基于 Bloom Filter 的安全 P2P 共享模型

严华云[1,2] 关佶红[1]
(同济大学电子与信息工程学院 上海 201804)[1] (湖州师范学院信息工程学院 湖州 313000)[2]

摘 要 针对当前对等网中虚假文件的问题,提出了一种安全 P2P 共享模型(SPSM)。在该模型中为了激励节点共享自己的资源,引入虚拟货币(VC)以激励各个节点共享自己的资源;并在模型中引入了举报机制,即当网络中一个节点下载了虚假文件后就向 CA(Certification Authorities,认证中心)举报提供虚假资源的节点,经 CA 甄别后将该恶意节点放入恶意节点集;为了节省存储空间,SPSM 根据自身的特点,采用了 Bloom Filter 的变体 DBF 来存储恶意节点。为了验证提出的 SPSM 模型的有效性,将其与 Trust 模型进行了比较,结果表明 SPSM 模型比 Trust 模型更有效。

关键词 Peer-to-Peer,网络安全,Bloom Filter
中图法分类号 TP393 **文献标识码** A

Security P2P Sharing Model Based on Bloom Filter

YAN Hua-yun[1,2] GUAN Ji-hong[1]
(College of Electronics & Information Engineering, Tongji University, Shanghai 201804, China)[1]
(School of Information & Engineering, Huzhou Teachers College, Huzhou 313000, China)[2]

Abstract To resolve the problem of inauthentic files, this paper proposed a security P2P sharing model (SPSM). To incentive all the nodes sharing its resources, this paper introduced virtual currencies in SPSM; and introduced a prosecutive rules in SPSM, that is some nodes would prosecute a node which uploaded an inauthentic files, then CA (certification authorities) would put the malicious node into malicious sets when validating the identity of malicious node, to save the storage spaces, and considing the character of SPSM, this paper used DBF, the variants of Bloom Filter, to store the malicious sets in SPSM. To validate the validity of SPSM, this paper compared the performances of SPSM and Trust model, the results of experiments show that the performances of SPSM are more effective than Trust's.

Keywords Peer-to-Peer, Network security, Bloom filter

1 相关工作

对等网(P2P)是一种新型的基于应用层的通信和计算模型,是一种基于现有物理网络结构的覆盖网络(overlay),具有负载均衡性、可扩展性、鲁棒性、容错性和自组织性等特性。这些特性虽然为用户提供了便捷性,但同时使 P2P 易于传播虚假文件,从而导致恶意入侵、网络攻击等安全隐患。当前,为解决 P2P 中的虚假文件问题主要采用信誉模型,该模型通过 P2P 系统中的各个节点间的交互,采用一系列的方法来评价每个节点,从而为以后的节点间交互提供判断的依据。

信誉模型主要包括以下种类。

集中式信誉模型:在集中信誉管理中,存在少数中心节点,由中心节点负责整个网络的监督,如 eBay 的用户反馈系统[1]。

基于角色的信誉模型:如文献[2]中节点依据其兴趣,加入不同的社区。社区是拥有共同兴趣的节点集合,同一个节点可以加入不同的社区。依据节点对于不同社区的隶属程度,决定其在不同方面的可信度。

全局信誉模型:每个 peer 通过与其它 peers 交互,形成自己的局部信誉。系统收集这些局部信誉,计算全局信誉,如 Eigentrust[3] 就是用这种方法来得到全局的信誉值。

基于贝叶斯网络[4]模型:每个节点为所有与其交互过的节点建立一个贝叶斯网络(BN)。通过 BN,请求者可根据自己关心的内容,计算服务提供者的可信概率。每种概率表达了 peer 在某一方面的可信度。

基于神经网络的信誉模型:它的基本思路是通过神经网络聚合多个局部名誉来近似得到全局名誉[5]。

现有信誉模型中,由于给每个节点都给出了一个全局或局部的信誉值,当需要下载文件时,选择高信誉值节点作为源节点进行下载,这就导致了一个问题,即对等网中信誉值高的节点的负载量过大,这有违我们建立对等网的初衷。另一个问题是现有计算信誉值的方法中,对提供虚假文件下载的处

到稿日期:2009-06-05 返修日期:2009-09-23 本文受国家自然科学基金项目(60573183,60872057,60803053),浙江省自然科学基金杰出青年团队项目(R1090244),浙江省自然科学基金项目(Y107293,Y1080212),浙江省科技计划项目(2008C21083),湖州市科技攻关项目(2008GG11)资助。

严华云(1972-),男,博士生,副教授,CCF 会员,主要研究方向为对等网和网络安全等,E-mail:yanhy123@gmail.com;关佶红(1969-),女,博士,教授,博士生导师,CCF 高级会员,主要研究方向为空间数据库、分布计算、信息检索、地理信息系统及应用等。

理不严厉，一般仅仅当成了一次不成功的下载。为了避免这些问题的出现，本文提出了一种新的模型。

本文针对对等网安全内容共享问题做出的主要工作如下：

①将网络中提供虚假文件的节点区别于其它由于能力或网络的原因而导致不成功下载的节点，对这种提供虚假文件的恶意节点进行举报；在举报模型中，需要一个或几个中心节点作为 CA(Certification Authorities)来处理举报，CA 要管理密钥对$\langle PK_n, RK_n\rangle$的分发；CA 将被举报并确认的恶意节点集传送给网络中每一个节点；

②为了节省网络带宽和节点的匿名性，本文引入 Bloom Filter 的变体 DBF，以存放这种恶意节点集；

③为了解决对等网中搭便车(free-riding)问题，将资源标以虚拟价格(文中简单将文件大小定为其价格)，引入虚拟货币(VC)，以激励对等网中节点提供上传。

2 安全 P2P 共享模型 a

安全 P2P 共享模型(Security P2P Sharing Model，简称 SPSM)分为两部分：

对提供虚假文件的节点实行举报。具体来说就是采用 PKI 机制。当节点下载到虚假文件，则对下载源进行举报，恶意节点集合由专门的一个认证中心(Certification Authority，CA)管理。为了节省网络带宽和节点的匿名性，将恶意节点集合元素映射到 Bloom Filter 中，然后对恶意集合里的节点进行管制。即节点下载时不选择恶意集合中的节点，或者以后其它节点严厉地都不给恶意节点提供下载。

针对对等网中 Free-riding 问题，本文引入了虚拟货币，以便激励网络中的节点共享出自己的资源。

2.1 节点加入

在 SPSM 中，节点首先需加入到该 P2P 网络，然后利用自己的 P2P 网络中的 ID 号向认证中心(CA)进行注册，由 CA 分发给该节点一个密钥对$\langle PK_n, RK_n\rangle$，用于以后的认证。同时，CA 还要分给该节点一定量的初始货币，以保证该节点可以在该网络中下载文件。节点的具体加入过程如算法 1 所示。

算法 1 SPSM 中节点加入算法

1. 在对等网中找一任意节点 m；
2. N. join(m)；//具体见文献[6]的加入算法(figure7)；
3. 节点 N 发送一个消息到 CA 注册；
4. CA 分发给节点 N 密钥对(PK_n, RK_n)；
5. CA 分发给节点 N 一定量的虚拟货币。

该节点加入算法为了满足 SPSM，在 Chord 的节点加入算法的基础上引入了 PKI 的密钥分发和虚拟货币 VC。

2.2 选择下载源

在对等网中，同一个资源可能有多个副本。如何选择下载源，是需要考虑的问题。在信誉系统中，主要由信誉值决定源节点的选择；而在 SPSM 中，选择源节点由能够提供的带宽和网络距离等决定。具体实现需要给源节点一个评分，以决定选择源节点(优先选择得高分的节点)。节点 i 给源节点 j 的具体评分如式(1)所示：

$$Score(i,j)=\alpha\frac{Bw(j)}{Ccn(j)+1}+\beta\frac{1}{dis(i,j)} \quad (1)$$

Score(i,j)表示节点 i 给源节点 j 的评分。式中的参数意义见表 2。式(1)第一部分表示连接上源节点如果均分带宽可以分到的带宽，下载源能够提供的带宽越大越好；式(1)第二部分表示节点 i 和源节点的物理距离，物理距离越近越好。源节点选择算法如算法 2 所示。

算法 2 SPSM 中源节点选择算法(下载 File i)

1. 节点 ID(m)计算 File i 的哈希值 HFi=Hash(File i)；
2. 在对等网中用值 HFi 查找到节点 ID(j)；
3. 在 ID(j)中，将拥有文件 File i 的节点数组 ListFi[n](共 n 个节点)返回给 ID(m)；
4. i=0，optimalNode=−1；
5. ListFi[i]如在 BloomFilter 中，转第 7 步，否则转第 6 步；
6. 根据式(1)，若 ListFi[i]的得分高于 optimalNode，则 optimalNode= ListFi[i]；
7. 若 i≥n，转第 8 步；否则 i=i+1，转第 5 步；
8. return optimalNode. // optimalNode 若为−1 表示没找到下载源

当然，当一个文件比较大时，通常在对等网中采用的是分块下载，这时只要将每一块看成一个文件，利用算法 2 进行源节点的选择即可。

2.3 举报模型

在所有信誉(Trust)系统中，由于恶意节点可以在获得较高的信誉值后偶尔上传虚假文件，却几乎不会影响其信誉值；更有甚者，恶意节点之间可能会勾结组成一个恶意集，以提高恶意节点的信誉值；同时，在这种系统中，要不断地计算信誉值，这为系统带来了额外的负载。基于上述原因，本文建立了完全不同于信誉系统的安全 P2P 共享模型(SPSM)。其中最重要的是建立举报机制，即发现某一节点上传虚假文件，立即进行举报，并将这种恶意节点放入一个装载恶意集的 Bloom Filter 中，进而可以考虑对恶意节点进行惩罚(如降低其带宽，甚至不为其提供共享)；当节点选择下载源时，先从 Bloom Filter 中查看所选节点是否为恶意节点，以避免向恶意节点进行下载。举报模型如图 1 所示。

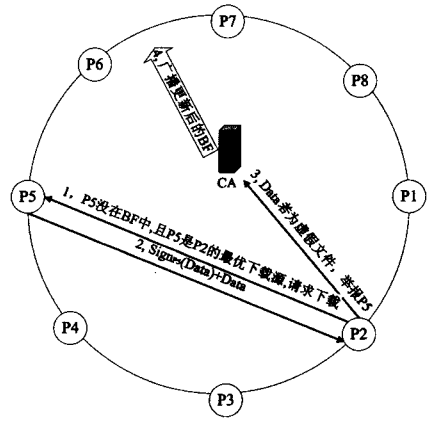

图 1 举报模型(其中 BF 表示 Bloom Filter，Sign$_{P5}$(Data)表示某节点 P5 对资源数据 Data 的签名)

SPSM 中举报过程如下：

①当某节点 P2 根据算法 2 发现拥有资源 Data 的最优源节点 P5 时，首先查看 P5 是否在 Bloom Filter 中。若不在 Bloom Filter 中，就向 P5 节点请求下载资源 Data；否则，选次最优节点进行刚才过程，直至找到源节点或查找失败。

②节点 P5 首先对所提供下载的资源数据 Data 用自己的私钥 RK$_{P5}$ 对其签名(Sign$_{P5}$(Data))，然后将签名和资源数据

一并上传给节点 P2。

③节点 P2 下载完毕后，检查该资源数据 Data 的真伪性。如果发现 P5 节点提供了虚假文件，则将数据 Data 并其签名举报到 CA。

④CA 接收到举报后，用 P5 的公钥对 P5 的签名进行验证。确认其上传了虚假文件后，将其加入保存恶意节点集的 Bloom Filter(为了匿名和减少网络流量)中。Bloom Filter 每次增加节点后，就对该网络进行一次广播。对凡是被放进该恶意节点集的节点实行惩罚(这类似于现实生活中的情况)，例如一段时期(或一直)不对恶意节点集中的节点提供下载；本文考虑到维持对等网的稳定性，采用的仅是不向恶意节点下载。在该举报机制中采用 PKI 机制，是为了防止中间节点的篡改和源节点的抵赖。

当共享资源的容量比较大时，为了解决向认证中心 CA 举报时带来较大的网络流量，可以对共享资源的哈希值采用 PKI 的机制，用以解决流量问题。这种解决方式需要对等网络中的每一个新的共享资源都要到 CA 上进行登记注册。

2.4 激励模型

为了抑制对等网中搭便车(Free-riding)问题，本模型中采用的激励方式为当前大多数共享网站类似的处理方式，即以虚拟货币的方式来促进对等网中各个节点贡献自己的资源。其原理如图 2 所示，具体步骤如下。

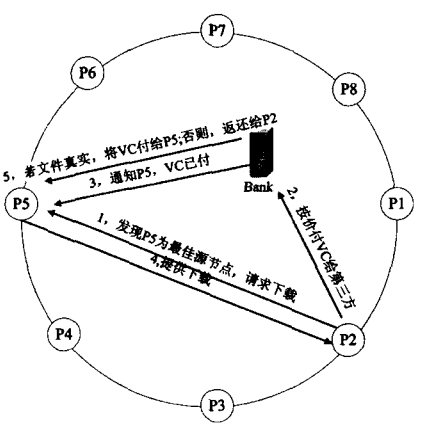

图 2 激励模型(其中 VC 表示 Virtual Currencies)

①当某节点 P2 根据算法 2 发现 P5 为最佳下载源时，向其请求下载 Data；

②节点 P2 将虚拟货币 VC 付给可信第三方 Bank；

③Bank 通知节点 P5 已收到节点 P2 的 VC，节点 P5 开始为 P2 提供下载；

④节点 P5 向 P2 提供下载；

⑤若此次下载不存在虚假文件问题，Bank 则将 VC 付给节点 P5，否则将 VC 返还给节点 P2。

其中，Bank 节点可以是图 1 的举报模型中的 CA 节点，也可以是专门的一个或多个节点，其作用是管理网络中节点的虚拟货币。

采用虚拟货币的机制能够有效避免信誉机制中的团体虚假评价的问题。

至于激励模型的实现细节，首先确定模型中的资源的价格，本文简单地采用资源的大小作为价格的大小。对于初始虚假货币的数量，可以根据实际情况确定，主要是要求能够保证整个网络系统的流通问题。对于网络中多个节点同时向一个节点请求下载时，可以考虑连接数量的限制和评价分配带宽的办法。

3 Bloom Filter 及其参数选择

Bloom Filter[7]是一种空间效率很高的随机数据结构。它利用位数组很简洁地表示一个集合，并能以一个高概率判断一个元素是否属于这个集合。其具体的工作原理是：为了表达 $S=\{x_1,x_2,\cdots,x_n\}$ 这样一个 n 个元素的集合，Bloom Filter 使用 k 个相互独立的哈希函数(Hash Function)，它们分别将集合中的每个元素映射到 $\{1,\cdots,m\}$ 的范围中。对任意一个元素 x，第 i 个哈希函数映射的位置 $h_i(x)$ 就会被置为 $1(1\leqslant i\leqslant k)$。注意，如果一个位置多次被置为 1，那么只有第一次会起作用，后面几次将没有任何效果。

Bloom Filter 的这种高效是有一定代价的：在判断一个元素是否属于某个集合时，有可能会把不属于这个集合的元素误认为属于这个集合，这种情况称为“错误率”(false positive)。因此，Bloom Filter 不适合那些“零错误”的应用场合。而在能容忍低错误率的应用场合下，Bloom Filter 通过极少的错误换取了存储空间的极大节省。

3.1 Bloom Filter 的选择

自从 Bloom Filter 被提出以来，有关学者考虑到其应用背景的不同而对 Bloom Filter 进行了一些改进。如提出 CBF[8]，以解决网络应用环境下的压缩问题；由于传统 Bloom Filter 只能往里面增加元素，不能从中删除元素，DCF[9]将 Bloom Filter 的每位扩展成多位，以解决集合中元素删除问题；由于传统 Bloom Filter 事先要大致确定集合元素的个数，为了解决集合的元素不断增加(没有减少的情况)的问题，国防科技大学提出的 DBF[10]采取的办法是先用一个能处理较少元素的 Bloom Filter 进行处理。当此 Bloom Filter 达到能够处理元素的极限时，再生成一个和初始 Bloom Filter 长度相同的 Bloom Filter。新元素映射到最新生成的 Bloom Filter 中，在几个子 Bloom Filter 同时进行查询。关于 Bloom Filter 及其一些变体更详细的介绍可以参考文献[11]。

选 Bloom Filter 的时候，考虑到本系统中恶意节点集的元素个数 n 不确定，并且系统采用的是发现一个恶意节点就插入到 Bloom Filter 中，这个过程只有元素的增加，不需删除元素，因此 SPSM 中选用 DBF 作为本文的 Bloom Filter。其详细内容参考文献[10]。

3.2 确定哈希函数个数

假设全集中共有 u 个元素，允许的最大错误率为 ε，X 为全集中任取 n 个元素的集合，$F(X)$ 表示 X 的 Bloom Filter。那么对于集合 X 中任意一个元素 x，在 $s=F(X)$ 中查询 x 都能得到肯定的结果，即 s 能够接受 x。显然，由于 Bloom Filter 引入了错误，s 能够接受的不仅仅是 X 中的元素，还能够接受 $\varepsilon(u-n)$ 个错误元素。因此，对于一个确定的 Bloom Filter 来说，它能够接受总共 $n+\varepsilon(u-n)$ 个元素。在 $n+\varepsilon(u-n)$ 个元素中，s 真正表示的只有其中 n 个元素，所以一个确定的 Bloom Filter 可以表示为 $\binom{n+\varepsilon(u-n)}{n}$ 个集合。m 位的 Bloom Filter 共有 2^m 个不同的组合，进而可以推出，m 位的 Bloom Filter 可以表示为 $2^m\binom{n+\varepsilon(u-n)}{n}$，而全集中可以表示的 n 个

元素的集合个数为$\binom{u}{n}$，为了让 m 位的 Bloom Filter 能够表示任意 n 个元素的集合，应该有：

$$2^m\binom{n+\varepsilon(u-n)}{n}\geqslant\binom{u}{n} \tag{2}$$

由式(2)可得：

$$m\geqslant\log_2\frac{\binom{u}{n}}{\binom{n+\varepsilon(u-n)}{n}}\approx\log_2\frac{\binom{u}{n}}{\binom{\varepsilon u}{n}}\geqslant\log_2\varepsilon^{-n}$$

$$=-n\log_2\varepsilon \tag{3}$$

对于使用 k 个哈希函数，向 m 位长的 Bloom Filter 中装入 n 个元素后位向量中某一位仍然为 0 的概率 p 为：

$$p=(1-\frac{1}{m})^{kn}\approx e^{-\frac{kn}{m}} \tag{4}$$

则错误率 fp 为：

$$fp=[1-(1-\frac{1}{m})^{kn}]^k\approx(1-p)^k=e^{k\ln(1-p)}$$

$$=e^{-\frac{m}{n}\ln p\ln(1-p)} \tag{5}$$

在式(5)中，令 $g=-\frac{m}{n}\ln p\ln(1-p)$。根据对称性法则可知，当 $p=\frac{1}{2}$ 时，g 取最小值，则 fp 取最小值。

错误率 fp 最小的条件为：

$p=\frac{1}{2}$，即 $e^{-\frac{kn}{m}}=\frac{1}{2}$

因此有：

$$k=\ln 2\cdot(\frac{m}{n}) \tag{6}$$

并且有：

$$fp=(\frac{1}{2})^k=(\frac{1}{2})^{\frac{m}{n}\ln 2}\approx(0.6185)^{\frac{m}{n}} \tag{7}$$

由式(3)和式(6)推出：

$$k=\ln 2\cdot(\frac{m}{n})\geqslant-\ln 2\cdot\log_2\varepsilon \tag{8}$$

式中，当 $\varepsilon=0.01\%$ 时，k 大于等于 9.21034037。由此可知，为了保证用 m 位的 Bloom Filter 表示任意 n 个元素的集合，哈希函数个数 k 为 10 时是近似的最优个数。本文在实验部分采用 10 个哈希函数。

另一方面，为了理解各个参数对错误率的影响，表 1 列出了标准 Bloom Filter 中各个参数和错误率之间的关系。

表 1　标准 Bloom Filter 中各参数和错误率的关系表

m/n	8	10	12	13	14	16
k	6	7	8	9	10	11
错误率 fp	0.0216	0.0082	0.0031	0.0019	0.0012	0.00046

从表 1 可以看出，当 $k=10$ 时，其错误率为 0.0012012，这已经能够满足我们对错位率的要求。

从上面两方面分析得出，标准 Bloom Filter 中采用 10 个哈希函数是比较合适的。

而 DBF 是多个标准 Bloom Filter 的拼接，因此上述推导对 DBF 而言也是适用的。因此实验中的 DBF 采用了 10 个哈希函数。

4　仿真及结果分析

本文从以下两个方面进行了实验：一是系统中的负载均衡问题，一是系统中下载的虚假文件率问题。

4.1　实验参数说明

模拟 SPSM 时，考虑到实现的方便性，采用了 Chord 的 P2P 结构，并在 peersim[12] 的 Chord 基础上实现了 SPSM，采用其中的轮转周期模型(cycle-based model)。其中涉及的相关参数，如表 2 所列。

表 2　SPSM 中各种参数的设置

参数	参数说明
N(nodeNumber)	对等网中节点个数(设为 100)
Bw(bandWidth)	节点的带宽(设为 10)
Mcn(maxConNumber)	节点的最大连接数(设为 5)
Ccn(currentConNum)	节点的当前连接数
VC(virtual currencies)	节点当前的虚拟货币量(初值设为 150)
uploadedSize	节点提供的上传流量
Mp(maliciousPercent)	恶意节点比例(默认设为 0.1)
fileNumber	初始文件个数(设为 10，分布在任意 10 个节点上)
C(cycles)	轮转周期数(设置为 8)
α，β	式(1)中两部分的系数，分别设为 0.9 和 0.1
fileSize(cost)	每个文件的大小(价格)(在 20～40 之间均匀分布)
dis(i,j)	节点 i,j 间的物理距离(简单起见，设其等于 overlay 上的距离)

4.2　负载均衡

系统中负载均衡实验如图 3 所示。

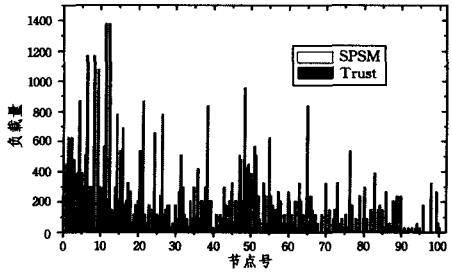

图 3　各节点的负载量

图 3 表示各个节点的负载量情况。SPSM 表示本文的安全 P2P 共享模型，Trust 采用的是基于信誉的模型。从图 3 中可以看出，Trust 中少数节点的负载非常大，而有不少的节点完全没有提供下载，这和真实对等网环境下的统计结果是一致的，即少数节点承担了大量的负载，大多数节点都 Free-riding；而 SPSM 中各个节点的负载量更均匀些，出现零负载量的节点更少。

SPSM 负载更均匀的原因是选择下载源的机制不同：在 Trust 中，选择下载源的时候选择节点信誉值较高的节点进行下载，这样容易导致信誉值高的节点更长时间提供下载，从而其信誉值更高。这样不断重复，从而导致少数节点在网络中的下载量占有整个网络的下载量的决定部分；在 SPSM 中，由于不用考虑信誉值，选择下载源的时候考虑的是带宽的问题，选择连接数较少的从而能够提供更高带宽的节点作为下载源，这样就不至于让少数的节点来承担更多的下载量。

4.3　虚假文件率

下载的虚假文件比实验如图 4 所示。

图 4 表示虚假文件率随系统中恶意节点比的变化曲线。从图 4 中可以看出，Trust 系统中当恶意节点率超过 40%时，虚假文件率急剧上升，这说明在 Trust 系统中恶意节点对系统的影响是很大的(此处显示 Trust 的虚假文件率比文献[3]的要高，其原因是轮转周期 C 选得较小，从而总的下载次数较小)；相反，在本文提出的 SPSM 系统中，随着恶意节点比率

的不断增大，虚假文件率基本上没有多少影响。

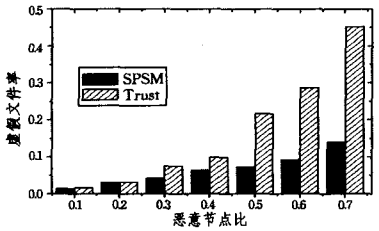

图 4　下载虚假文件率随恶意节点比变化图

SPSM 中虚假文件率更低的原因是系统中采用了举报机制。由于当一个恶意节点为其它节点提供了虚假文件后，该恶意节点会被举报，从而其它节点不会再从该恶意节点进行下载。而本系统中设置了每个节点的最大连接数 Mcn，因此每个恶意节点最多能够提供 Mcn 次虚假文件上传，对于有 N 个节点的网络中，当恶意节点比例为 Mp 时，在该网络中最大的虚假文件上传次数(uploading times of maximum inauthentic files，简写为 $Tmif$)为：

$$Tmif=N*Mp*Mcn \tag{9}$$

而总的下载次数(total downloading times，简写为 Tdt)为：

$$Tdt=N*C \tag{10}$$

因此 SPSM 中最大虚假文件率(inauthentic file ratio，简写为 Ifr)为：

$$Ifr=\frac{Tmif}{Tdt}=\frac{N*Mp*Mcn}{N*C}=\frac{Mp*Mcn}{C} \tag{11}$$

从式(11)可以看出，SPSM 中最大虚假文件率随恶意节点的比例 Mp 的变大而变大，随最大连接数 Mcn 的变大而变大，随轮转周期 C 的变大而变小。从图 4 来看，其 Mcn 为 5，C 为 8。由于 Mp 的量级更小，因此随着 Mp 的变大虚假文件率基本没多大影响。在该系统中，可以通过提高轮转周期数 C 来进一步降低虚假文件率，即在一个长期存在 SPSM 中其虚假文件率可以更低。

总之，SPSM 比基于信誉的系统的虚假文件率更低。

结束语　本文提出的 SPSM(安全 P2P 共享模型)是基于举报机制的，即一经发现恶意节点即对其进行举报，从而避免其它节点向该恶意节点进行下载；同时采取虚拟货币购买文件的方式，以激励网络中节点上传文件；系统中节点通过提供上传文件以挣取 VC，从而保证以后下载文件有足够的虚拟货币。实验显示 SPSM 具有较好的性能。

参 考 文 献

[1] Resnick P, Zeckhauser R. Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system [M]. Advances in Applied Microeconomics, 2002, 11: 127-157

[2] Li N, Mitchell C J, Winsborough W H. Design of a role-based trust management framework [C] // Proc. of the 2002 IEEE Symp. on Security and Privacy. Washington, USA, 2002

[3] Kamvar S D, Schlosser M T, Garcia-Molina H. The EigenTrust Algorithm for Reputation Management in P2P Networks [C]// Proc. of WWW. Budapest, Hungary, 2003

[4] Wang Yao, Vassileva J. Bayesian Network - based Trust Model [C]// Proc. of IEEE/WIC International Conference on Web Intelligence. Halifax, Canada, 2003

[5] Song Weihua, Phoha V V. Neural network-based reputation model in a distributed system [C]// Proc. of IEEE 2004 CEC. San Diego, California, USA, 2004

[6] Stoica I, Morris R, Karger D, et al. Chord: A scalable peer-to-peer lookup service for internet applications[C]// Proc. of SIGCOMM. SanDiego, California, USA, 2001

[7] Bloom B. Space / Time trade - offs in hash coding with allowable errors[J]. Communications of the ACM, 1970, 13(7): 422-426

[8] Mitzenmacher M. Compressed Bloom Filters [J]. IEEE/ACM Transactions on Networking, 2002, 10(5): 604-612

[9] Aguilar-Saborit J, Trancoso P, Muntes-Mulero V. Dynamic Count Filters[C]// Proc. of SIGMOD. Chicago, USA, 2006

[10] Guo Deke, Wu Jie, Chen Honghui, et al. Theory and Network Applications of Dynamic Bloom Filters[C]// Proc. of IEEE INFOCOM. Barcelona, Spain, 2006

[11] Broder AMitzenmacher M. Network applications of bloom filters: A survey[J]. Internet Mathematics, 2005, 1(4): 485-509

[12] peersim [EB/OL]. http://peersim.sourceforge.net/

(上接第 52 页)

[2] 梁坚，敖青云，尤晋元. 安全协议的时限责任分析 [J]. 电子学报，2002，10：35-39

[3] 黎波涛，罗军舟. 不可否认协议时限性的形式化分析[J]. 软件学报，2006，17(7)：1510-1516

[4] Coffey T, Saidha P. Logic for verifying public-key cryptographic protocols[J]. IEEE Proc Computers and Digital Techniques, 1997, 144(1): 28-32

[5] Kudo M, Mathuria A. An Extended Logic for Analyzing Timed-Release Public-Key Protocols[J]. ICICS, 1999: 183-198

[6] 范红，冯登国. 一种分析 Timed-release 公钥协议的扩展逻辑 [J]. 计算机学报，2003，22：832-838

[7] Bieber P. A logic of communication in hostile environment[C]// Proceedings of the Third IEEE Computer Security Foundations Workshop. Franconia, New-Hampshire: IEEE Computer Society Press, 1990: 14-22

[8] 毛晨晓，罗文坚，王煦法. 分析安全协议密码系统相关缺陷的模态逻辑方法[J]. 小型微型计算机系统，2006，27(7)：1223-1228

[9] Zhou J, Gollmann D. A fair non-repudiation protocol[C]// Proc. of the 1996 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 1996: 55-61

[10] Kim K, Park S, Baek J. Improving fairness and privacy of Zhou-Gollmann's fair non-repudiation protocol[C]// Gong K, Niu Z, eds. 2000 IEEE Int'l Conf. on Communication. Beijing: IEEE Computer Society Press, 2000, 3: 1743-1747