文章编号:1001 - 9081(2007)03 - 0590 - 03

一种基于公钥体系的 P2P 激励机制

温建华,高海锋
(复旦大学 信息科学工程学院,上海 200433)
(stickto@ gmail. com)

摘 要:针对 P2P 网络的搭便车行为及网络资源的同质化现象,提出了一个基于 PKI 体系和结构化 P2P 网络的激励机制。该激励机制不但鼓励节点提供资源下载,还让资源发布者从中受益,从而有效地抑制搭便车行为,减轻了资源的同质化现象。

关键词:P2P;激励;公钥体系;结构化 P2P 网络。
中图分类号: TP393.08;TP393.07 **文献标识码**:A

A peer-to-peer incentive mechanism based on PKI

WEN Jian-hua, GAO Hai-feng
(*School of Information Science and Engineering, Fudan University, Shanghai* 200433, *China*)

Abstract: To solve free rider and homogenization problems in peer-to-peer (P2P) network, an incentive mechanism based on public key infrastructure (PKI) and constructed P2P network was proposed. The mechanism not only encourages node to provide downloading function, but also benefits resources publisher. It restrains free riding behavior effectively, and alleviates homogenization.

Key words: peer-to-peer (P2P); incentive; Public Key Infrastructure (PKI); constructed P2P network

0 引言

近年来,随着 P2P 技术的日益成熟,越来越多的基于 P2P 技术的网络应用在互联网上悄然兴起。从早期的 Nasper[1],到时下最为流行的文件下载应用 BitTorrent[2] 和 eMule[3],P2P 网络已经成为了互联网不可或缺的一部分。

P2P 网络的结构本身,从有中心节点的 Nasper,到无中心非结构化的 Gnutella[4]、Freenet[5],再到现在的基于 DHT (Distributed Hash Table) 的结构化 P2P 网络如 Chord[6]、CAN[7] 及 Pastry[8] 等,也在不断地进化。

然而,目前的 P2P 网络,无论是结构化的还是非结构化的,都基于一个假设,那就是每个参与的节点都能善意地,最大化地提供网络资源。但单个节点往往希望最大化自身的网络效用[9]。由于目前的 P2P 网络没有考虑这个事实,一方面使得 P2P 网络中搭便车者(Free Rider)盛行。根据对 Gnutella 网络的调查显示[10],近 70% 的节点是搭便车者,他们不作任何贡献或作少量的贡献,却向网络索取大量的资源;而有近半数的资源来自网络的 1% 的共享节点,这使得网络资源集中化,造成网络拥堵,从而引发了公共悲剧问题[11]。另一方面,节点拥有的资源同质化日趋严重,用户无法从 P2P 网络获得有效的资源。

随着公钥基础设施(Public Key Infrastructure, PKI)[12] 建设的完善,数字证书已经日益普及。本文提出了一种基于结构化网络和 PKI 体系的激励机制,它不但鼓励节点提供资源下载,还让资源加入者从中受益,从而不但可以有效地抑制搭便车行为,更使得网络资源日益丰富。

1 框架

1.1 基础

首先引入几个概念:贡献值、上传下载比、资源价格和分配比例。

贡献值是指节点对 P2P 网络所作的贡献。每个在 P2P 网络中的节点都有一个贡献值 C。

上传下载比是指每个节点提供的上传带宽与下载带宽的比值,记为 r。

每个资源都付出一定的贡献值才能够使用,即资源价格 p。当节点从 P2P 网络下载资源时,若资源价格为 p,那么它应该支付 p 点贡献值,即其贡献值变为 $C - p$。

分配比例 β 是指提供下载所得的收益中分配给资源发布者的比例,即 βp 分配给资源发布节点,$(1-\beta)p$ 分配给提供资源下载的节点,以鼓励节点发布资源。

为了鼓励节点多作贡献,目前主要有两种激励措施[13]:金钱支付和差异化服务。前者涉及到虚拟货币及支付系统等问题,尽管可以采用微支付等手段,但它并不实用[14]。本文采用后者作为主要的激励措施,通过调整节点下载的优先次序,来达到差异化服务的目的。

当多个节点向某个节点请求文件时,由于上传带宽的限制,被请求节点无法同时为所有节点提供资源,此时为所有的请求节点计算优先系数 k,公式如下:

$$k = \begin{cases} C * r, & C \geqslant 0 \\ C/r, & C > 0 \end{cases}$$

采用高 k 值优先下载的原则,具有较高 k 值的节点先行下载,较低 k 值的节点则加入等待队列。

收稿日期:2006 - 09 - 17

作者简介:温建华(1977 -),男,江西石城人,硕士研究生,主要研究方向:P2P 网络; 高海锋(1948 -),男,江苏人,副教授,主要研究方向:下一代计算机网络、分布式计算.

1.2　激励协议

在资源 R 投入到 P2P 网络并最终下载到用户节点的过程中,存在以下参与节点:

O :Owner,资源的发布节点;

S :Sender,资源的提供下载节点;

U :User,资源的使用节点,它从 S 处下载资源;

M :Mediation,中介仲裁节点。

其中,对某一资源,只存在一个发布节点 O,在资源的传播过程中可以存在多个发送节点 S,也会为多个节点 U 所使用。而且节点 U 在下载资源后,同样可以作为发送节点提供资源给其他用户节点。

为了保障这个激励机制的正常运行,设计如下协议:

资源发布协议　如图 1。

1.1　资源拥有节点 O 对资源 R 做摘要:$h_1 = H(R_2)$,然后找到结构化网络中应该存储 h_1 的节点 R,将 h_1、p 和 β 等信息存储到这个节点上;

1.2　资源拥有节点 O 将 R 和 h_1 发给 Sender 节点。

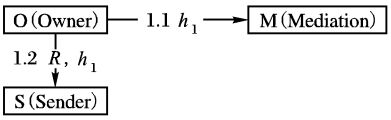

图 1　资源发布

资源下载协议　如图 2。

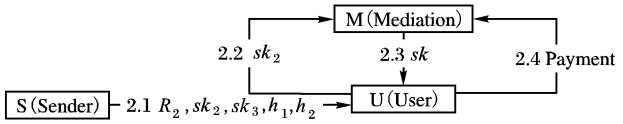

图 2　资源下载

2.1　节点 S 为此次下载产生随机密钥 sk,并用它对 R 进行加密得:$R_2 = E_{sk}(R)$,然后对 R_2 做摘要并用自己的私钥 ssk 加密得:$h_2 = E_{ssk}(H(R_2))$。用节点 M 的公钥 mpk 加密 sk 得:$sk_2 = E_{mpk}(sk)$,再用节点 S 的私钥对 sk_2 做加密得:$sk_3 = E_{ssk}(sk_2)$。将 R_2, sk_2, sk_3, h_1 和 h_2 发给用户节点 U;

2.2　用户节点用节点 S 的公钥解密 h_2 得:$h'_2 = D_{sss}(h_2)$,同时对 R_2 做摘要得 $h''_2 = H(R_2)$,对比 h'_2 和 h''_2,若相同,则向中介节点 M 发送 sk_2;

2.3　中介节点 M 用自己的私钥解密 sk_2 得:$sk = D_{msk}(sk_2)$,将 sk 发给用户节点 U ;

2.4　用户节点 U 用 sk 解密 R_2 得:$R = D_{sk}(R_2)$,再对 R 做摘要得:$h'_1 = H(R_2)$,如果 h'_1 值与 h_1 相符,通知节点 M 按比例支付贡献值给节点 O 和 S。

1.3　安全性分析

作为中介节点的 M,同时具备仲裁职能。在发送节点 S 和用户节点 U 发生争执时,由 M 来裁决哪个节点抵赖。采用本文的协议,M 只须与 S 或 U 中的一个节点沟通即可判断出哪个节点抵赖,从而可以有效地减低了仲裁的成本与复杂度。针对 S 或 U 的抵赖情况,分析如下:

1)发送节点 S 抵赖

1.1 节点 S 发送的内容不是指定的资源 R,那么在资源下载协议2.4中,用户节点 U 对 R_2 解密后做摘要的值 h'_1 就不会等于 h_1,从而节点 S 无法得到支付;

1.2 节点 S 未发送正确的密钥 sk,在资源下载协议2.4中节点 U 无法解密 R_2,同样节点 S 无法得到支付。

2)用户节点 U 抵赖

2.1 节点 U 声称根本没有收到过资源,那么在资源下载协议2.2中,它就不可能发送 sk_2 给节点 M,显然节点 U 抵赖;

2.2 节点 U 声称收到不正确的资源 R,则它应该向节点 M 提供 R_2, sk_2, sk_3, h_1 和 h_2。节点 M 用节点 S 的公钥解密 h_2 得到 h_1,同时对 R_2 做摘要得到 h'_1,对比两者以确保节点 U 提供的 R_2 的真实性。同样节点 R 用节点 S 的公钥解密 sk_3 得到 sk'_2,与 sk_2 对比以确保节点 U 提供的 sk_2 的真实性。然后节点 M 重复资源下载协议2.4中节点 U 的操作,从而可以确定 U 是否抵赖;

2.3 节点 U 声称收到错误的密钥 sk,采用2.2的方法同样可以验证节点 U 是否抵赖。

2　实验结果

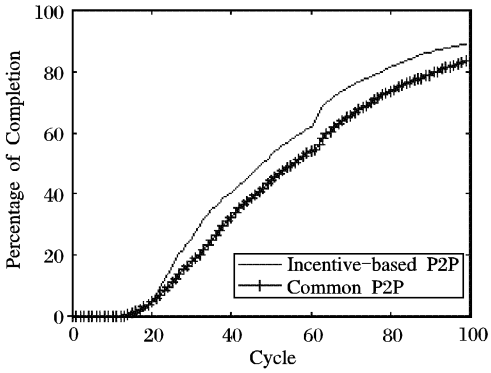

图 3　所有节点完成情况对比

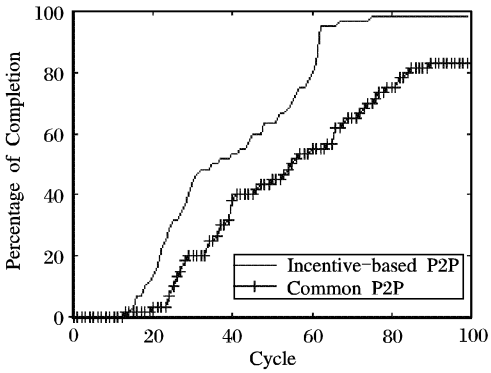

图 4　资源发布节点完成情况对比

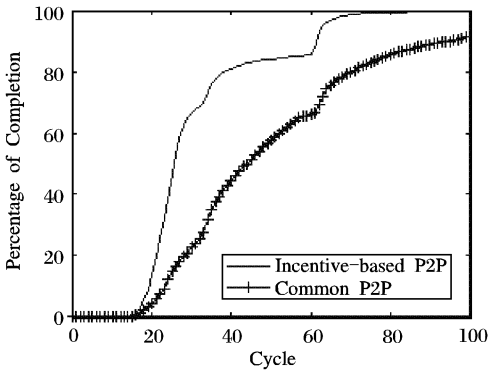

图 5　高贡献节点($r \geq 1$)完成情况对比

为评价本文的激励机制,采用 PeerSim[15] 进行仿真实验。假设有 50000 个节点,每个节点初始的贡献值 C 均为 0,然后为节点随机地分配上传带宽和下载带宽,并保证一半节点上传下载比 r 大于或等于 1.0,另一半节点 r 小于 1.0。将 60 个资源随机地分配到网络中的 60 个节点上,每个节点一个资源,也就是说,这 60 个节点是资源发布节点。实验采用循环制(*Cycle*),每一次循环节点之间交换一次文件。如果一个节点

拥有了这 60 个资源,我们认为它是已完成节点,反之为未完成节点。

从图 3 ~ 图 5 中可以看出,在引入了本文的激励机制后,所有节点、资源拥有节点和高贡献节点($r \geq 1.0$)的完成情况都得到了有效的改善。而从图 6 中,我们可以发现,本文的激励机制前期循环中,对低贡献节点($r < 1.0$)有明显的抑制作用,从而为高贡献节点提供更好的服务;在后期的循环中,由于高贡献节点完成度较高,低贡献节点的完成情况也开始好转。

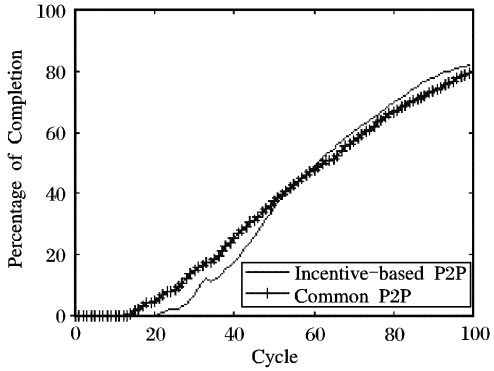

图 6 低贡献节点($r < 1$)完成情况对比

从实验结果可以看出,本文的激励机制可以有效地抑制节点的自私行为,并鼓励节点发布资源和提供资源下载。

3 结语

本文针对 P2P 网络中搭便车和资源同质化的问题,提出了基于节点贡献值的提供差异化服务的激励机制,不但鼓励节点提供资源下载,还鼓励节点为 P2P 网络加入新的资源,以丰富网络资源。在此基础上,本文提供了一套基于 PKI 和结构化 P2P 网络的资源发布和下载协议来保证激励机制的有效实现。

参考文献:

[1] Nasper website. http://www.nasper.com[EB/OL], 2006.
[2] BitTorrent website: http://www.bittorrent.org[EB/OL], 2006.
[3] eMule website. http://www.emule.org[EB/OL], 2006.
[4] Gnutella website. http://www.gnutella.com[EB/OL], 2006.
[5] CLARKE I, SANDBERG O, WILEY B, *et al*. Freenet: A distributed anonymous information storage and retrieval system[A]. FEDERRATH H, ed. Proceedings of the Workshop on Design Issues in Anonymity and Unobservability [C]. Berlin: Springer-Verlag, 2001. 46 - 66.
[6] STOICA I, MORRIS R, KARGER D, *et al*. Chord: A scalable peer-to-peer lookup service for internet applications[A]. ACM SIGCOMM 2001[C]. 2001.
[7] RATNASAMY S, FRANCIS P, HANDLEY M, *et al*. A Scalable Content-Addressable Network[A]. SIGCOMM'01[C]. 2001. 161.
[8] ROWSTRON A, DRUSCHEL P. Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems [A]. GUERRAOUI R, ed. Proeedings of the IFIP/ACM International Middleware Conference[C]. London: Springer-Verlag, 2001. 329 - 350.
[9] SHNEIDMAIN J, PARKES DC. Rationality and self-interest in peer to peer networks[A]. Second international workshop on peer-to-peer systems (IPTPS), LNCS 2735[C]. Springer-Verlag Press, 2003. 47 - 52.
[10] ADAR E, HUBERMAN B. Free riding on Gnutella[R]. Xerox PARC, 2000.
[11] FELDMANY M, LAIZ K. Quantifying disincentives in peer-to-peer networks, workshop on economics of peer-to-peer systems[A]. LNCS 2735[C]. CA: Springer-verlag, 2003. 117 - 122.
[12] HOUSLEY R, POLK T. Planning for PKI[M]. John Wiley & Sons, 2001.
[13] GOLLE P, LEYTON-BROWN K, MIRONOV I, *et al*. Incentives for Sharing in Peer-to-Peer Networks[A]. Proceedings of the 2001 ACM Conference on Electronic Commerce[C]. 2001.
[14] BURAGOHAIN C, AGRAWAL D, SURI S. A Game Theoretic Framework for Incentives in P2P Systems[A]. Third IEEE International Conference on Peer-to-Peer Computing (P2P 2003)[C]. Linkoping, Sweden, 2003.
[15] PeerSimwebsite. http://peersim.sourceforge.net[EB/OL], 2006.

(上接第 589 页)

文献[4],长度为 $O(\log_2 N)$,N 是网络中的节点总数。仿真时节点数目为 60,公钥数目为 60 × 5,每个节点都随机挑选一些公钥进行查询,对每次查询均记录其路径长度。图 8 为概率密度随路径长度变化的曲线图。从图中可见,密度最大的路径长度值近似等于 $(1/2)\log_2 N$,N 为节点数目。

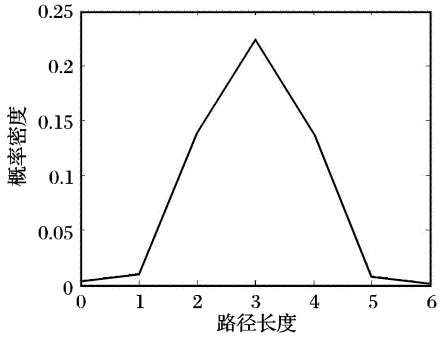

图 8 节点数为 60 时查找路径长度的概率密度曲线

4 结语

本文以基于 P2P 网络,提供 VOD 服务的 CDN 为背景,根据其稳定、上下线不频繁的特点,提出了分布式 PKI(DPKI)的安全认证方法。DPKI 基于安全成熟的 PKI 机制,同时由于其 P2P 结构,提高了系统的可扩展性,避免了 PKI 中 CA 的单点失效问题。通过对仿真结果的分析得出,在负载均衡及查询路径长度上均体现出了 P2P 的优势。

本文的系统并未把 PKI 的所有功能均离散并实现,比如证书的有效期和归档,私钥的备份和恢复,如何在分布式结构中实现这些功能仍是亟待考虑的问题。

参考文献:

[1] LEE H, KIM K. An adaptive authentication protocol based on reputation for peer-to-peer system[A]. The 2003 Symposium on Cryptography and Information Security[C]. 2003.
[2] Groove Networks. A white paper: groove security architecture[EB/OL]. http://www.groove.net/products/workspace/security.html, 2002 - 10.
[3] PERLMAN R. An overview of PKI trust models [J]. IEEE Network, 1999, 130(6): 38 - 43.
[4] SKARMETA AFG, PEREZ GM, REVERTE SC, *et al*. PKI services for IPv6[J]. IEEE Internet Computing, 2003, 7(3): 36 - 42.
[5] BUBNIS E, EVANS S, FISCHER P, *et al*. Open-source PKI on SELinux[A]. DARPA Information Survivability Conference and Exposition[C]. 2003, 2. 170 - 175.
[6] STOCIA I, MORRIS R, KARGER D. Chord: a scalable peer-to-peer lookup service for internet application[A]. Proceedings of the 2001 ACM SIGCOMM Conference[C]. 2001. 149 - 160.