Computer Communications 35 (2012) 2044–2053

Contents lists available at SciVerse ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

@Trust: A trust model based on feedback-arbitration in structured P2P network

Xianfu Meng[a,*], Yalin Ding[a], Yue Gong[b]

[a] School of Computer Science and Technology, Dalian University of Technology, No. 2, Linggong Road, Dalian 116024, China
[b] Computer Science Department, Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609, USA

ARTICLE INFO

Article history:
Received 1 December 2010
Received in revised form 26 October 2011
Accepted 14 June 2012
Available online 23 June 2012

Keywords:
Peer-to-peer
Trust model
Arbitration
False feedback
Trust decision

ABSTRACT

Aiming at shortcomings in feedback information aggregation and trust decision in existing trust models, a novel trust model, named @Trust, is proposed for structured P2P networks. @Trust calculates the node's credibility of service, feedback and arbitration based on the evaluations of the specific service which were arbitrated according to the rule of majority in human society, to enhance the model against the malicious peers. @Trust also involves the applying of the credibility of specific services and the punishment mechanism to improve the trust decision and to resist the repeated attacks of the malicious peers. The simulation results show that @Trust has advantages in distinguishing out the false feedback and resisting the malicious peers, and thus improves the availability of P2P networks.

1. Introduction

P2P applications, represented by file sharing systems, such as eMule [1], Kazaa [2] and Gnutella [3] have been widely used in recent years. With the further growth of the Internet, the problem of P2P network security is attracting more attention. P2P networks to some degree facilitate spreading computer viruses, inauthentic files and false information because of their natures of open, anonymity and autonomy. The prevalence of VBS.Gnutella worm [4] is a typical example. The research in [5] has shown that when malicious peers propagate a large number of poisoned files, the consequence is indispensable. Network bandwidth and storage space are being wasted, thus resulting in obstacles to the normal operation of networks. Moreover, it has negative impacts on network user's experiences, so that users might lose their patience or even interests in using networks. In order to solve this problem, inspired by the features of the social network in real life, researchers introduced a variety of reputation-based trust models in P2P networks for protecting networks' normal operation. Empirically, trust models have been shown to have positive effects on enhancing P2P network security; especially when dealing with malicious peers, the models effectively restrict those peers' potentially harmful activities.

P2P trust models are mainly constructed on a basis of the evaluation feedback, produced by the transacting partners on the outcomes of the transactions, therefore, the credibility of the evaluation feedback is important, as it has significant impacts on the models' effectiveness. An early form of a trust model usually uses a node's global trust as its feedback credibility, based on which to determine false feedback from that particular node. This approach, however, does not suffice, as it fails to provide the ability to resist the coordinated attacks from malicious peers. Aiming to address this problem, researchers proposed the strategies of feedback similarity [6,7] and feedback filtering [8,9], expecting to eliminate the impacts from false feedback on peer credibility calculation. Nevertheless, due to the network scale, the technique of feedback similarity suffers from a computational problem, vector sparseness, while feedback filtering has its own problems as well: it succeeds in filtering out false feedback, yet some of the true ones are mistakenly screened out too. In addition, this technique has a lower ability to dynamically adapt for the situation where a node changes its activities. Thus, the calculation accuracy in peer credibility is limited. In the aspect of trust decision-making, a majority of models directly use the targeted peer's credibility to determine whether cooperation should be established without taking the credibility of specific services into account. This manner appears to have its limitations, for the reason that even for a peer having relatively high credibility, it is not necessarily able to contribute reliable and high-quality services in all conditions, and vice versa. In an effort to solve the above problems, in this paper, we present a feedback arbitration-based trust model, @Trust (@ is short for Arbitration Trust). Our main work is the following:

(1) Arbitration nodes arbitrate the evaluation feedback on specific services based on the rule of majority, which helps identify false feedback.

* Corresponding author. Tel./fax: +86 411 84706008.
E-mail addresses: xfmeng@dlut.edu.cn (X. Meng), dingdang880108@163.com (Y. Ding), ygong@wpi.edu (Y. Gong).

0140-3664/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.comcom.2012.06.007

(2) Each node is assigned service credibility, feedback credibility and arbitration credibility. Three types of credibility undertake different responsibilities in terms of decision-making and punishment in transactions.

(3) Arbitration nodes maintain credibility of specific services, in favor of rapidly and effectively making trust decisions for other nodes.

2. Related work

In the traditional networks, the trustable third parties are usually used for establishing trust relations between nodes, such as certificate authority (CA), however this centralized trust mechanism is not suitable for P2P networks [10]. Since 2001, when Aberer and Despotovic [11] firstly focused on trust management in P2P environments, targeting to the solutions of how to more appropriately and accurately describe peer credibility, many researchers, from different perspectives, have been presenting varieties of trust management models for different applications [6–17] in P2P networks, such as P2Prep [14], a reputation based model working for P2P file sharing applications, XRep [15], which considers resource reliability, the eigenvector-based model: EigenTrust [17], and the model based on social-cognitive theory [18], etc.

In P2P trust models, evaluation feedback is the key to calculate peer credibility, thus the authenticity of the feedback is fundamental to the effectiveness of a trust model [16]. However, in the early research, feedback mechanism-based trust models barely consider the actions of false feedback, which significantly affects the authenticity of node credibility [19]. In order to identify false feedback, Yu et al. introduced the concept of feedback credibility [20], yet no concrete mechanisms of how to evaluate the credibility of the feedback provider were presented. EigenTrust [17] and work in [10] proposed global reputation-based models where each node is assigned a global trust, used as that node's feedback credibility. Specifically, the models assume that the nodes with higher global trusts should also be capable to produce more credible feedback, but this assumption does not always hold, as it could be possible that a malicious node performs coordinated attacks [16], i.e. a malicious node could first improve its service credibility by providing high quality services, and then propagate false feedback, so as to take the advantage of high service credibility to subvert the reputation system. To prevent coordinated attacks, in recent work, researchers proposed the strategies of feedback similarity and feedback filtering. PeerTrust [6] and RBTrust [7] use personalized similarity measures to more heavily weigh feedback of peers who have provided similar evaluations for a common set of past partners. The basic idea is that between a node *i* and a node *j*, the higher the similarity, in terms of evaluating the peers in their common set, is, the more consistent their evaluations for the other peers in the network are. The approach uses a cosine function to calculate the similarity, Cr_{ij}, which works as the weight of the feedback from node *j*. When calculating a target node's global trust, node *i* weighs node *j*'s feedback on that target node by Cr_{ij}. This approach is somewhat successful in effectively preventing the coordinated cheats from malicious peers, but fails to accurately evaluate feedback in large scale networks, as there are few common transaction nodes in such networks. As proposed in [8] and the RunTrust model in [9], feedback filtering strategy is used to screen out potentially abnormal feedback. The filtering strategy in [8] works in the following manner. It first converts the feedback R_i into a binary variable O_i, and then normalizes O_i using the function of $O_i = \frac{O_i - \mu}{\sigma}$. If $O_i > t$ (where *t* is a pre-set threshold of deviation-tolerance), R_i would be filtered out. After this procedure, as the last step, all the remaining R_is are used for calculating the credibility of the target node. This strategy works well in the circumstance where well-meant peers are the majority in a network. However, it suffers from two problems. One is the lack of ability to dynamically adapt to the changes of malicious peers. The other is the possibility of losing true feedback. Both strategies of feedback similarity and feedback filtering map the feedback on a specific service to the feedback on that service's provider. In the mapping, the authenticity of the feedback is overlooked until the instant of calculating the peer credibility, at that time the feedback on the target peer is eventually examined. The way of using a peer as a unit to identify false feedback has an obvious drawback. Concretely speaking, in a network, a peer usually provides multiple services and a feedback peer evaluates a specific services based on that service's quality. However, when identifying false feedback to a target peer, the existing approaches just simply consider the feedbacks from other peers on all services provided by that target peer, but exclude inspecting the consistency of the feedbacks on each specific service. In consequence, the identification granularity is too coarse to detect false feedback, resulting in lower calculation accuracy of peer credibility.

In the aspect of trust decision-making, in most models [6–10] a peer decides to establish a transaction with a target peer just based on that peer's credibility, but not the credibility of the specific service the transaction involves. Note that the credibility of a peer is not always equated with the credibility of the service provided by that peer, as it is not guaranteed that a node with higher credibility can always provide reliable services, and vice versa. The ability to provide reliable services is background-sensitive (related to the peer's professional abilities or knowledge) [12]. For example, suppose peer *i* is an expert of computer science, but knows little about medicine. When peers who are good at medicine interact with peer *i*, they will probably not satisfy with peer *i*, leading to a decrease in peer *i*'s credibility. In this case, other peers, even if the transaction purposes are about computer science, might refuse to establish transactions with peer *i*, as its overall credibility has been decreased. Therefore, it is not reasonable to use peer credibility as the specific service credibility. Towards this problem, Damiani et al. presented XRep trust model [15]. The model first uses polling protocol to obtain the reputations of peers and resources, and then based upon both assists users to make decisions. This model, however, employs broadcast mechanism to propagate reputation queries, which has the drawbacks of high network cost, low system scalability and lack of considerations for false feedback.

3. Related definitions and modeling

3.1. Related definitions

For easy understanding, we first demonstrate several concepts used in the following sections.

Definition 1. Specific service (*SS*) and specific service credibility (*SSC*). *SS* indicates a specific service provided by a peer, while *SSC* is the credibility of such service.

Definition 2. Service peer (*SP*) and service credibility (*SC*). *SP* is a peer that provides a service in a transaction, while *SC* implies the overall credibility of all specific services provided by the peer, which is represented by a function of quantities and qualities of those specific services.

Definition 3. Feedback peer (*FP*) and feedback credibility (*FC*). *FP* stands for a peer that requests and receives a service in a transaction. This kind of peer evaluates and gives feedback on the received services, so is called feedback peers. *FC*, the credibility of an evaluation, is a function of the qualities of the evaluations that a peer gives, as well as the amount of services that peer received.