基于反馈评价的 P2P 网络信任机制研究 *

侯邱亮,周井泉
(南京邮电大学 电子科学与工程学院,江苏 南京 210003)

摘 要:为了提高 P2P 网络的安全性,提出一种 P2P 环境下以反馈信息评价作为可信度的信任机制,阐述了模型中的信任度的定义,并详细介绍了信任度的计算。对仿真系统进行了性能测试,并对测试结果进行了分析。仿真结果表明,该模型对于信息窃取、信息篡改等类型的恶意攻击有较好的抑制作用。

关键词:信任机制;信任度;通信成功率
中图分类号:TP393 **文献标识码**:A

Research of the trust mechanism of P2P network based on feedback from evaluation

HOU Qiu Liang, ZHOU Jing Quan
(College of Electronic Science and Engineering, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: In order to improve the security of P2P networks, we introduce a new trust mechanism of P2P network based on feedback from evaluation after every communications. This paper proposes the definition of trust in the model and the calculation of the trust in detail. Performance simulation of the system is tested and test results are analyzed, which show that the trust model can help to prevent several attacks of information stealing and modification in some ways.

Key words: trust mechanism; trust; communication success rate

随着 P2P 系统的广泛应用,安全问题也随之产生。主要体现在以下几个方面:由于共享特性带来的安全问题、中间节点的恶意攻击以及针对 P2P 系统结构安全漏洞的攻击等。在 P2P 系统中节点的信息传输往往需要经过多个中间节点的传递,由中间节点产生的威胁最大也最难防范。中间节点恶意攻击包括信息窃取、信息篡改等。

根据建立信任关系所用的方法,P2P 网络的信任模型大致可分为基于可信第三方的信任模型和基于反馈/评价的信任模型两类[1]。基于可信第三方的信任模型采用传统安全体系中的 PKI 技术,通过网络中的少数超级节点来监测整个网络的运行情况,并定期通告违规节点或对其进行处罚。这类系统往往依赖于少量中心节点,因此存在单点失效和可扩展性的问题。基于反馈/评价的信任模型分为资源建立可信度和为通信节点建立可信度两大类。为资源建立可信度的信任模型局限于信息共享的应用,不具有广泛的适用性。为通信节点建立可信度又分为全局信任和局部信任 2 种模型。全局信任模型对网络中所有通信反馈进行分析并为每个节点建立唯一的可信度。在 KAMVAR S 提出的 EigenTrust 模型中是根据节点通信的历史计算本地的信任度,并考虑节点的推荐信任信息,通过节点间信任度的迭代来实现信任的传播[2]。局部信任模型大多关注于提供机制使节点可以根据共享信息为给定节点计算局部信任值。 WANG Y 提出了 P2P 环境下基于贝叶斯网络的信任模型 [3],该信任模型主要关注于描述信任的不同方面,使得节点可以根据不同的场景来按需获取节点不同方面的性能。总之,对于信任度的计算,现有的信任度模型均给出了其各自的计算方法,这些方法在一定程度上提高了系统的安全性。

本文提出在 P2P 网络中引入信任度评价机制来降低恶意节点攻击,从而提高通信成功的概率。根据节点

* 基金项目:国家 863 项目(2009AA01Z202);江苏省科技支撑项目(BE2008134)

在通信交互过程中,其他节点对给定节点的评价来设定信任度,并相应地更新路由表高速缓存器中的信任值,使节点在以后的通信过程中有针对性地选择信任度高的节点作为传递消息的中间节点。

1 信任模型

1.1 信任度

反馈信任机制中关于一个给定节点的信任度的定义,需要考虑该节点与其他节点在以往通信交互过程中,其他节点对该节点的评价。参考文献[4]考虑了3个主要因素:

(1)给定节点收到来自其他节点的通信满意度信息的反馈;

(2)给定节点与其他节点的通信次数;

(3)反馈源信息的可信度。

本文中基于信任机制的P2P系统也是依赖节点的反馈信息来做出信任度评价的。反馈信息是节点在一次通信后接收到的关于通信内容的满意度,这反映了此节点完成其所负责部分通信的程度。

1.2 信任度的搜集、计算和更新

基于通信反馈满意度的信任机制,每个参与通信的节点在通信结束后进行相互反馈。而关于信任度的计算本文采用计算信任度的方法并进行改进,首先定义几个参数:

$I(u,v)$表示节点u与节点v之间的通信次数;

$I(u)$表示节点u与其他节点通信的总次数;

$P(u,i)$表示其他加入的节点与u的第i次通信;

$S(u,i)$表示节点u从$P(u,i)$次通信后得到的满意度;

$C_r(v)$表示节点v反馈源的可信度。

那么节点u的信任度可根据式(1)进行计算:

$$T(u)=\sum_{i=1}^{I(u)} S(u,i)\times C_r(p(u,i)) \tag{1}$$

式(1)中反馈满意度$S(u,i)$的数值在0和1之间。$S(u,i)$和通信次数$I(u)$可以在每次通信结束后自动收集,而反馈源的可信度则需要考虑节点过去的通信历史,定义如下:

$$C_r(p(u,i))=\frac{T(p(u,i))}{\sum_{j=1}^{I(u)} T(p(u,j))} \tag{2}$$

采用式(2)来计算反馈源可信度的前提是基于2个假设,首先恶意节点一定会提供错误的或误导的反馈信息以暴露自己恶意节点的身份,其次正常的节点总是提供正确的反馈信息。

其他通信节点可以通过$T(u)$的值来判断节点u的可信度。简单的判断条件为:如果$I(u)>C_1$并且$T(u)>C_2$,那么节点u就是可信的。其中C_1为节点u最少的通信次数门限值,C_2为节点u最低的可信程度。一个容忍度较高的节点门限值C_2会相对低一些。

考虑到现实中恶意节点并不总是提供错误或误导的反馈信息,正常的节点有时也会提供错误信息,因此本文对给定节点的信任度计算式(1)进行修改,加入节点的信任率T_r,以及适当调整参数α和β的值使得系统在具有恶意节点的网络中能够提高计算信任度值的准确性。修改公式如下:

$$T'(u)=\sum_{i=1}^{I(u)} S(u,i)\times C_r(p(u,i))\times\alpha T_r+\beta \tag{3}$$

其中T_r的值可以通过信任度矢量[5]得出。如节点u与节点v通信完成后,u对v的信任度矢量变为01100110,那么$T_r=\frac{(01100110)_2}{2^8}=0.398\ 4$,即网络节点信任率$T_r$的值为$m$位二进制向量的十进制数值除以$2^m$,因此$T_r\subset[0,1)$。调整参数$\alpha$取0到1之间的值,$\beta$为-1、0或1、初始值为0。定义参数$\mu(0<\mu<1)$来表示$\beta$变化的阈值[6]。当$T_r<\mu$时,恶意节点行为较多,$\beta$为-1;当$T_r>\mu$时,正常节点行为较多,$\beta$为1;其余情况下,设置$\beta$为0。

信任度的更新方式本文采用参考文献[7]提到的设置高速缓存器来收集节点以往通信过程中的信任度。高速缓存器的大小取决于覆盖网络的结构,以及每个节点的有用资源等因素。

2 基于信任机制的P2P模型系统

2.1 系统模型

考虑分布式结构化的P2P系统,以环形P2P网络为基本框架进行改进。在节点模型中添加2个模块,即信任度管理模块和数据定位模块。这样使得每个节点都参与信任度的计算。信任度管理模块用于进行反馈信息的发送和信任度的计算,并维护本地的数据库信息。数据定位模块用来放置和定位P2P网络中的信任值信息。

不同的P2P结构网络采用不同的数据定位方法,例如Gnutella采用基于泛洪的广播方法来搜索信息但是不考虑消息的可靠性,基于DHT算法的Chord[8]网络模型利用哈希函数将通信节点的IP地址转变为全局唯一标识符nodeID,并把关键字和存储位置之间建立一一对应关系,使得给定关键字后就可以唯一确定存储位置。每个节点加入网络都会拥有一个nodeID,并且节点的nodeID不会随着节点改变IP地址或不定时离开覆盖网络而改变。DHT算法首先根据nodeID找到节点的目的地址,然后再把nodeID转换成IP地址。在本文中关于一个节点u的信任数据,以及节点u每次通信后获得的反馈信息,都存储在通过哈希函数得到的具有唯一关键字标志的节点。简单的模型结构如图1所示。

每一个节点都存储许多其他节点的关键字信息,并且维护一张具有其他节点关键字信息的路由表。

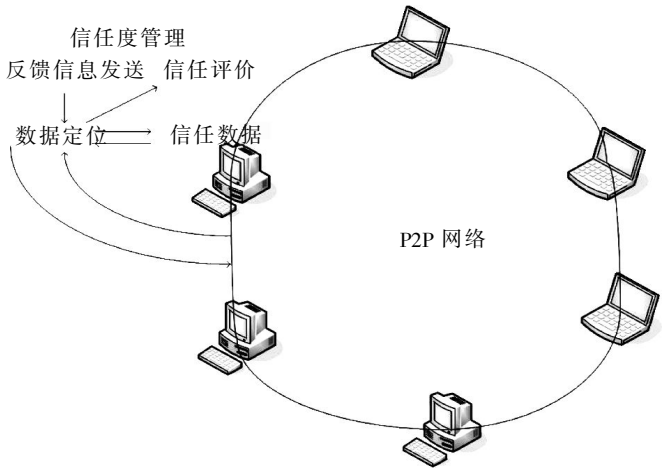

图 1 简单的网络拓扑结构

2.2 路由表及路由算法

本文采用基于 DHT 算法的 P2P 模型的路由表构建方式。路由表中存储邻居节点的信息包括 nodeID、关键字Key及信任度的值。简单的路由表设置如图 2 所示。

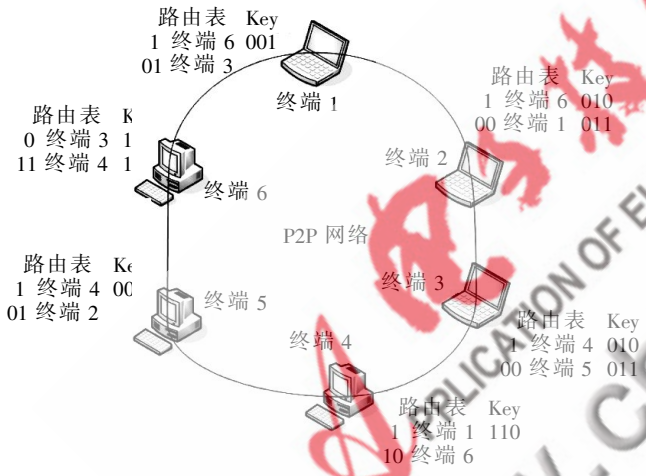

图 2 路由表设置

举例说明对图 2 中网络进行信息查询。当节点终端 2 接收到查询信息 Key 110，终端 2 没有需要的信任度值，那么它查询路由表寻找与 Key 110 有相同前缀的节点信息，这里 1 指向了终端 6，于是根据 1 查询消息发送到节点终端 6，终端 6 也没有需要的信任度值，继续查询终端 6 的路由表，路由表中有 11 指向了终端 4，将查询信息发送到终端 4，终端 4 本地 Key 为 110，于是返回查询需要的信任度值。

3 系统仿真及测试结果

通过仿真实验来验证所提出的系统在有恶意节点的情况下通信成功的概率，并将其与式(1)涉及的信任机制模型以及没有引入信任机制的 P2P 系统三者通信成功的概率进行比较。通过设置恶意节点的数目，以及节点的信任率，来验证系统在不同条件下三者通信成功的概率。

3.1 系统测试环境及参数设置

仿真工具采用 NetLogo 4.0.4。在仿真试验开始时设置 100 个通信节点，其中恶意节点数为 20 个，节点的信任率 T_r 为 40%，μ 为 0.6，α 为 0.4。为了简单起见，在环形 P2P 网络通信中，假设信息传递一圈为一次通信过程，网络中的每个节点在每圈信息传递过程中只进行一次通信。用跳数(time steps，信息在所有节点中传递完一次称为 1 step)来表示仿真时间，在每一跳中每个节点都要完成信息的查询、交换、信任度的更新以及反馈信息的发送。

3.2 仿真结果及分析

仿真结果如图 3、图 4 所示，图中横坐标表示通信的次数，1 step 代表一次通信，纵坐标表示通信成功的概率，虚线的信任模型曲线是在式(1)的模型下得出的，呈上升趋势的实线是改进信任模型式(3)下得出的，呈下降趋势的实线表示没有加入信任度的网络模型。图 3 试验按照 3.1 节的初始条件对系统进行设置，设置 $T_r<\mu$ (此时 $\beta=-1$)，使得系统从恶意行为较多的情况开始，可

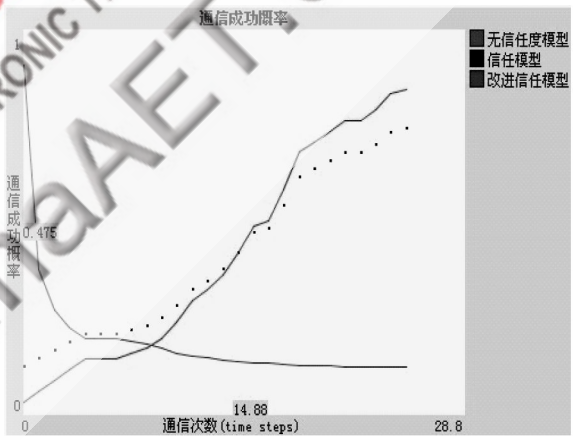

图 3 20 个恶意节点的情况

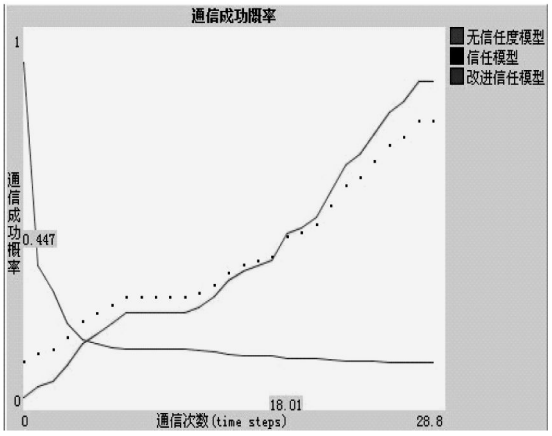

图 4 40 个恶意节点的情况

以看到改进的模型从第 14 次通信(忽略小数部分)开始成功的概率就超过了式(1)的信任模型,并在以后的通信过程中也有一定的优势。

图 4 所示试验将恶意节点数设为 40 个,其他条件不变,保持了节点信任率参与可信度计算的比率并且同样从系统恶意行为较多的情况开始仿真。由仿真结果图可以看到与图 3 相比变化不大,即虽然恶意节点增多了,但是通过设置适当的 α 值还是能够保持较高的通信成功概率。

由 2 次试验结果可以看到,加入节点信任率 T 以及调整参数 α 和 β 后,节点计算信任度的准确性有所提高,使得信息在选择路由时根据信任度的高低选择的中间节点更加可靠,进而通信成功的概率不断地提高。

本文提出了一种基于反馈评价信任机制的模型,通过节点间在通信结束后互相反馈信任信息来计算节点的信任度,同时也考虑到节点的信任率,通过仿真试验看出,信任机制模型通信成功的概率还是很高的。相较于改进前的模型,系统在抑制恶意节点的效率也有所提高。

参考文献

[1] 田慧蓉. P2P 网络信任模型的研究 [J]. 电信网技术, 2007,07(7):28-31.

[2] KAMVAR S , MARIO T S, HECTOR G M. The eigentrust algorithm for reputation management in P2P networks [C]. In proceedings of the 12th international conference on World Wide Web, 2003:640 - 651.

[3] WANG Y, VASSILEVA J. Bayesian network-based trust model [C]. In proceedings of the 2003 IEEE/WIC International Conference on Web Intelligence . 2003:372.

[4] LI Xiong, LIU Ling , PeerTrust: supporting reputation-based trust for Peer-to-Peer electronic communities [J]. IEEE Trans, Knowledge and Data Eng. 2004,16 (7): 843-857.

[5] ALI A S, ERSIN U, MARK R P. A reputation-based trust management system for P2P networks[C]. ACM International Conference on Information and Knowledge Management (CIKM'01),2001:310-317.

[6] 苏瀚, 汪芸. P2P 环境中基于信任度的服务路由系统的研究[J]. 计算机应用研究, 2006,(09):230-233.

[7]Li Xiong, LIU Ling . Building trust in decentralized peer-to-Peer electronic communities [C]. International Conference on Electronic Commerce Research (ICECR-5).2002.

[8] STOICA I , MORRIS R , KARGER D , et al. A scalable peer-to-peer lookup protocol for internet applications [J]. IEEE/ACM Transactions on Networking.2003,11(1):17-32.

(收稿日期:2009-08-21)