一种新的P2P安全积分机制

支萌萌,王汝传
(南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:在P2P网络中,大部分节点都不愿意主动地共享自身资源,这就产生了大量只享受资源而不共享资源的Free Rider。为了减少节点的这种自私行为,在更大程度上激励节点共享资源,并防止节点联合欺骗行为的发生,在密码学的基础上,提出了一种建立在积分值基础上的安全激励方案。通过实现一套安全的通信协议机制,本方案能够有效地保证积分值的准确性和真实性。在促使节点共享资源的同时,防止节点的抵赖和欺骗行为,对促进P2P网络中资源的共享有较好作用。

关键词:对等计算;激励;安全;资源共享
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)08-0137-03

A New Secure Incentive Mechanism in Peer-to-Peer System

ZHI Meng-meng, WANG Ru-chuan
(College of Computer, Nanjing University of Posts & Telecommunication, Nanjing 210003, China)

Abstract: A lot of peers in the current P2P network would not share their resource actively, so that many peers in the system are free riders, which only use the resource of other peers but never share their own resource. In this thesis, a secure incentive mechanism based on peer's contribution will be given. Based on cryptography, by establishing a security communication protocol, this mechanism could ensure the accuracy and reliability of integral value, and could not only urge peers to share their resource, but also effectively restrain the cheating behavior in the network.

Key words: peer-to-peer; incentive; security; resource sharing

0 引 言

P2P技术可以使网络中的各种资源得到充分的利用,因此它已经成为非常热门的一项技术。但是大多数P2P网络中的节点为了最大化自身利益,都不愿意共享自身资源,这就产生了大量的Free Rider[1]。

目前国内外已经有相关的研究机构对P2P计算环境中的激励机制进行研究,并应用于某些实用化的系统中,但在应用中发现很多问题[2]。加利福尼亚大学的seti@home项目[3]和北京大学的MAZE文件共享系统都采用了基于积分的激励机制结果发生了seti@home项目中部分用户更改了客户端软件,MAZE中很多用户合作作弊,从而获得了更高的积分的事件[4]。

因此确保积分在获取、传递以及保存过程中的安全性是非常必要的,也是激励机制能否正常运行的关键。提出了一种安全的激励机制,在促使节点共享资源的同时,有效地确保积分值的可靠性,以保证激励机制能够正确运行。并且预防了P2P网络中的欺诈和抵赖行为。

收稿日期:2008-11-21;**修回日期**:2009-03-02
基金项目:国家自然科学基金(60573141,60773041);江苏省自然科学基金(BK2008451);国家高科技863计划项目(2006AA01Z201,2006AA01Z439,2007AA01Z404,2007AA01Z478);江苏省高技术研究计划(BG2006001);南京市高科技项目(2007软资127);现代通信国家重点实验室基金(9140C1105040805);江苏省博士后基金(0801019C);江苏高校科技创新计划项目(CX08B-085Z,CX08B-086Z)
作者简介:支萌萌(1986-),男,安徽蚌埠人,博士研究生,研究方向为计算机网络、对等计算和消息安全等;王汝传,教授,博士生导师,研究方向为计算机软件、计算机网络和网格、对等计算、信息安全、无线传感器网络、移动代理和虚拟现实技术等。

1 P2P激励机制

1.1 相关定义

积分值:每个网络中的节点都有一个积分值S,它反映了节点对网络贡献的大小。

资源价格:网络中的资源都有价格P。节点索取或贡献资源,就会付出或得到相应价格的积分。

绝对贡献:代表着节点贡献和索取的差值。当节点贡献大于索取时C为正,反之为负。

假设系统中每个节点的初始积分为 initial_ S 的话,那么系统运行过程中节点的积分值就为:S = initial_ $S + P * C$。

1.2 协 议

在协议中涉及到的概念和符号有:

PeerID:节点 ID。P2P 网络中的每个参与节点都有唯一的标识,它由系统自动生成并分配。

FileID:现在大多数 P2P 系统中的文件传输采用的都是分块传输的方式,FileID 是一个文件块的标识。它采用哈希函数对文件块进行哈希生成[5]。一个 FileID 可以唯一标识一个文件块。

Time:记录了文件块交易的时间。

DS:文件发送方的数字签名。

作为防止抵赖[6]的凭证,同时考虑到易用性和实用性,采用 XML 文件对以上信息进行保存。每个节点都保存有两个 XML 方件:SF 和 RF。其中 SF 用来保存节点发送文件块产生的各个信息,而 RF 用来保存节点接收文件块而产生的各个信息。在消息的传递以及文件保存过程中,将采用加密技术[7~9],以保证协议的安全性。

SF 中记录的条数与 RF 中的记录条数之差:$N(SF) - N(RF)$ 就是结点对网络的绝对贡献 C。节点的积分值:S = initial_ $S + [N(SF) - N(RF)] * P$。为了防止被恶意篡改,节点的积分值不是以数值的方式进行存储,而是在需要时读取 SF 和 RF 中记录的条数,进行计算后得出。

无论是在有中心的 P2P 网络、无中心的非结构化或者结构化 P2P 网络(DHT)[10]中,节点 B 通过相应的路由协议找到资源的拥有节点 A,请求下载资源。协议开始运行,协议的流程图如图 1 所示。

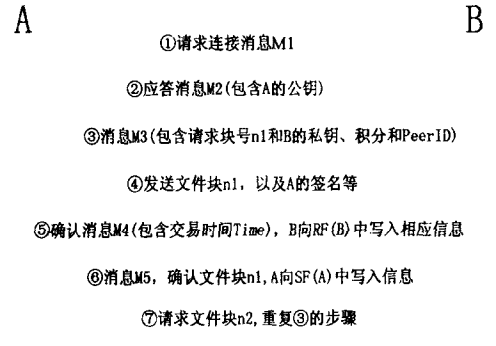

图 1 协议流程图

为防止消息的丢失,协议中所有的消息都设定了重传机制,每个消息最大重传次数为 3 次。超过最大次数,则认定网络不正常,协议终止。协议过程如下:

①A 将资源和资源的哈希值(FileID)一起发布在网络上,节点 B 向 A 发送请求连接的消息 M1;

②A 收到 B 的请求消息后,向 B 发送应答消息 M2。M2 中同时包含了 A 的公钥 PubKey(A);

③B 收到 A 消息,保存下 A 的公钥 PubKey(A),并向 A 发送消息 M3,把 PeerID(B)和自身积分值 S = initial_ $S + P * C$、自己的对称私钥 PriKey(B),以及要请求下载的文件块号一起,经过 PubKey(A)加密后发送给 A;

④A 用 PriKey(A)对消息解密,得到 B 的积分值、PeerID(B),以及 B 的私钥 PriKey(B)。并根据 B 的积分值排队,如果 B 的积分值不够,则把 B 加入等待队列。如果 B 的积分值够高的话,则发送文件块 n1。

由于 FileID 就是文件块的摘要,A 用自己的私钥 PriKey(A)对 FileID 加密,形成 A 的数字签名 DS(A)。然后,把数字签名、文件块、自身 PeerID(A)用 PriKey(B)加密以后发送给 B;

⑤B 收到 A 的文件块及消息后,用自己的对称私钥 PriKey(B)对其解密,得到文件块 n1。将 n1 用相同的哈希函数再哈希一次,得到 FileID,如果与摘要相同,则交易正确,并把 A 的 PeerID(A)、A 的数字签名 DS(A)、文件块接收完成时间 Time,连同文件块的 FileID 一起写入 RF(B)中;然后向 A 发送文件块确认消息 M4,其中包含了文件块接收完成的时间 Time,经过 PriKey(B)加密后发送;如果与 FileID 不同,则出现了错误,需要发送消息通知重传;

⑥A 收到第⑤步确认消息后,用 PriKey(B)对其解密,并把 Time、PeerID(B)、FileID 写入 SF(A)中。在本方案中规定,只要文件 SF 中多了一条记录,就会根据记录中的 PeerID 向对方发送一条确认消息。因此,A 在向 SF(A)中写入记录以后给 B 发送一条确认文件块 n1 的消息 M5;

⑦B 收到 M5 之后,则发送消息 M6 请求下一文件块,然后重新进入第③步往下运行,或者通知文件传送结束。

最后,在一次交互完成后,A 和 B 的 SF 和 RF 中的记录数 N(SF)和 N(RF)都会产生变化,相应的 A 和 B 的积分值:S = initial_ $S + P * [N(SF) - N(RF)]$ 就是新的积分值。

1.3 安全性分析

有了协议的保证,可以很好地防止节点的抵赖和欺骗行为。对于那些试图抵赖和欺骗的节点,通过查看 XML 文件就可以进行裁决。

1)资源发送节点抵赖。

(1)资源的发送节点 A 试图否认曾经发送过文件。查看 B 的 RF(B),其中保存有 A 的 PeerID,传送的 FileID,交易的 Time,以及 A 的签名,使得 A 无法否认;

(2)A 发送虚假文件。协议第⑤步中进行 FileID 检查时,如果与 A 发布的 FileID 不同,则说明 A 传送了虚假文件,此时 A 收不到确认消息,无法向 SF(A)中写入记录。

2)资源接收节点抵赖。

资源接收节点 B 否认收到过 A 的文件或者声称收到虚假文件。查看 SF(A),协议第⑥步中 A 只有收到 B 的文件块接收确认消息之后才会向 SF(A)中写入记录,说明 SF(A)中的文件块记录都是由 B 确认过的。所以 SF(A)中保存的 PeerID,FileID 以及交易 Time 使得 B 无法抵赖。

在协议中,只要密钥安全,就避免了恶意篡改通信中的消息。对于本地存储的 XML 文件,采取加密存储的方式,而且如果删除其中任何一个文件,则软件将不能运行,不能参与网络的活动。

2　实验结果

为了检验以上协议的可行性,在项目开发的软件平台中加入了上述协议。软件运行后产生的两个 XML 文件 SF 和 RF 如图 2 和图 3 所示。

```
<?xml version="1.0" ?>
- <xmlRoot>
  - <sendfile>
    - <Score1>
        <FileID>A0287B34A76C120D63EF9756BDE64FD0213EBC5F7</FileID>
        <PeerID>CC12087C5DE3CD78A013AC4DE6C8D0A8E1F3C4A5B</PeerID>
        <Time>14:32:25</Time>
      </Score1>
    - <Score2>
        <FileID>BD56109013EDFB544803EA8b524b935BDE034ABCC</FileID>
        <PeerID>CC12087C5DE3CD78A013AC4DE6C8D0A8E1F3C4A5B</PeerID>
        <Time>14:32:30</Time>
      </Score2>
  </sendfile>
</xmlRoot>
```

图 2　文件 SF

```
<?xml version="1.0" ?>
- <xmlRoot>
  - <recfile>
    - <Score1>
        <FileID>A0287B34A76C120D63EF9756BDE64FD0213EBC5F7</FileID>
        <PeerID>A012B77D3A018C974B87C90F65E432C38A96D08EA</PeerID>
        <Time>14:32:25</Time>
        <DS>B98E67C0123ABE7653B8967D8462A01B</DS>
      </Score1>
    - <Score2>
        <FileID>BD56109013EDFB544803EA8b524b935BDE034ABCC</FileID>
        <PeerID>A012B77D3A018C974B87C90F65E432C38A96D08EA</PeerID>
        <Time>14:32:30</Time>
        <DS>A28CD01CA64EF946BCA058EFBAC021BA</DS>
      </Score2>
  </recfile>
</xmlRoot>
```

图 3　文件 RF

从实验结果中可以看出,两个节点进行了两个文件块的传输。可以从 SF 中看到文件接收者的 PeerID,从 RF 中看到发送者的 PeerID,以及交互的两块文件的 FileID,交互时间以及数字签名等信息。这些信息为积分值的验证和裁决节点的抵赖和欺骗行为提供了凭证。保证了激励机制的正常运行,有效地促使节点共享资源。

3　结束语

激励机制能否有效地起作用,其最关键的一点就在于积分值的正确性和真实性。文中提出的方案,可以有效地保证积分值的有效性,使节点不能轻易通过抵赖和欺骗的手段获得积分值,进而有效地促使了节点共享资源。

参考文献:

[1] Ma R T B, Lee Sam C M, Lui J C S, et al. An incentive mechanism for P2P networks[C]//Proc Int Conf Distrib Comput Syst. Hachioji, Tokyo, Japan: [s. n.], 2004: 516 - 523.

[2] Kim Jung - Tae, Park Hae - Kyeong, Paik Eui - Hyun. Security Issues in Peer - to - Peer Systems[C]//7th Int. Conf. Adv. Commun, Technol. Phoenix Park, South Korea: [s. n.], 2005: 1059 - 1063.

[3] Anderson David P, Jeff C, Eric K, et al. SETI @home: An Experiment in Public - Resource Computing [J]. Communications of the ACM, 2002(45): 56 - 61.

[4] Golle P, Leyton - Brown K, Mironov I, et al. Incentives for sharing in peer - to - peer networks[C]//Proc. ACM Conf. Electron. Commer. Tampa, FL, United States: [s. n.], 2001: 264 - 267.

[5] 邢书宝,李　刚,薛惠锋. 一次一密加密系统设计与实现[J]. 计算机技术与发展, 2007, 17(3): 150 - 152.

[6] 周　鹏,鱼　滨. 基于 P2P 分布式数据库实时更新[J]. 计算机技术与发展, 2007, 17(5): 144 - 147.

[7] 张维凤,张代远. P2P 网络中基于文件路由模型搜索方法的改进[J]. 计算机技术与发展, 2006, 16(12): 111 - 113.

[8] 张国治,党小超,魏伟一. 基于信任域的 P2P 访问控制模型研究[J]. 计算机技术与发展, 2006, 16(8): 228 - 230.

[9] 温建华,高海锋. 一种基于公钥体系的 P2P 激励机制[J]. 计算机应用, 2007, 27(3): 590 - 592.

[10] 杨　帆,沙　瀛,程学旗. 一个 P2P 分布式数字签名系统[J]. 计算机应用, 2007, 27(2): 308 - 310.