软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(Suppl.(2)):52−60

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

一种基于价格的 P2P 匿名通信系统激励机制*

郑 明[1,2,3], 吴建平[1,2], 刘 武[1,2]

[1](清华信息科学与技术国家实验室(筹)(清华大学),北京 100084)

[2](清华大学 网络科学与网络空间研究院,北京 100084)

[3](国防科学技术大学 人文与社会科学学院 军队政治工作研究所,湖南 长沙 410074)

通讯作者: 郑明, E-mail: zhengm09@outlook.com, http://www.tsinghua.edu.cn

摘 要: 提出了一种基于价格的 P2P 匿名通信系统激励机制.通过对 P2P 系统和匿名通信系统研究中提出的激励机制进行归纳和分析,对搭便车用户给 P2P 匿名通信系统造成的影响进行定性和定量分析.提出在 P2P 匿名通信系统中通过对掩饰流量、中转流量和出口流量进行区别定价,建立流量价格体系,量化用户生产和消费的系统资源.引入价格机制一方面能够有效激励 P2P 匿名通信系统中用户提供流量中转和出口服务,从而提高整个 P2P 匿名通信系统的性能,另一方面也促使"搭便车"用户为系统提供掩饰流量,提高整个系统的匿名性,还能促使用户在申请匿名服务时根据自身需求申请适当的中转节点数,避免系统资源的不必要消耗.基于应用场景的用户策略分析证实了基于价格机制的 P2P 匿名通信系统激励机制的有效性.

关键词: P2P;匿名通信;激励机制;价格体系

中文引用格式: 郑明,吴建平,刘武.一种基于价格的 P2P 匿名通信系统激励机制.软件学报,2015,26(Suppl.(2)):52−60. http://www.jos.org.cn/1000-9825/15015.htm

英文引用格式: Zheng M, Wu JP, Liu W. Price-Based incentive mechanism for P2P anonymous communication system. Ruan Jian Xue Bao/Journal of Software, 2015,26(Suppl.(2)):52−60 (in Chinese). http://www.jos.org.cn/1000-9825/15015.htm

Price-Based Incentive Mechanism for P2P Anonymous Communication System

ZHENG Ming[1,2,3], WU Jian-Ping[1,2], LIU Wu[1,2]

[1](Tsinghua National Laboratory for Information Science and Technology (Tsinghua University), Beijing 100084, China)

[2](Institute of Network Science and Cyberspace, Tsinghua University, Beijing 100084, China)

[3](Institute of Military Political Work, College of Humanities and Social Sciences, National University of Defense Technology, Changsha 410074, China)

Abstract: This paper proposes a price-based incentive mechanism for P2P anonymous communication system. Through pricing on dummy traffic, relay traffic and export traffic, the P2P anonymous communication system builds a pricing system. The pricing system quantifies the user's system resource production and consumption. First, it can effectively stimulate users in P2P anonymous communication system to provide relay and export services. These services effectively improve system performance. Secondly, the pricing system can motivate free-riders in providing dummy traffic. The dummy traffic enhances the system's anonymity. Finally, the pricing system is also capable of prompting the user to request the appropriate relay nodes according to their needs in order to avoid unnecessary consumption of system resources. User policy analysis based on scenarios confirms the validity of price incentives P2P anonymous communication system.

Key words: peer to peer; anonymous communication; incentive mechanism; price system

随着互联网的迅速发展,用户对隐私和安全的需求也日益增长.匿名通信是一种有效的隐私保护机制.P2P

* 基金项目: 国家自然科学基金(20121302362)
收稿时间: 2014-05-02; 定稿时间: 2014-08-22

体系具有分布式、可扩展性、健壮性、高性能、隐私保护和负载均衡的特性.基于 P2P 的匿名通信系统也具有 P2P 体系的优势,所有的参与者都可以提供中继转发的功能,因而可以极大地提高匿名通信系统的灵活性和可靠性.但是 P2P 体系所固有的“搭便车”问题也会导致匿名通信系统的效率大幅降低、性能下降和服务质量受限.并且“搭便车”节点的频繁加入和退出系统也会影响到通信的匿名性[1].目前应用最广泛、用户数量最多、Internet 中最成功的公共匿名通信服务 Tor 的同时在线用户已经接近 60 万,但是其拥有的 relays 节点仅有 3 000 左右,Bridges 节点仅有 1 000 左右,用户和中继的比例达到 67:1[2].即使是 Tor 这种成功的公共匿名通信系统也一直受到“搭便车”行为的影响,导致用户获得的服务质量下降.造成 P2P 匿名通信系统服务质量下降的主要原因是用户理性选择适合自身的策略导致匿名通信系统中带宽资源、转发节点和出口节点缺乏.因此,节点激励机制的引入对于 P2P 匿名通信很重要.

节点激励机制是通过自定义的机制刺激和孤立客体活动,以促进和激励主体与客体之间的互动.节点激励机制在 P2P 网络中的作用是促进节点更多地参与到 P2P 网络中,减少“搭便车”的行为,避免“公共物品的悲哀”.激励机制应该具有公平性、自治性、可扩展性和安全性.需要注意的是,激励机制应该有具体的量化标准,有具体的激励方法,能够对“搭便车”行为有效抑制,并且能够解决节点动态变化的问题.

我们对 P2P 匿名通信系统中用户的“搭便车”行为特征进行分析,提出了基于价格机制的 P2P 匿名通信激励机制.针对匿名通信系统中的不同类型流量,系统制定不同的价格,通过对 P2P 匿名通信系统资源生产、消费的价格机制进行设计,激励用户在积极参与系统服务、稳定在线时间、提供系统资源、保证系统效率的同时保证系统的公平性,避免对“搭便车”用户的惩罚.

本文第 1 节介绍相关工作.第 2 节分析 P2P 匿名通信系统中用户节点.第 3 节研究搭便车行为对 P2P 匿名通信系统的影响.第 4 节提出基于价格机制的 P2P 匿名通信系统的激励机制设计.第 5 节分析加入激励机制后,用户在不同应用场景下的策略选择.第 6 节中讨论加入激励机制对性能和安全性的影响.第 7 节进行总结和展望.

1 相关工作

1.1 匿名通信网络中的激励来源

现实网络中匿名通信系统的激励来自群体的支持、有偿服务和政府的支持这 3 个方面.最成功的公共匿名服务系统 Tor 的节点激励主要来自于群体的支持,也就是互联网上志愿者们为了维持 Tor 的运行而自愿贡献的资源.也有部分节点激励来自政府支持,例如,各研究机构为进行 Tor 相关研究而投入资源提供中转和出口服务.Freedom 和 Anonymizer 的节点激励是有偿服务,通过向用户收费用于支付给 ISP 的带宽费用,并向用户提供匿名服务.AN.ON 是由德国政府直接资助的,但是 2007 年已经停止资助了,只能转为寻求群体支持和有偿服务.此外,Acquisti[3]等人曾经提出对匿名性需求高的用户为其他匿名需求低的用户提供中转服务以实现自身的匿名性.但是,这种模式在高延时匿名通信系统上可以应用,能否在低延迟匿名通信系统上应用还没有结论.而且匿名需求高的用户愿意支付的开销会影响到参与用户的数量和提供的匿名性.因此,一般匿名通信系统的激励机制的设计都是基于激励来自群体的支持这一假设.

1.2 P2P网络中的激励机制

1.2.1 基于直接互惠的激励机制

最简单的激励机制就是直接互惠.谁在交互时提供的服务好,就回报谁.谁提供的服务不好,就惩罚谁.BitTorrent[4]使用一报还一报策略,Scrivener[5]使用信用记录在本地保存其他节点的协作情况来实现公平的带宽共享.Wallach 等人[6]在 2003 年提出一种审计机制来发现欺诈者,并将其逐出系统.Samsara[7]通过平等交换存储空间来保证公平和定期查询节点来验证是否真实提供了存储.Tangler[8]要求用户在消费资源之前先提供一段时间资源作为试用期.

1.2.2 基于声誉的激励机制

声誉系统是节点利用历史交互信息来制定其在未来交互时所采用的策略.Dingledine[9]总结了很多记录节点声誉的方法.如果新节点加入系统时被赋予一定的声誉值,那么恶意节点很容易通过重新加入系统来洗白自身声誉.Resnick[10]认为要提高陌生节点的加入成本.EigenTrust[11]通过一种分布式算法,根据节点以往的表现来计算全局信任值.Blanc[12]等人建议用可信权威来管理所有节点的声誉值.声誉系统在文件分享型 P2P 网络中获得了很大成功,但是,因为匿名用户节点之间不一定会发生交互,多次交互又会影响系统的匿名性,所以其不适用于匿名通信系统.

1.2.3 基于交易和支付的激励机制

基于交易和支付的激励机制一般采用量化资源的方法来建立交易体系.SHARP[13]是一个用户通过可信节点进行资源交易的框架.KARMA[14]和 Seal[15]通过建立多个审查者来记录每个节点的资源使用情况.Golle 等人[16]为 P2P 系统建立微支付体系,用博弈论模型来分析用户策略.

1.3 匿名通信系统中的激励机制

激励机制一直是匿名通信系统设计的重要环节.Franz[17]等人提出为每个 Mix 节点提供独立的电子支付来进行激励,但是因为每跳都会和 Mix 以及 Mix 目录服务器产生交互信息,所以效率不高.PAR[18]提出一种微型支付模型,向提供服务的中继节点进行小额付费,通过为系统提供服务来获得收入.但是这种模型是基于一种还停留在理论设计阶段的电子银行系统的,所以还无法实际运行.Dingledine 等人[19]提出在 Tor 中利用目录服务器给工作好的中转节点赋予金星,提升这些中转节点的数据的中转优先级以提高其应用的性能,以此激励节点.Jansen 等人[20]提出 BRAIDS 机制,将 Tor 的服务按照性能不同分为 3 个类型,节点通过提供服务获得替代电子货币,节点使用替代电子货币来支付不同类型的服务费用.Tortoise[21]是通过提高中继节点的流量优先级,限制每个连接的流量速率来激励用户成为中继节点.

2 P2P 匿名通信系统中的用户节点分析

基于 P2P 体系对等、独立和自组织的特点,P2P 匿名通信系统不能强制要求参与的匿名用户保持在线,提供转发或者出口服务.只能提供给用户多种选择,采用激励机制激励用户理性的选择自身的策略.

2.1 用户加入P2P匿名通信系统的原因

P2P匿名通信系统中的用户按照需求不同可以分为身份匿名型和流量匿名型两大类.身份匿名型用户主要是需要隐藏自身真实身份、IP 地址、访问习惯、个人资料等信息.因此,身份匿名型用户需要较强的匿名性,最少需要 3 个辅助节点来避免 IP 地址或者通信对象的直接暴露.他们需要在访问特定网站,例如艾滋病网站或者电子投票网站时避免被恶意攻击者收集身份信息并分析.流量匿名型用户主要是需要突破 ISP 或者政府部门设置的流量过滤设备.例如,避免文件分享应用 BitTorrent 被 ISP 过滤,或者访问 Youtube,facebook 等被屏蔽的网站.

2.2 P2P匿名通信系统节点行为模式

P2P 匿名通信系统是一种特殊的 P2P 系统.P2P 匿名通信系统与文件分享等资源共享型 P2P 应用系统不同,流量对应的内容因为经过匿名化之后不可估值,所以只有流量本身具有价值.流量由带宽和在线时间决定.因此,按照累计在线时间和累计提供带宽划分 P2P 匿名通信系统中的节点类型才有实际意义,特别是表现在对理性节点的分析上.例如,许多用户选择节点长时间在线,愿意提供服务给其他用户,这是 P2P 精神之所在.相反,有些用户会根据自己的通信需要选择短时间登录系统,不愿意或者没有资源提供给其他节点,这些节点所提供的服务流量就会少.同时,每个节点的活动并不是恒定不变的,用户会根据自身的需求选择节点策略,用户策略的变化直接影响了节点在线时间和提供带宽的变化.因此,P2P 匿名通信系统只能根据历史服务流量和在线时间来判断节点的行为模式,将用户为系统提供的可用带宽作为节点资源分配时的依据.

根据用户在线时间的不同,可以将用户分为稳定在线节点和随机在线节点.为了避免需要经过长期数据收集才能得出用户在线规律这一复杂的计算过程.我们假设用户在加入系统前将宣告自己的在线时间,将用户分

为承诺在线节点和非承诺在线节点.而在统计用户在线规律时只需要考虑用户是否承诺和承诺是否被遵守.通过承诺在线时间的方法,可以更简便地统计出系统的在线节点数量和可用资源.

2.3 P2P匿名通信中搭便车产生的原因

P2P 匿名通信系统中用户的“搭便车”行为按照用户的考虑可以分为资源消耗型和安全顾虑型两类,资源消耗型是在 P2P 系统中,“搭便车”用户为了节约带宽等资源,在获取共享资源的同时却不愿意共享自身的资源,这种行为在 P2P 匿名通信中主要表现为在线时间短、贡献带宽低、拒绝加入掩饰流(dummy traffic)等方式;安全顾虑型是用户在考虑保护自身安全的情况下,拒绝为其他节点提供某些服务,这种行为在 P2P 匿名通信中主要表现为拒绝转发消息,拒绝作为出口节点(exit-point),设置转发规则拒绝转发某些协议等方式[22].

3 搭便车行为对 P2P 匿名通信影响分析

3.1 资源消耗型搭便车用户对P2P匿名通信的影响的定性分析

从定性角度来说,资源消耗型搭便车用户在有通信需要时加入 P2P 系统,在完成通信需求后离开 P2P 系统.从匿名性的角度而言,P2P 匿名通信系统依靠节点相互协作,转发消息来实现节点的匿名.如果系统中存在大量资源消耗型搭便车用户,这些用户在线时间很短,在任意一个时刻,P2P 匿名通信系统中存在的在线节点就会很少,此时,攻击者如果控制部分节点,则很容易被选中进入匿名信道,导致发送者的匿名性被破坏.此外,资源消耗型用户不会产生掩饰流量.这就导致只有正在通信的节点会产生有效流量,有利于攻击者甄别出参与通信的节点,P2P 匿名通信系统的节点无法从其他节点处得到保护.从性能的角度而言,资源消耗型搭便车用户贡献的带宽低,如果系统中存在大量资源消耗型搭便车用户,整个 P2P 匿名通信系统的资源就会被这些搭便车用户大量占用,导致愿意提供资源的用户得不到优质的服务,从而离开 P2P 匿名通信系统;而且,如果这些资源消耗型搭便车用户进入匿名信道,由于他们在线时间短且随机上下线,一次通信过程中可能需要多次更换信道上的节点,一方面导致恶意节点有可能进入匿名信道,另一方面由于重组信道导致通信延时增加,影响正常用户体验.

3.2 安全顾虑型搭便车用户对P2P匿名通信影响的定性分析

从定性角度来说,安全顾虑型搭便车用户的匿名意识更高,为了保护自身的匿名性而拒绝提供某些服务.从匿名性的角度而言,由于安全顾虑型搭便车用户的存在,管理节点需要收集用户节点提供的转发规则,在管理节点和建立匿名信道时提供给发送者准确的信息.这将导致匿名集的规模大幅度减小.从性能角度而言,由于安全顾虑型搭便车用户的出口规则设置,某些协议将被拒绝转发,这有可能导致用户体验变差.

更重要的是,安全顾虑型搭便车用户有可能无法被激励机制激励,这些用户是否愿意提供某些服务取决于用户对这些服务的安全顾虑和激励效果的权衡,一般情况下无法进行定量分析并给出参考策略.

3.3 资源消耗型搭便车用户对P2P匿名通信影响的定量分析

3.3.1 匿名度的计算方法

匿名通信系统的匿名度一般采用信息熵的方法来计算.假设系统有 N 个节点,p_i 是节点 i 被确认为通信发送者的概率,系统的熵 $H(X)=-\sum_{i=1}^{N}(p_i\log_2 p_i)$. 在理想情况下,$N$ 个节点都表现得行为特点一致,这使得每个节点被确认为匿名通信发送者的可能性为 $1/N$.在此情况下,匿名通信系统的熵为 $H^*(X)=\log_2 N$, 匿名通信系统的匿名度的定义即可具体化为 $D(X)=H(X)/H^*(X)$. 在考虑恶意节点必然存在,且存在 M 个的情况下,如果没有其他攻击方法,仅排除恶意节点,则此时系统的熵值为 $\log_2(N-M)$.即系统的匿名度可表示为 $D(X)=\log_2(N-M)/\log_2 N$. 在攻击事件 F 存在的情况下,匿名通信系统 X 的匿名度可以定义为 $D(X)=\sum_{\omega\in\Omega}\left[P(F=\omega)H(X\mid F=\omega)\right]/H^*(X)$.

3.3.2 存在搭便车用户的系统匿名度计算方法

一般匿名通信系统只考虑合法用户和恶意用户数量与攻击方法对系统匿名度的影响.P2P匿名通信系统还

需要考虑合法用户中搭便车用户的数量.在不考虑其他攻击方法的情况下,系统总共有 N 个节点,其中含有搭便车用户 F 个,恶意用户 M 个.因为搭便车用户不参与信道构建,所以在攻击者观测时,这些搭便车用户可以视为不在线.系统的匿名度可以表示为 $D(X)=\log_2(N-M-F)/\log_2 N$.在不考虑其他攻击方法的前提下,恶意节点的比例和搭便车节点的比例对系统的匿名度影响是一样的,也可以理解为,从系统匿名度上来说,搭便车节点和恶意节点造成的影响是一样的.因此,将搭便车节点激励为正常节点是非常必要的,而且能够对整个系统的匿名度产生积极的影响.

4 基于价格机制的 P2P 匿名通信激励机制设计

P2P 匿名通信系统应当对用户为系统做出的历史贡献给予相应的回报,而不是仅仅考虑在线节点的利益.因此,有必要将用户和节点两个概念进行解耦合.我们设计的激励机制应当是建立在用户基础上的,无论用户是否在线,都应该统一考虑.

只有将用户生产或者消费的系统资源进行具体量化才能准确地衡量用户的贡献,因此,我们将用户历史生产流量作为量化贡献的唯一标准.结合 P2P 匿名通信系统中"搭便车"行为的原因,我们又考虑到掩饰流量、中转流量和出口流量的价值权重应当有所区别.为激励用户更多的参与中转和作为出口,我们将出口流量的价格定义为掩饰流量的 P_3 倍,将中转流量价格定义为掩饰流量的 P_2 倍.确定了一般等价物——掩饰流量之后,匿名系统就可以对用户生产和消费的流量进行一般量化,衡量出用户为系统做出的历史贡献.

在 P2P 匿名通信系统中,用户可分为两类.用户可以选择成为假名用户或者匿名用户.假名用户在系统中拥有账户,可以将自身节点设置为中转或者出口节点,可以将生产和消费的流量计入账户供下次连接时使用或者转赠其他账户.匿名用户在系统中不保留账户.在 t 时间内,匿名通信系统中有 N_1 个提供出口服务节点,N_2 个提供中转服务节点,N_3 个提供掩饰服务节点,$f(i)$表示用户 i 需求的带宽,$g(i)$表示用户 i 供给的带宽.总需求带宽不大于总供给带宽.

4.1 价格体系

系统将用户 i 提供的资源纳入资源分配体系,并根据系统拥有的中转和出口带宽、服务占用的中转和出口带宽确定 t 时间内中转流量价格 $P_2=P_2'\times\left(1+\sum_{i=1}^{N_1+N_2+N_3}f(i)\Big/\sum_{i=1}^{N_2}g(i)\right)$ 和出口流量价格 $P_3=P_3'\times\left(1+\sum_{i=1}^{N_1+N_2+N_3}f(i)\Big/\sum_{i=1}^{N_3}g(i)\right)$ 的溢价变化,P_2'和 P_3'分别初始赋值为 2 和 4.

4.2 生产和消费

匿名用户因为没有账户,不存在利用历史积累消费,所以只能通过实时生产掩饰流来获得服务.匿名用户 i 在每次连接 P2P 匿名通信系统时,申报需要使用的中转节点数量 M 和匿名系统可以使用的带宽 $g(i)$.匿名通信系统在匿名用户 i 连接后,根据用户 i 提供的带宽值返回相应数量的目标地址,其中只有一个地址为有效下一跳,其他地址为掩饰地址.用户 i 节点开始向这些地址发送数据流.此时,匿名用户 i 可用带宽为 $f(i)=g(i)/(P_3+M\times P_2)$,$i\in N_3$.假名用户在系统中拥有账户,可以积累历史生产流量.假名用户 i 每次连接 P2P 匿名通信系统时申报匿名系统可以使用的带宽 $g(i)$,并可以用一定数量的历史生产流量作为担保,承诺在 t 时间内稳定在线,成为稳定在线节点,并提供中转或出口服务.如果假名用户 i 完成在线时间承诺,并在 t 时间期间有 $x(0<x<1)$ 比例的带宽被系统使用,用于中转或出口服务,则将生产的流量 $G(i)$计入用户 i 的帐户,如果未能完成在线时间承诺,则将担保的历史流量扣除.此时,提供中转服务的假名用户生产获得的流量 $G(i)=(1-x+x\times P_2)\times g(i)\times t$,而 $G(i)=(1-x+x\times P_3)\times g(i)\times t$ 则是提供出口服务的用户生产获得的流量.当假名用户需要使用系统服务进行消费时,用户根据自身需求,申请 M 个中转节点和 1 个出口节点.系统根据用户 i 在 t 时间内消费的流量 $F(i)=(P_3+M\times P_2)\times f(i)\times t$ 进行计费.若假名用户生产与消费平衡,且并未使用生产积累,则此时提供中转服务的用户 i 的可用带宽为 $f(i)=(1-x+x\times P_2)\times g(i)/(P_3+M\times P_2)$, 提供出口服务的用户 i 的可用带宽为 $f(i)=$

$(1-x+x\times P_3)\times g(i)/(P_3+M\times P_2)$. 从掩饰、中转和出口流量的价格设置可知,我们设计价格机制的目的一方面是鼓励用户更多参与中转和出口服务,另一方面是鼓励用户按需申请中转节点.因为用户在申请服务时需要的中转节点越多,需要支付的生产流量就越多,这样可以促使用户根据自己的实际需求申请适当的中转节点数量.文件分享和抗审查需求的用户可以通过减少中转节点的方式获得自身收益的最优.需要保持匿名强度的用户可以通过申请更多的中转节点来保证自己的匿名性.

5 用户的策略分析

假设在一定时间段 t 内,3 名用户,即假名用户 A,B 和匿名用户 C 进入系统,开始申请匿名通信服务.假名用户 A 为安全顾虑型用户,考虑到自身安全,只愿意提供带宽给系统作为中转服务.假名用户 B 为志愿用户,愿意提供带宽作为出口服务.匿名用户 C 为资源顾虑型用户,只享受服务不提供服务.假设 P_2 的初始赋值为 2,P_3 的初始赋值为 4,假定供求关系平衡,且不产生流量价格变化.

5.1 场景1

A,B,C 用户均为身份匿名用户,需要通过多节点协作,以隐藏自身信息.用户 A,B,C 为满足最低匿名需求,均申请 2 个中转节点,1 个出口节点.假设假名用户 A,B 生产和消费平衡.系统使用了用户提供带宽的比例为 x.此时,用户 A,B,C 生产和可用消费带宽比例如图 1 所示,随着系统使用假名用户资源比例的增长,假名用户 B 和用户 A 对系统贡献的资源价值在增长的同时,其可用带宽比例也在不断上升.这符合激励机制的设计理念,贡献越大,获得的回报就越大.匿名用户 C 因为其为系统提供的资源价值没有增长,所以可用带宽数量没有变化,因此越来越不如假名用户 A 和 B.假名用户 B 由于生产的出口流量的价值比假名用户 A 生产的中转流量价值高,因此能够获得更大的可用消费带宽比例.

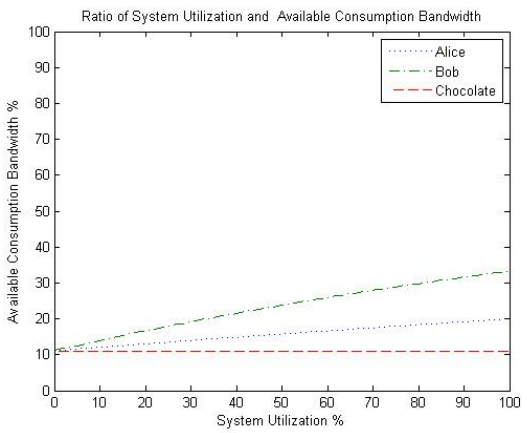

Fig.1 Identity anonymous user production and consumption ratio of available bandwidth

图 1 身份匿名用户生产和可用消费带宽比例

5.2 场景2

用户 A,B,C 均为流量匿名型用户,需要通过匿名系统混淆自身通信特征,以获得文件分享服务.用户 A,B,C 为满足最低混淆需求,均只申请一个出口节点.假设假名用户 A,B 生产与消费平衡.系统使用了用户提供带宽的比例为 x.此时,用户 A,B,C 随时间增长而获得的生产和可用消费带宽比例如图 2 所示.

对比图 1 和图 2 可以看出,在场景 2 中,当用户 A,B 仅使用一个出口服务器时,相对于场景 1 能够更有效地提高自身的可用消费带宽比例.用户 C 获得的可用带宽比例也比场景 1 高.因此,用户在不需要较高匿名度时,使用较少中转节点能够更有效地利用自身带宽.通过场景 1 和场景 2 的对比可以看出,价格机制在激励用户按需申请资源和实现贡献与回报正反馈方面,都对用户有明显的激励作用.

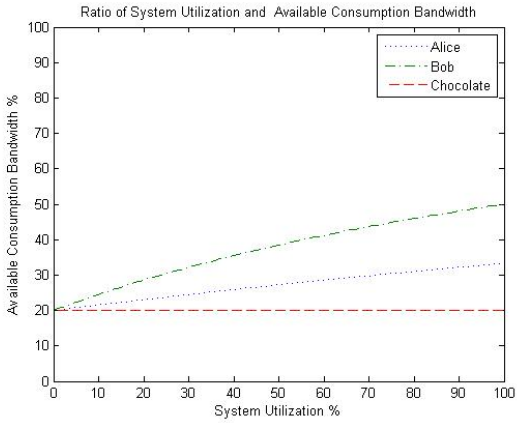

Fig.2 Traffic anonymous user production and consumption ratio of available bandwidth

图 2 流量匿名用户生产和可用消费带宽比例

5.3 场景3

假名用户 *A*,*B* 和匿名 *C* 再次进入系统.在再次进入系统之前,用户 *A* 和用户 *B* 曾经为系统提供服务并有历史生产积累存在.假设假名用户 *A*,*B* 在再次进入系统之后生产与消费平衡,且使用积累进行消费.假定历史生产积累可以按照用户提供带宽的一定比例(例如 20%)进行消费.系统使用了用户提供带宽的比例为 *x*.此时,用户 *A*,*B*,*C* 在积累并未消费完之前,随系统占用率增长而获得的可用消费带宽比例如图 3、图 4 所示.图 3 为身份匿名用户,图 4 为流量匿名用户.

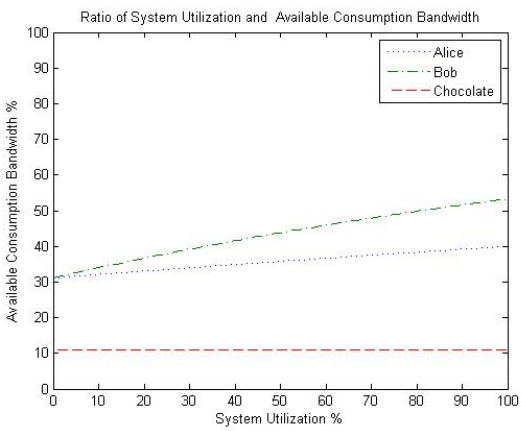

Fig.3 Identity anonymous user production and consumption ratio of available bandwidth

图 3 身份匿名用户生产和可用消费带宽比例

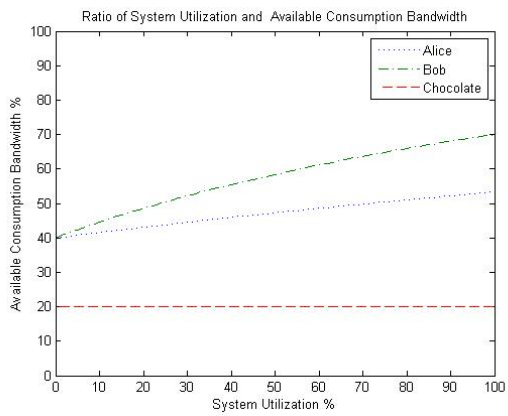

Fig.4 Traffic anonymous user production and consumption ratio of available bandwidth

图 4 流量匿名用户生产和可用消费带宽比例

将图 3、图 4 与图 1、图 2 比较可以看出,如果假名用户在空闲时段加入系统进行生产积累,与无积累的假名用户相比能够获得更大的可用消费带宽.无论是进行匿名 Web 访问,还是进行文件分享,都比无积累的情况下更有优势.当用户的生产积累消费完毕后,又回归到场景 1 或者场景 2 的状态.

在场景 3 中,价格机制可以促使用户在空闲时段投入一定量的资源来获得需要服务时更大的使用带宽.这样,系统也可以获得更多的在线节点和带宽资源.

6 讨 论

在 P2P 匿名通信系统中增加了激励机制,不可避免地会对系统的性能和安全性造成一定的影响.为了确定这些影响的作用,从性能和安全性两个方面进行讨论.

6.1 性能影响

匿名用户由于其不存在积累流量,所以在每次申请服务时,其获得的可用带宽只与其自身提交的带宽 B 和申请的中转节点数量 K 相关.在信道建立之时,客户端根据系统反馈的下一跳节点数量限制单地址的流量速率.匿名用户在获得 $B/(2K+5)$速率的可用匿名通信服务带宽的同时,为系统提供$(2K+4)B/(2K+5)$速率的掩饰流.因为确定可用速率是在申请建立信道时确定的,因此,激励机制不会影响到通信过程中的请求平均时间等性能问题.

假名节点在请求服务时则是根据自身节点类型、提交的自身带宽、申请的中转节点数量、是否拥有历史积累、提供服务的带宽情况来获得系统反馈的服务节点数量.据自身节点类型、提交的自身带宽、申请的中转节点数量这 3 个参数在申请通信服务时就已经确定,因此,假名节点可能由于历史积累消耗完毕和为系统提供服务带宽的变化而变化可用带宽.

无论是哪种情况,系统为节点提供服务的依据都是按照公平性、多劳多得的原则,采用激励机制的目的是维持系统的平衡,而不是单纯追求服务性能的提高.

6.2 安全性影响

假名节点在提供服务时需要向管理节点上报服务流量以便于统计假名节点的历史积累.如果假名节点采用实时更新的方式与管理节点沟通,恶意观察者将观察到管理节点地址.这将影响到系统的安全性.因此,采用定期或者定量流量更新的方式,通过第三方渠道,例如电子邮件或者社交网络方式上报能够避免假名节点与管理节点的直接连接,从而避免激励机制对系统的安全性造成影响.

7 结论与展望

P2P 匿名通信系统具有特殊性,其匿名特征使得节点不可能记录其他节点的声誉或者交互历史记录,只能由系统来记录和统计.常用的 P2P 节点激励机制在考虑到匿名性需求之后,很难直接套用.现有的 P2P 匿名通信系统激励机制从性能优化方面考虑,限制文件分享匿名用户流量或者要求其为系统提供资源,而对于更多的 Web 匿名用户不作要求.这些激励机制实际上无法实现对等匿名节点的互惠互利.如果现有匿名通信系统中高资源志愿者节点流失,系统的服务能力会受到很大影响,用户性能和匿名性也会下降.

与性能优化导向的激励机制相比,基于价格机制的激励机制更能体现出用户贡献的反馈,在系统实现上更多地考虑了节点的公平性.出口流量使匿名服务得以实现.中转流量为系统提供了匿名性.掩饰流量加强了系统的匿名性.3 种流量的价格分别代表了不同的系统贡献程度.用户不再因为使用匿名服务的应用不同而被区分服务,而是根据自身使用系统资源情况实时为系统提供等价资源.这样构建的 P2P 匿名通信系统是均衡发展的.通过用户场景分析可知,用户在权衡自身投入资源和可能获得收益之后,倾向于成为中转或者出口节点以获得更好的用户体验.

下一步的工作将主要研究两个方面:一方面是由于节点突发离线造成的其他用户流量损失量化及补偿;另一方面是系统用户历史生产流量和实时消费流量如何通过税收福利机制来调节,保证系统的良好运转.

致谢 在此,我们向对本文的工作给予支持和建议的清华大学网络安全实验室的老师和同学表示感谢.

References:

[1] Wright M, Adler M, Levine BN, Shields C. Defending anonymous communication against passive logging attacks. In: Proc. of the 2003 IEEE Symp. on Security and Privacy (IEEES&P2003). IEEE Computer Society Press, 2003. 28−43.

[2] https://metrics.torproject.org
[3] Acquisti A, Dingledine R, Syverson, P. On the economics of anonymity. In: Wright RN, ed. Proc. of the FC 2003. LNCS 2742, Heidelberg: Springer-Verlag, 2003. 84−102.
[4] Cohen B. Incentives build robustness in BitTorrent. In: Proc. of the Workshop on Economics of Peer-to-Peer Systems. 2003.
[5] Nandi A, Ngan TWJ, Singh A, Druschel P, Wallach DS. Scrivener: Providing incentives in cooperative content distribution systems. In: Alonso G, ed. Proc. of the Middleware 2005. LNCS 3790, Heidelberg: Springer-Verlag, 2005. 270−291.
[6] Wallach DS, Druschel P. Enforcing fair sharing of peer-to-peer resources. In: Proc. of the 2nd Int'l Workshop on Peer-to-Peer Systems (IPTPS). 2003.
[7] Cox LP, Noble BD. Samsara: Honor among thieves in peer-to-peer storage. In: Proc. of the 19th ACM Symp. on Operating System Principles (SOSP 2003). 2003.
[8] Waldman M, Mazières, D. Tangler: A censorship resistant publishing system based on document entanglements. In: Proc. of the 8th ACM Conf. on Computer and Communication Security (CCS 2001). 2001.
[9] Dingledine R, Freedman MJ, Molnar D. Accountability measures for peer-to-peer systems. In: Peer-to-Peer: Harnessing the Power of Disruptive Technologies. O'Reilly and Associates, 2000.
[10] Resnick P. The social cost of cheap pseudonyms. Journal of Economics and Management Strategy, 2001,10(2):173−199.
[11] Kamvar SD, Schlosser MT, Garcia-Molina H. The EigenTrust algorithm for reputation management in p2p networks. In: Proc. of the 12th Int'l World Wide Web Conf. 2003.
[12] Blanc A, Liu YK, Vahdat A. Designing incentives for peer-to-peer routing. In: Proc. of the 24th IEEE INFOCOM. 2005.
[13] Fu Y, Chase JS, Chun BN, Schwab S, Vahdat A. SHARP: An architecture for secure resource peering. In: Proc. of the 19th ACM Symp. on Operating System Principles (SOSP 2003). 2003.
[14] Vishnumurthy V, Chandrakumar S, Sirer EG. KARMA: A secure economic framework for p2p resource sharing. In: Proc. of the Workshop on Economics of Peer-to-Peer Systems. 2003.
[15] Ntarmos N, Triantafillou P. Seal: Managing accesses and data in peer-to-peer sharing networks. In: Proc. of the 4th IEEE Int'l Conf. on P2P Computing. 2004.
[16] Androulaki E, Raykova M, Srivatsan S, Stavrou A, Bellovin SM. PAR: Payment for anonymous routing. In: Borisov N, Goldberg I, eds. Proc. of the PETS 2008. LNCS 5134, Heidelberg: Springer-Verlag, 2008. 219−236.
[17] Golle P, Leyton-Brown K, Mironov I, Lillibridge M. Incentives for sharing in peer-to-peer networks. In: Proc. of the 3rd ACM Conf. on Electronic Commerce. 2001.
[18] Franz E, Jerichow A, Wicke G. A payment scheme for mixes providing anonymity. In: Proc. of the Int'l IFIP/GI Conf. on Trends in Distributed Systems for Electronic Commerce (TREC'98). 1998. 94−108.
[19] Dingledine R, Wallach DS. Building incentives into Tor. In: Proc. of the Financial Cryptography (FC 2010). 2010.
[20] Jansen R, Hopper N, Kim Y. Recruiting new tor relays with BRAIDS. In: Proc. of the ACM Conf. on Computer and Communications Security (CCS). 2010.
[21] Moore WB, Wacek C, Sherr M. Exploring the potential benefits of expanded rate limiting in Tor: Slow and steady wins the race with tortoise. In: Proc. of the 2011 Annual Computer Security Applications Conf. (ACSAC 2011). 2011.
[22] Guo RL. Research and design of user incentive mechanism in P2P anonymous communication system [MS. Thesis]. Harbin: Harbin Institute of Technology, 2006 (in Chinese with English abstract).

附中文参考文献:

[22] 郭人路.P2P 匿名通信系统用户激励机制的研究与设计[硕士学位论文].哈尔滨:哈尔滨工业大学,2006.

郑明(1977－),男,湖南湘潭人,博士,讲师,主要研究领域为网络安全,隐私保护,匿名通信,渗透测试.

吴建平(1953－),男,博士,教授,博士生导师,CCF 会士,主要研究领域为计算机网络.

刘武(1966－),男,博士,副教授,主要研究领域为网络安全.