidireccional consegue ainda assim obter um valor exacto, interrogando menos nós, comparativamente a modos de funcionamento simplesmente directos.

5.2 Confiança Diversificada

5.2.1 Procedimento Experimental

Começou-se por considerar uma rede de 100 nós de densidade igual a 50 ligações/rede. De seguida, tendo por base os diferentes tipos de nós definidos, fez-se variar o número de pares hábeis a fazer recomendações correctas na rede. Inicialmente, a rede exibe um conjunto de 10 nós dignos de estabelecer boas recomendações e gradualmente acresce-se esse valor em 10 unidades, até se atingir uma configuração de rede onde 90 nós recomendam bem e os restantes mal. Estabeleceu-se ainda que para cada uma dessas configurações, o nó que requisita o valor de confiança deve tomar essa decisão de acordo com um número de caminhos predefinidos. Inicialmente, um par julga o destino como confiável ou não confiável, tendo apenas por base uma única opinião recebida dos seus conhecidos. O número de opiniões que o nó deve receber até uma decisão acresce de uma unidade, em cada simulação, até um máximo de 10 opiniões. Cada uma dessas simulações compreende 20 ciclos. Em cada ciclo de simulação o nó que requisita a confiança de um destino é sempre de natureza cooperativa (nó do tipo A). Como destino são considerados 5 nós de cada tipo. Assim, findo os 20 ciclos de simulação sabe-se que 5 nós do tipo A, 5 nós do tipo B, 5 nós do tipo C e 5 nós do tipo D foram julgados em termos de confiança por parte de nós do tipo A.

Se por um lado se faz variar o número de nós hábeis a recomendar, por outro, a rede mantém constante a quantidade de nós que prestam serviços de forma honesta e desonesta (50 nós bons a prestar serviços).

Partindo da execução dos três algoritmos de confiança diversificada desenvolvidos, procedeu-se à análise de um conjunto de resultados provenientes de diferentes cenários experimentais. Os valores contidos nas listas de recomendação dos vários nós (de acordo com a tabela 2) da rede reflectem dois níveis de punição[1]: punição fraca (valor de punição corresponde a metade do valor mediano de confiança) e punição forte (valor de punição corresponde a um décimo do valor mediano de confiança)

Além dos resultados obtidos para cada uma das punições referidas, foram introduzidos os cenários: utilização de um threshold (apenas são consideradas as recomendações de nós que apresentem valores de confiança superiores ao valor mediano) e listas de recomendação inversa forjadas (os nós maus prestadores de serviço devolvem recomendações incompletas e maquinadas como tentativa de enganar o nó que solicita um serviço). O ponto fulcral destes cenários consiste em expor o nó de origem a um conjunto de situações e determinar se ainda assim este consegue decidir correctamente em termos de confiança no serviço prestado por determinado destino. Uma decisão incorrecta consiste em não confiar num bom prestador de serviços ou confiar num mau prestador de serviços. Em contrapartida, uma decisão correcta resume-se a confiar num bom prestador de serviços ou não confiar num mau prestador de serviços.

Punição Fraca Na figura seguinte apresentam-se os cenários de punição fraca e de punição fraca com utilização de um valor de limiar.

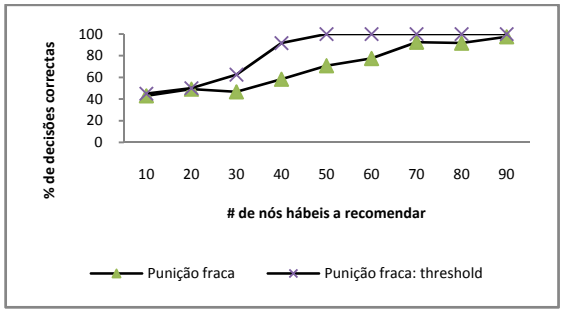

Figura 2 – Punição fraca.

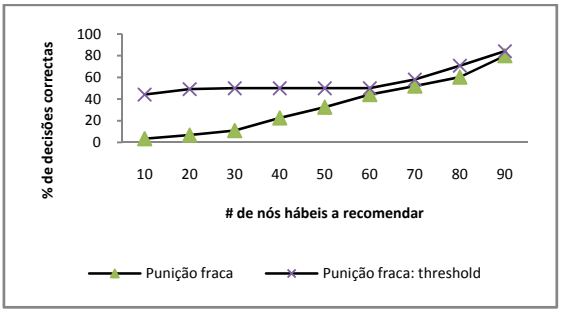

Figura 3 – Punição fraca: lista forjada.

O gráfico da figura 2 demonstra que a percentagem de decisões correctas, para ambos os cenários apresentados, é aceitável. Nomeadamente, sem a utilização de *threshold*, quando o número de nós hábeis a recomendar é superior a 40 a percentagem de decisões correctas supera os 50%.

Com a utilização de *threshold*, esta percentagem é alcançada mesmo para quando o número de nós que estabelecem recomendações correctas é igual a 20.

Tal como se referiu anteriormente, o número de entidades que prestam serviços correcta ou incorrectamente mantém-se constante. Neste sentido, caso o nó de origem, ao invés de tomar uma decisão com base em recomendações da rede, optasse por avaliar o destino de um modo completamente aleatório (decidindo à sorte),

seria expectável que a percentagem de decisões correctas fosse aproximadamente 50, independentemente do número de nós hábeis a recomendar. Por este motivo, um resultado favorável deve superar a percentagem de 50 decisões correctas.

Considerando a situação em que o destino devolve uma lista de recomendação inversa maquinada, o nó de origem tende a tomar um maior número de decisões incorrectas (figura 3).

Punição Forte No presente subcapítulo há um agravamento do valor de punição. Neste sentido, um funcionamento malicioso é penalizado de uma forma mais acentuada. A figura 4 apresenta os resultados dos cenários de punição forte, com e sem utilização de um valor de *threshold*. Os resultados apresentados sugerem uma melhoria em relação ao cenário equivalente de punição fraca. No caso em que o destino devolve uma lista de recomendação inversa forjada, para a situação de punição forte (figura 5), os resultados indicam que não há uma degradação em termos de decisões correctas. O destino ao indicar apenas os valores mais elevados está automaticamente a revelar o conjunto de nós mal intencionados que actuam com o intuito de melhorar a reputação desse destino.

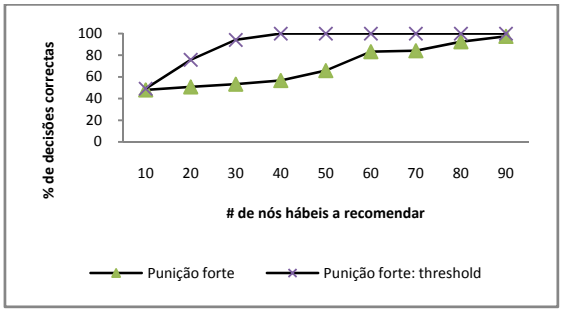

Figura 4 – Punição forte.

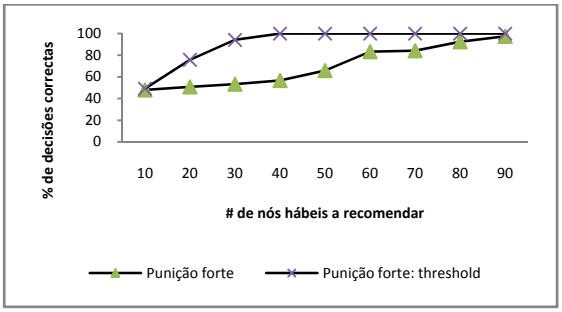

Figura 5 – Punição forte: lista forjada.

Assim, a origem ao receber a lista de recomendação inversa forjada do destino, pesa as opiniões contidas nessa lista de acordo com o respectivo valor de punição. Sendo este valor bastante penalizador, o nó de origem não será induzido em erro e o destino é incapaz de ver o seu valor de reputação aumentado.

Conclusão dos Resultados de Confiança Diversificada Independentemente do cenário considerado, os resultados de confiança diversificada sugerem uma tendência evidente: à medida que o número de nós habilitados a exercer boas recomendações aumenta, a percentagem de decisões correctas é igualmente maior.

Outra conclusão clara prende-se com a utilização de um *threshold*. Um nó que interrogue apenas os seus conhecidos acima de um limiar (ex.: valor mediano de confiança) alcançará uma percentagem de decisões correctas superior ao que conseguiria se interrogasse todos os nós sem critério.

Por último, é de destacar que a omissão de valores na lista de recomendação inversa do destino é bastante prejudicial para o funcionamento da rede. A utilização de um valor de punição elevado permite resolver o efeito danoso causado por estas listas.

6 Conclusão

O primeiro objectivo deste trabalho foi a concepção de um modelo, baseado em relações de confiança transitivas, que funcionasse num qualquer sistema distribuído, independentemente do seu tipo de arquitectura ou organização. Além destes requisitos, tal modelo deveria ser capaz de alcançar um valor de reputação sem implicar um elevado conjunto de interacções. No sentido de concretizar esta ideologia, começou-se por considerar um tipo de recomendação inovador, ao qual se designou de recomendação inversa. Partindo do desenvolvimento de algoritmos de recomendação directa e de recomendação inversa, foi implementado um modelo bidireccional que utiliza ambos os tipos de recomendação previstos neste artigo. Nos resultados obtidos, estão patentes os benefícios desta solução, concretamente no que respeita ao número de nós que se devem interrogar até à obtenção de um valor global de confiança credível.

Tendo conhecimento dos diferentes níveis de colaboração que um agente da rede pode apresentar, considerou-se a necessidade de estabelecer um mecanismo que evitasse a degradação do funcionamento das soluções desenvolvidas, nomeadamente das que fazem uso de listas de recomendação inversa. Assim, foi

estipulado um segundo objectivo no sentido de alcançar um mecanismo que funcionasse como incentivo ao funcionamento cooperativo e penalizasse os nós de índole maliciosa. Sem esta ideologia, estes nós não se sentiriam motivados a fornecer um *feedback* honesto, dado que a omissão de alguma da informação de recomendação poderia fazer elevar o seu valor de reputação. No sentido de encontrar uma protecção contra este tipo de comportamentos, idealizou-se uma noção de confiança bipartida, onde passam a ser considerados os valores de: confiança na recomendação e confiança no fornecimento de recursos ou serviços; Este mecanismo permite pesar as opiniões que vão sendo recebidas com o valor de confiança na recomendação que está associado ao nó que faculta essas mesmas opiniões. Por este motivo, um nó que seja reconhecido pelo seu mau funcionamento será associado a valores de confiança baixos.

Os resultados experimentais apresentados para esta fase demonstram que em certas situações, a utilização de valores de confiança bastante penalizadores pode conduzir a que a rede se mostre praticamente indiferente ao funcionamento malicioso de alguns dos seus constituintes.

Além de combater algumas das técnicas que visam comprometer o funcionamento das redes P2P, a confiança diversificada permite representar de um modo mais realista o comportamento dinâmico que os vários nós de uma rede apresentam.

Referências

[1] S. Kamvar, M. Schlosser and H. Garcia-Molina (2003), "The EigenTrust Algorithm for Reputation Management in P2P Networks", Budapest, Hungary, ACM Press.

[2] C.Yu (2005), "Reputation Propagation between Decentralized P2P Environments", Helsinki, Finland, Seminar on Internetworking.

[3] T. Grandison and M. Sloman (2001), "A Survey of Trust in Internet Applications", IEEE Communications Surveys and Tutorials, London, UK.

[4] S. Marti and H. Molina (2005), "Taxonomy of trust: Categorizing P2P reputation systems", Science Direct, Stanford, California, USA.

[5] K. Lai, M. Feldman, I. Stoica and J. Chuang (2003), "Incentives for Cooperation in Peer-to-Peer Networks", California, USA.

[6] Zhu, B., Jajodia, S. and Kankanhalli, M.S. (2006) 'Building trust in peer-to-peer systems: a review', Int. J. Security and Networks, Vol. 1, Nos. 1/2, pp.103–112.

[7] J.Douceur (2002), "The sybil attack", Microsoft Research.

[8] E. Damiani, S. Vimercati, S. Paraboschi, P. Samarati and F. Violante (2002), "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks.", Washington, USA. ACM Press.

[9] K. Walsh and E. Sirer (2006), "Experience with an Object Reputation System for Peer-to-Peer Filesharing", NY, USA.

[10] Gnutella Developer Forum (2003): The Annotated Gnutella Protocol Specification v0.4 website: http://rfc-gnutella.sourceforge.net/developer/stable/.

[11] L. Xiong and L. Liu (2004), "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities", Georgia, USA, IEEE Computer Society.

[12] F. Cornelli, E. Damiani, S. Vimercati, S. Paraboschi and P. Samarati (2002), "Choosing Reputable Servents in a P2P Network", Italy.

[13] M. Srivatsa, L. Xiong and L. Liu (2005), "TrustGuard: Countering Vulnerabilities in Reputation Management for Decentralized Overlay Networks", Chiba, Japan, ACM Press.

[14] A. Cheng and E. Friedman (2005), "Sybilproof Reputation Mechanisms", NY, USA, ACM Press.

[15] H. Zhang, A. Goel, R. Govindan, K. Mason and B. Roy (2004), "Making Eigenvector-Based Reputation Systems Robust to Collusion".

[16] B. Ooi, C. Liau and K. Tau (2003), "Managing trust in peer-to-peer systems using reputation-based techniques", Singapore.

[17] J. Han and Y. Liu (2006), "Dubious Feedback: Fair or Not?", HongKong, ACM Press.

[18] P. Dewan (2004), "Peer-to-Peer Reputations", Arizona, USA, IEEE Computer Society.

[19] PeerSim. PeerSim website: http://PeerSim.sourceforge.net/.