文章编号:1001 - 9081(2006)04 - 0833 - 03

一种 P2P 网络安全的信誉度模型设计

宋金龙,董健全,邹亮亮
(上海大学 计算机工程和科学学院,上海 200072)
(songjinlong66@163.com)

摘 要:通过建立一种信誉度模型来隔离恶意节点,保证网络安全可靠并能够提供更好质量、更加有效的服务。从信誉角度构造了一个安全的 P2P 网络,给出了求解信誉度的数学模型和具体算法以及决定信誉度的一些因素,并进行了实验模拟分析,验证此信誉度模型能够有效隔离恶意节点。

关键词:信任值;信誉度;网络安全;P2P
中图分类号: TP393.08 **文献标识码**:A

Design of a reputation model for P2P network security

SONG Jin-long, DONG Jian-quan, ZOU Liang-liang
(*School of Computer Engineering and Science, Shanghai University, Shanghai* 200072, *China*)

Abstract: In order to ensure network secure and reliable and provide better and more qualified service, a reputation model was proposed to isolate bad peer. The mathematical model and algorithm to resolve reputation were given, and the factors which influences reputation were introduced. Simulating and analysis shows that the reputation model can isolate bad peer effectively

Key words: trust; reputation; network scurity; P2P

0 引言

P2P 又被称为对等网或点对点技术,是一种网络模型,在这种模型中所有的节点都是对等的(称为对等点),各节点具有相同的责任与能力并协同完成任务。对等点之间通过直接互连共享信息资源、处理器资源、存储资源甚至高速缓存资源等,无需依赖集中式服务器或资源就可完成。这种模式与当今广泛使用的客户端/服务器(C/S)的网络模式形成鲜明对比,C/S 模式中服务器是网络的控制核心,而 P2P 模式的节点则具有很高的自治性和随意性。随着像 Napster、Gnute11a 这种信息共享应用程序变得越来越流行,P2P 技术受到人们的广泛关注。

P2P 网络是一种开放的,不受限制的网络,Peer 点之间以松散自由的方式联系,在这样的环境特别适合攻击者发布恶意代码。为了防止病毒每个 Peer 点都各自为战,通过安装防火墙,杀毒软件来隔离这些恶意 Peer 点,同时也隔离了友好的 Peer 点。结果使 Peer 点之间很难合作和信息共享,从而违背了 P2P 网络最初提出的开放性,合作性。

单个 Peer 点由于信息有限,区分恶意结点和友好结点具有独断性,非常不准确。基于信誉度模型的 P2P 网络建立在群体 Peer 点上,群体 Peer 点之间交换信息,评价节点的好坏更加精确。

1 计算信誉度的数学基础

1.1 信任值的存储和计算[1]

信任值是基于 Peer 点之间过去所进行的服务(下载文件,资源共享和信息交流等)质量的统计,用一个信任值向量表示某个 Peer 点的信任程度,为每个 Peer 都维护一张为其提供服务的所有 Peer 的信任值表格。

信任值向量用一个二进制数组表示,长度 n 位,1 代表一次好的服务,0 代表不好的服务。当 $Peer_A$ 第一次向 $Peer_B$ 要求服务时,$Peer_A$ 为这个 $Peer_B$ 点建一个信任值向量,初始化全为 0,由于 $Peer_A$ 和 $Peer_B$ 并以前并没有任何联系,这些位不代表任何意义,此时有效位数为 0。在进行一次服务时,信任值向量右移一位,如果服务质量好的话,移入一位 1,否则移入一位 0,如图 1 所示。根据 $Peer_A$ 就可以计算对 $Peer_B$ 的信任值,如图 2 所示。

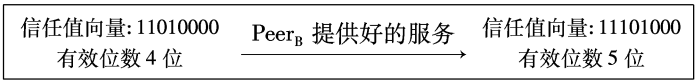

图 1 $Peer_A$ 从 $Peer_B$ 得到诚实的服务后更新信任值向量

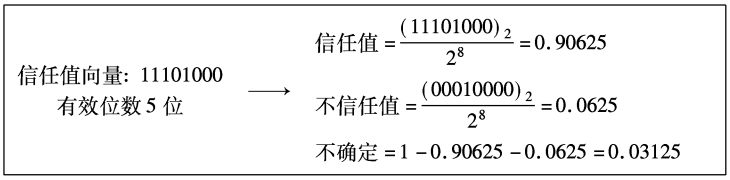

图 2 $Peer_A$ 根据信任值向量计算对 $Peer_B$ 的信任值

上述信任值表示能够保证信任值在最近时间内有效,但由于最近一次服务占整个信任值的 50%,会存在一个问题:如果一个节点在最近几次提供好的服务,其信任值上升太快,会造成一个节点很容易骗取信任值。为了在有效时间内使得每次服务的所占比例相等,准确计算信任值,采取如图 3 所示计算方式。

利用图 3 所示的公式建立一张信任值向量表,如图 4 所示。

收稿日期:2005 - 11 - 01 **基金项目**:上海市科委发展基金资助项目(7A05722)
作者简介:宋金龙(1972 -),男,上海人,硕士研究生,主要研究方向:网络、数据库、人工智能; 董健全(1952 -),女,上海人,副教授,主要研究方向:数据库、人工智能、网络; 邹亮亮(1981 -),男,上海人,硕士研究生,主要研究方向:网络、数据库、人工智能.

信任值向量：11101000
有效位数 5 位 ⟶ 信任值 $=\frac{4}{8}=0.5$；不信任值 $=\frac{1}{8}=0.125$；不确定 $=1-0.5-0.125=0.375$

图 3 $Peer_A$ 计算对 $Peer_B$ 信任值的另外一种方法

Peer 标识	信任值向量	有效位数
P_8	10111000	5
P_7	11000000	2
P_5	10100000	3
P_6	00110000	4
…	…	…

信任值高 ↓ 信任值低

图 4 信任值向量表

图 4 中 P_8 节点信任值最高，并不代表 P_8 节点是一个诚实的节点，只是对本节点提供了好的服务，有可能 P_8 在骗取信任值。P_8 点到底是否可信，则要参考本节点信任值向量表中的 m 个最信任的节点对 P_8 的评价。

1.2 信誉度的计算

1.2.1 信任值的合成

当节点 a 想通过节点 b 对节点 c 的评价时，这就涉及到信任值传递问题，如图 5 所示。

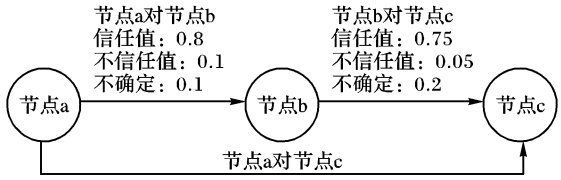

图 5 已知节点 a 到节点 b 到节点 c 的信任值传递过程

如何计算节点 a 对节点 c 信任值，用 *Tab* 代表节点 a 对节点 b 的信任值，*Dab* 代表节点 a 对节点 b 不信任值，*Uab* 代表节点 a 对节点 b 的不确定值，如图 6 所示。

ab \ bc	*Tbc*=0.75	*Dbc*=0.05	*Ubc*=0.2
Tab=0.8	0.6	0.04	0.16
Dab=0.1	0.075	0.005	0.02
Uab=0.1	0.075	0.005	0.02

Tac *Dac* *Uac*

图 6 信任值的合成

可以按如下公式计算 Tac, Dac, Uac[2]：

$$Tac = Tab \times Tbc + Tab \times Ubc + Uab \times Tbc = 0.6 + 0.16 + 0.075 = 0.835 \quad (1)$$

$$Uac = Uab \times Ubc = 0.02 \quad (2)$$

$$Dac = 1 - Tac - Uac = 1 - 0.835 - 0.02 = 0.145 \quad (3)$$

1.2.2 信誉度的计算

节点 a 计算对节点 b 的信誉度，节点 a 选择其最信任的 m（阈值）个最信任的节点和节点 a 到网上查询 n（阈值）个节点 a 不了解的节点对节点 b 的评价，计算公式：

$$R_{ab} = \alpha\overline{T}_m + (1-\alpha)\overline{R}_n \quad (4)$$

$$\overline{T}_m = \frac{\sum_i^m T_i}{m} \quad (5)$$

$$\overline{R}_n = \frac{\sum_j^n R_j}{n} \quad (6)$$

在计算公式(5)时，如图 7 所示，将 m 个节点对节点 b 的评价转化为 m 条链路，分别标识为($l1, l2, \cdots, lm$)，每链路的最大长度不超过 θ。然后对所有链路的信任值求平均值。在处理每条链路时分三种情况，如图 7 所示。

(1)在 $l1$ 链路上，节点 P_a 找到最信任节点 P_1 时，P_1 从自己保存的信任值向量表中找到对 P_b 的信任值，根据信任值合成公式计算 P_a 对 P_b 在链路 l1 上的信任值。

(2)在 $l2$ 链路上，节点 P_a 找到最信任节点 P_7，P_7 查找自己的信任值向量表中没有找到对 P_b 的信任值，继续查找下去，如果超出规定阈值 θ，则 P_a 对 P_b 在 l2 链路值为 0。

(3)在 lm 链路上，节点 P_a 找到最信任节点 P_4，P_4 查找自己的信任值向量表中没有找到对 P_b 的信任值，就将这个请求转发最信任的节点 P_5，如此到 P_8，P_8 信任值表里有对 P_b 的信任值，根据信任值合成公式算 P_a 对 P_b 在 lm 上的信任值。

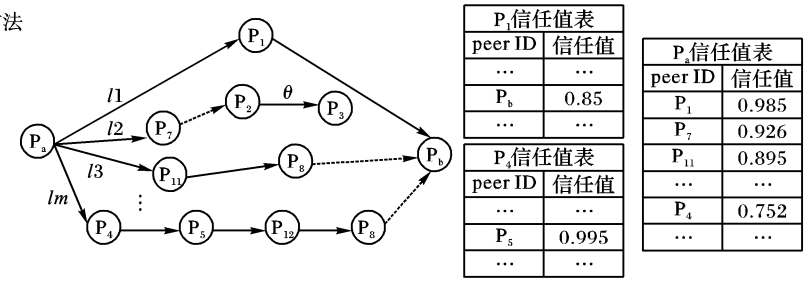

图 7 P_a 点上最信任的 m 个节点对 P_b 节点的评价

计算公式(6)相对简单，就是 P_a 向网上发出查询 P_b 信誉度值的请求，然后从响应中任意选择 n 个对 P_b 的信誉度值求平均值。下面是 P_a 点保存的信誉度表，如表 1 所示。

表 1 节点 P_a 保存的信誉度

Peer 标识	信誉度	计算时间
P_2	0.958	2005-02-01
P_5	0.354	2005-06-06
P_6	0.987	2005-05-23
P_8	0.568	2005-08-2

1.2.3 在 P_a 上求 P_b 信任度的算法伪代码

```
If(Pa 节点信誉度表存在 Pb 的信誉度并且计算时间没有失效)
  begin
  从节点信誉度表读取对 Pb 的信誉度值;
  If(信誉度是否超过可信信誉度阈值)
    执行一些操作;
  Else 结束算法;
  End
  Else begin
    向网上发出查询 Pb 的信任值的请求
    从响应中取 n 个值,计算公式(6),求得 R_n
    从信任值表选取 m 个节点;
    For i=0 to M do Begin
      For j=0 To θ do begin
        If(Pi 点的信任值表中存在 Pb 的信任值并且搜索下一
          节点数小于 θ) begin
          合并信任值,保存 Ti;
          退出循环;
        End
      Else begin
        下一节点数加 1;
        合并信任值,从 Pj 信息值表找到最信任的节点 Pj-1;
      End
    End
    保存 Ri = 0;
  End
  计算公式(4);
  保存 Rab;
End
```

2　补充说明

信誉度的决定因素根据不同的应用可能不同,本文从恶意代码、内容、态度和速度几个方面进行衡量,如图 8 所示。

图 8　信誉度的决定因素

恶意代码对信誉度影响较大,一个节点提供几次安全的服务,信誉度的上升速度比此节点发布一次恶意代码的信誉度下降速度要慢,这样做主要是为了防止某些恶意节点为了骗取信任度;态度是指节点有这个服务,但节点不提供此服务;内容是指服务内容的重要性方面,比如我们下载一个文件是个普通文件,安全性并不高,那么节点的信誉度上升不是很高;速度是指提供服务的速度。

在保存信任值时本文采用的是二进制数组,而不是浮点数,主要考虑信誉度应该是最近时间内节点之间所进行的服务,时间比较长的信任值已经没有多大参考价值,因此使其无效。

公式(4)中的 $1-\alpha$ 要取值很小,一般不超过 15%。这很像人类社会,当我们想了解一个人是否诚实时,我们非常相信最信任的朋友所提供的信息,而我们不了解的人的信息只是作个参考。

公式(5)的阈值 m 和公式(6)的阈值 n 选择要合适,太大会增加计算速度和网络负担,太小不能准确反映出信誉度。图 6 链路长度 θ 也要选择合适的值。

我们把信誉度保存在一张表格中,如图 7,如果信誉度在有效时间内,就没有必要计算,减少网络负担。

3　实验模拟及结果

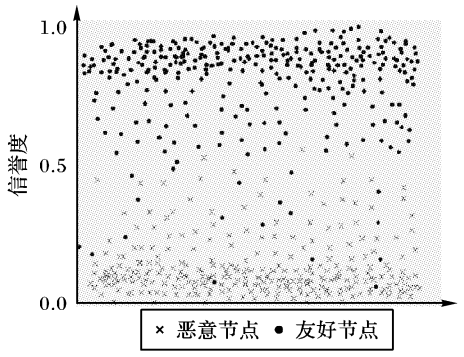

图 9　某一时刻所有节点的信誉度情况

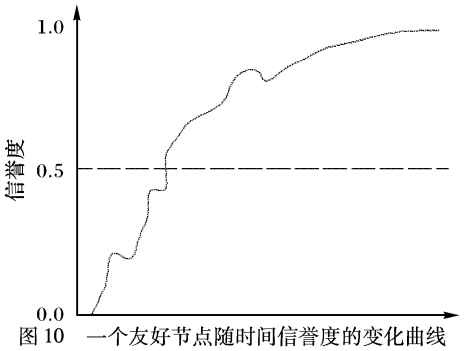

图 10　一个友好节点随时间信誉度的变化曲线

根据上面算法进行模拟,模拟程序用 Java 编写,在模拟环境中建了一个相应的规则库用以评判节点的信任值并调整信任值变化的速度和方向。采用面向方面编程 AOP(AspectJ)和规则编程语言 Jess 设计,使调整信任值向量的程序和主程序分开设计,以便可以随时动态地调节这些规则而不影响主程序运行。实验模拟了 200 节点的行为,每个节点是一个实体,每个实体定义了多个属性(包括恶意代码,态度,内容,速度),每个属性随机赋值。在模拟欺骗行为时,定义了一个属性表示欺骗行为的发生率。运行这些实体计算他们的信誉度。假设在 200 个节点中有 100 为友好节点,100 个为恶意节点,这里友好节点从来不发布恶意代码,但考虑态度,内容,速度因素。恶意节点也模拟几种情况,恶意节点有不同的欺骗行为,假设节点分别有 25%、50%、75% 的欺骗行为。节点之间的服务都是随机的产生。观察节点上所保存的信息表在某个时刻的信誉度情况如图 9 所示,从图中可以看出当把信誉度提高到一定程度,可以完全将友好节点和恶意节点区分开。另外观察了一个友好节点的信誉度变化情况如图 10 所示,一个恶意节点的信誉度变化情况如图 11 所示,从图中可以看出一个节点随着时间的增加,其信誉度基本保持不变。

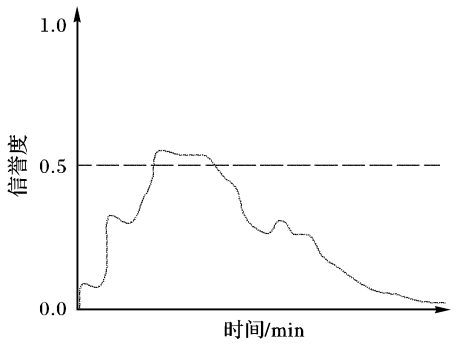

图 11　一个恶意节点随时间信誉度的变化曲线

4　结语

从信誉度角度构造了一个安全 P2P 网络,给出信誉度的计算方法,并通过实验进行了模拟。实验模拟结果说明信誉度的评价是有效的,建立一个用于 P2P 安全的信誉度机制是可行的。在 P2P 网络环境中有很多因素会影响到信誉度,信誉度计算和评判会存在一定的误差,进一步工作会从提高信誉度的准确性和信誉度模型本身的安全性方面进行探讨。

参考文献:

[1] SELPK AA, UZUN E, PARIENTE MR. A Reputation - Based Trust Management System for P2P Networks[A]. IEEE International Symposium on Cluster Computing and the Grid[C]. 2004.

[2] DEWAN P, DASGUPTA P. Securing P2P Networks Using Peer Reputations: Is there a silver bullet?[A]. IEEE Consumer Communications and Networking Conference(CCNC 2005)[C]. Las Vegas, Nevada, USA, 2005.

[3] CHEN R, YEAGER W. Poblano: A distributed trust model for peer-to-peer networks[R]. Technical Report, TR-I4-02-08, 2002.

[4] JURCA R, FALTINGS B. An Incentive Compatible Reputation Mechanism[A]. Proceedings of the IEEE International Conference on E-Commerce[C]. 2003.

[5] AZZEDIN F, MAHESWARAN M. Trust Modeling for Peer - to - Peer based Computing Systems[A]. Proceedings of the International Parallel and Distributed Processing Symposium[C]. 2003.

[6] YAMAMOTO A, ASAHARA D, ITAO T, *et al.* Distributed Pagerank: A Distributed Reputation Model for Open Peer-to-Peer Networks[A]. Proceedings of the 2004 International Symposium on Applications and the Internet Workshops[C]. 2004.

[7] DERBAS G, KAYSSI A, ARTAIL H, *et al.* TRUMMAR - A Trust Model for Mobile Agent Systems Based on Reputation[A]. Proceedings of the IEEE/ACS International Conference on Pervasive Services[C]. 2004. 113 - 120.