Peer-to-Peer 环境下的信任模型研究*)

张 旭 孟 魁 肖晓春 张根度
(复旦大学计算机与信息技术系 上海 200433)

摘 要 开放、共享、匿名的 peer-to-peer 网络已经取得了越来越多的应用,无中心对等的特性也吸引了越来越多的用户,但同时也成为了网络攻击者传播恶意内容或病毒的温床。由于其网络中的节点不受约束,节点间存在着自愿的交易行为,因此节点之间的信任很难通过传统网络的机制来制约和建立。本文旨在通过借鉴人类社会网络中的信任关系来建立一种信任模型,通过定义一系列信任的因子,用以制约用户行为,同时为用户寻求服务前提供参考。最后通过和其他信任模型的对比,我们的模型能够有效地激励用户提供反馈,遏制节点的不诚实行为。

关键词 信任系统,Peer-to-Peer 网络

A Reputation-based System Model in Peer-to-Peer Networks

ZHANG Xu MENG Kui XIAO Xiao-Chun ZHANG Geng-Du
(Department of Computer and Information Technology, Fudan University, Shanghai 200433)

Abstract The open and anonymous nature of a Peer-to-Peer network makes an ideal medium for many applications. However the feathers that contribute the success also make it possible to be attacked and abused. The peers are not willing to be responsible for their historical behavior because of lack of supervisor; and it's not easy to set up a trust mechanism in a traditional way to solve the problem during the transaction. In this paper, following the analyses of the trust in social network, we set up a trust model and introduce some feathers to implement the trust in Peer-to-Peer networks. Later, compared with some existing models, we will find that our approach can stimulate the feedback and decrease the dishonest behaviors efficiently.

Keywords Trust system, Peer-to-Peer networks

1 引言

对等网络(Peer-to-Peer)被美国《财富》杂志称为改变因特网发展的四大新技术之一,甚至被认为是无线宽带互联网的未来技术。基于 P2P 的网络应用为个人用户提供了前所未有的便利,同时也有效地整合了网络的潜在资源,使互联网成为了自由交换信息的媒介,大大便利了用户对信息的获取。虽然 P2P 网络目前面临着很多的社会、法律和技术等问题的困扰,但仍不妨碍其成为互联网的主流应用之一。但是正像 P2P 网络所宣扬的平等共享精神一样,在这类系统中往往没有制约,资源的共享是用户的自愿行为,用户不用承担法律道义上的责任,因此节点之间信任关系往往很难从传统的网络中借鉴。我们可以从人类社会中的人际关系的信任中得到启发,来建立一套信任机制,对 Peer-to-Peer 环境中的种种问题加以探讨解决。

在 P2P 网络中,由于用户都是匿名的,因此像目前流行的 Emule 一样的文件共享应用,用户在交易之前,一般对服务提供者毫无所知。如果服务提供者提供了损坏的文件,则浪费了下载者的时间,如果提供的是恶意的病毒,则后果更不堪设想。这样,我们就需要在 P2P 网络中建立一套信任机制,来约束节点行为,为节点交易或者服务前提供一定的信用信息,让节点自己决定是否担当风险来获取服务。

对于一系列网络社区中的信任管理问题,如 eBay, Amazon, Yahoo! Auction 等,从我们的经验和一些调查得出了一系列现有 P2P 电子社区中的问题和风险[1]。

* 很多现有的电子信任系统中缺少有效的机制来甄别善意节点和恶意节点,所以用户很容易得到不可靠或虚假的服务,严重的可能感染病毒。

* 现有的很多电子信任系统不能提供有效的激励,使用户在交易完成后提供反馈。如果没有足够的反馈信息,这样的信任系统就失去了意义。

* 大部分的电子信任系统对有策略的恶意破坏束手无策,例如某些节点可以通过一定时间来积累信任度,然后利用自己的高信任度来欺骗用户。

* 还有存在的问题就是 P2P 网络中信任信息的传输过程,如何能够有效地保证其不被修改,不被损坏。

本文借鉴社会网络中的人际关系模型,建立了分布式环境中的信任度模型,对影响节点信任度的几个向量进行了定义与说明,最后通过一系列协议来解决信任度的向量之间的综合与更新。

2 模型概述

2.1 模型的定义和表示

类似于在现实社会的人际关系网络,在虚拟的 P2P 网络环境中,节点交易之前对服务节点信任的判断一方面来自于自己以往的交易经验,另一方面来自于网络中其他节点的推荐。于是在我们模型的信任定义中,同时考虑到了本地信任 TL(Local Trust)和外部推荐 TR(Recommend Trust),所以一个节点的信任定义如下:

定义 1 称节点每次交易后的评价为 *Eval*(Evaluation),

*)Supported by thge National Natural Science Foundation of China under Grant No. 60373021(国家自然科学基金)。**张 旭** 硕士研究生,主要研究领域为网络安全、网络信任体系。

其中 $Eval$ 的取值为 $Eval\in[0,1]$之间的离散值，评价的结果越靠近 1，则说明节点得到了比较满意的服务，否则相反。

定义 2 本地信任值 TL 为节点存储在本地的历史交易信息，$TL_{ij}=\sum_{t} f(t_{ij})*Eval_{ij}$，其中 TL_{ij} 为节点 i 对节点 j 的本地信任值，t_{ij} 为节点 i 与节点 j 的交易时间，$f(t_{ij})$为时间依赖函数，可以保证近期的交易获得较大的权值，历史的交易对本地信任值的影响较小。时间依赖函数的定义为 $f(t_{ij})=\frac{t_{ij}-t_o}{\sum_{i,j}(t_{ij}-t_o)}$，其中 t_o 为节点加入网络的时刻，$\sum_{i,j}(t_{ij}-t_o)$为所有交易的时间求和。

时间依赖函数的设定是为了赋予近期交易的信任评价较大的权值，因为相对于历史的信任值来说，我们更加关注节点的近期行为，近期行为可以体现节点在最近一段时间内的信用记录，帮助我们进行更准确的判断。而且时间依赖函数的加入也体现了信任信用的建立较难，破坏容易的特性（Easy-destruction-hard-construction）[10]。

定义 3 反馈信息的范围参数 N_j。我们知道，在社会关系中，当从越多人哪里获知的东西往往越可靠，所以判断网络中节点的信任值的时候，反馈节点的数量 s(Scope)也是一个需要考虑的因素，得到的反馈节点数量越多，我们认为得到的信息越可靠。

$$N_j=\begin{cases}\sin\left(\frac{\pi}{2*itm}*s\right) & s\in[o,itm]\\ 1 & \text{else}\end{cases}$$

这里，我们可以根据网络规模指定阈值 itm，如果得到提供反馈的节点数量大于阈值时，N_j 取 1，说明此时我们对于得到的反馈数量已经达到了能够相信的程度；否则说明得到的反馈数量比较少，可信度不高。

定义 4 外部推荐节点的信任度 TR（Recommend Trust)反映了其他节点对待评估节点的交易历史评价，$TR_j=N_j*\sum_{r=1}^{s}(C_r*TL_{rj})$，这里 Cr 为节点 r 的推荐可信度，$C_r=\frac{TL_{ir}}{\sum_{k=1}^{s}TL_{ik}}$，我们通过节点 i 存储的本地信任度来计算推荐可信度。如果在节点交易开始时，没有本地存储的信任值，那么我们可以设置 $C_r=1/s$，其中 s 为收到的反馈节点的数量。

这里我们有个节点的信任度与推荐可信度一致的假设，我们认为能够提供诚实服务的节点同时也能够提供中肯正确的反馈评价，而且这个假设同样可以简化模型，减轻系统负担。

定义 5 设 T_j 为节点 j 获得的最终信任评价值，它来源于网络中其他节点的推荐信任评价反馈值和用户的本地交易历史信任评价值 TL_{ij}，$T_j=(1-\omega)*TL_{ij}+\omega*TR_j$，其中 ω 为常量，$0<\omega<1$。

对于刚刚加入 P2P 网络的节点或者没有主见的节点来说，由于此类节点用户更愿意相信其他节点的推荐信息，可以将 ω 值设置大些；对于一些刚愎自用的节点来说，宁愿相信自己的判断，则可以将 ω 值设置的小些，一般我们可以设为 0.5[2]。

2.2 信任值的更新求解协议

a. 交易后信任值的更新

节点在交互后，被服务节点将对服务提供节点进行评价过程 Evaluation-Local（ID$_i$，ID$_j$，Eval，t），同时更新本地档案的存储信息，如图 1，计算本地信任值。

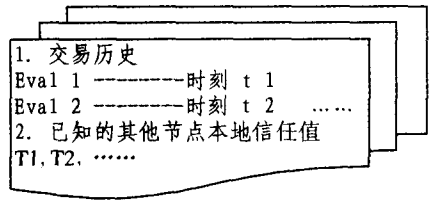

图 1 节点的本地存储信息

Algorithm 1 Evaluation-Local (IDi, IDj, Eval, t)
excuted at peer i
Input: IDj, t Output: Tj
Procedure
  Store (IDj, Eval, t);
  $f(t)<=\frac{t}{\sum_{i,j}t_{ij}}$;
$Tj<=Compute(\sum f(t_{ij})*Eval)$;
  If (IDj not exists)
    Store (IDj, Tj);
  Else
    Update (Tj);
End

从以上的协议可以看出，当节点 i 和节点 j 完成一次交易后，无论成功或失败，都会影响到存储在本地的信任值，而且时间因子保证了近期的交易评价具有较高的权值。

b. 交易前信任值的计算

节点在交易前要获知提供服务节点的信任值，首先向网络中查询其他节点对该节点的历史交易信任值的反馈 Compute-Trust (IDi, IDj, itm, T1…Ti)。当获得一定信任值后即可以计算提供服务节点的信任值，如图 2。

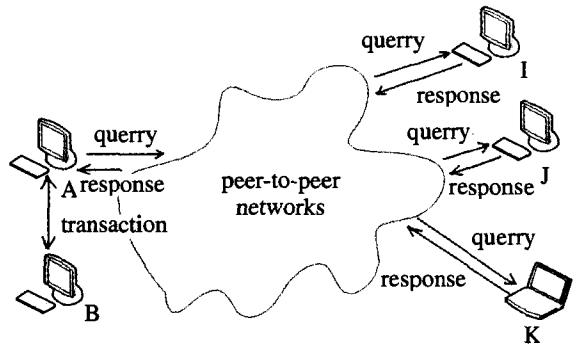

图 2 信任值的查询

Algorithm 2 Compute-Trust (IDi, IDj, itm, T1…Ti, s)
excuted at peer i
Input: IDi, IDj, itm, T1…Ti, Output: T (u)
Procedure
While ($r<s$) do
  Query (IDi, IDj, TLrj);
Return 得到各个节点的本地存储信任值 TL1j, TL2j…TLsj
End While
If ($r<=s$)
  $N_j<=\sin(\frac{\pi}{2*itm}*s)$;
Else
$N_j<=1$;
End if
If (节点非初次交易，存在本地信任值)
$Cr<=\frac{TL_{ir}}{\sum_{k}^{n}TL_{ik}}$
Else
$C_r<=1/s$
End if
$TR_j<=Compute(N_j,C_r,TL_{rj},s)$
$Tj<=Compute(\omega,TLij,TRj)$
Return (Tj);
End

（下转第 73 页）

占用路由时间，由动态路由过程中随时出现的一次或几次失败而触发。然后，利用概率理论和检测过程，迅速、准确地定位故障地点。

链路检测过程进行得彻底、准确、快速，从而保证了鲁棒路由算法的有效性和稳定性，使之具有触发迅速、适应性强、抗毁能力高等特点。尤其是在战争等条件恶劣的环境使卫星网络仍能正常工作。

我们下一步的工作是进一步详细地仿真，研究链路检测与路由算法的关系，使链路检测过程更好地应用到路由策略中去。

参 考 文 献

1 Clark W, Mischa S. Identification of faulty links in dynamic-routed networks [J]. IEEE Journal on Selected Areas in Communications, 1993, 11 (9): 1449～1460

2 Markus W, Cecilia D, Hans-Jorg V, et al. ATM-based routing in LEO/MEO satellite networks with intersattelite links [J]. IEEE Journal on Selected Areas in Communications, 1997, 15(1): 69～82

3 Werner M. A dynamic routing concept for ATM-based satellite personal communication networks [J]. IEEE Journal on Selected Areas in Communications, 1997, 15(8): 1639～1648

4 Chang H S, Kim B W, Lee C G, et al. Topological design and routing for low-earth orbit satellite networks [A]. In: Proc. of IEEE GLOBECOM [C]. Singapore: Singapore, 1995. 529～535

5 Chang H S, Kim B W. FSA-based link assignment and routing in low earth orbit satellite networks [J]. IEEE Transactions on VehicularTechnology, 1998, 47(3): 1037～1048

6 Uzunalioglu H, Akyildiz I F, Bender M D. A routing algorithm for LEO satellite networks with dynamic connectivity [J]. ACM-Baltzer J Wireless Networks (WINET), 2000, 6(3): 181～190

7 Ekici E, Akyildiz F, Bender M D. A distributed routing algorithm for datagram traffic in LEO satellite networks [J]. IEEE/ACM Transactions on Networking, 2001, 9(2): 137～147

8 Katzela I, Schwartz M. Schemes for fault identification in communication networks [J]. IEEE Transactions on Networking, 1995, 3(6): 753～764

9 Bouloutas A, Hart G W, Schwartz M. Simple Finite-State Fault Detectors for Communication Networks [J]. IEEE Transactions on Communications, 1992, 40(3): 477～479

10 Liu G, Mok A K, Yang E J. Composite events for network event correlation [J]. Integrated Network Management VI, 1999. 247～260

(上接第 53 页)

从以上的更新过程可以看出，在交易开始之前，节点 i 与节点 j 进行交互，首先要向网络中发出查询 Query(IDi, IDj)，得到分布式网络中其他节点对节点 j 的信任反馈，节点 i 利用本地存储的各个节点的信任值作为对推荐节点的信任度权值进行计算 Cr，如果节点 i 本地没有交易信任记录，则可以取 Cr 为 $1/s$，然后得到节点 j 的推荐信任值 TRj。最后计算出节点 j 总的信任值 Tj。

相关工作与结论 直接信任度评价反映的是评价方与被评价方的交易经验，由评价方根据被评价方交易时表现出的服务质量给出。推荐信任度反映的是评价方给出直接信任度评价的可靠程度。由于对信任的认知具有强烈的主观性和模糊性，通常很难用常规的精确的度量值对信任(直接信任或推荐信任)进行评价和处理。不少学者对于信任(直接信任或推荐信任)的度量和描述提出了许多不同的方案[9]。

Ernesto Damiani 等人提出了节点和资源相结合的信任模型(servant and resource-based reputation)[6]，认为该模型能够有效地解决新加入节点的冷启动(cold-start)问题，热门的资源可以使节点在短期内获得一定的信任度，但是如何有效地区别两种声誉进行交易也是待解决的问题。Sabater Jordi 提出的 REGRET 模型[8]，认为节点当中存在着小团体，在考虑单独节点信任的同时，也要考虑到团体之间、团体和个人之间的相互信任，但是却导致模型很复杂，较大地增加了网络和节点的处理负担，而且不能够有说服力地确定各种信任之间的权值关系。Ali Aydin Selcuk 等人利用二进制向量来存储信任值[3]，把交易评价简化为成功和不成功，我们认为这样容易导致比较极端的评价，例如一个节点提供的服务不够好就认为失败是不公平的。

我们的模型提出了时间依赖函数 $f(t)$ 的概念。我们认为由于信任不仅仅是历史积累，同时近期行为也是需要考虑的重要要素。因为近期的行为体现着节点的现在和未来的信任走向。通过时间因子来赋予近期的交易评价较大的权值。同时时间依赖函数也制止了某些节点的企图通过积累信任值进行欺骗的行为，因为声誉信任在我们的模型中建立较难，但是降低却很容易，比较有效地反映了信任值的建立较难，破坏容易的特性(easy-destruction-hard-construction)。同时我们还提出了反馈范围 s (scope)的概念，因为得到反馈的范围越广，得到的评价越可信，如果仅仅是几个节点的评价，则可信度不高，因为很可能是小团体的作弊行为。但是我们的模型也有不足之处，例如没有考虑到节点信任值传输中的安全问题，这将是我们今后研究工作的重点。

参 考 文 献

1 Xiong L, Liu L. PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. IEEE transactions on knowledge and data engineering, 2004, 16(7)

2 窦文，王怀民，等. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型. 软件学报，2004，15(4)

3 Selcuk A A, Uzun E, Pariente M R. A Reputation-BasedTrust Management System for P2P Networks. IEEE/ACM CCGRID 2004

4 Hui K Y K, Lui J C S, Yau D K Y. Small World Overlay P2P Networks. IWQOS. In: Twelfth IEEE International Workshop, 2004

5 Ratnasamy S, Shenker S, Stoica I. Routing Algorithms for DHTs: Some Open Questions. In: First Intl Workshop on Peer-to-Peer System, 2002. 45～52

6 Damiani E, di Vimercati D C, Paraboschi S. A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks. CCS'02, Nov. 2002

7 Cai M, Frank M. RDFPeers: A Scalable Distributed RDF Repository based on Structured Peer-to-Peer Networks. WWW2004, May 2004

8 Jordi S, Carles S. REGRET: A Reputation Model for Gregarious Societies. In: 4th Workshop on Deception, Fraud and Trust in Agetn Societies, 2001

9 Meng K, Wang Y, Zhang X, et al. A Trust Management Model for Virtual Communities. CIT2005, 2005. 741～745

10 Zhong Y, Yu Y, et al. Dynamic Trust Production Based on Interaction Sequence: [technical report, CSD-TR 03-006]. Dept. of Computer Science, Pudure University, 2003