文章编号:1001 - 9081(2006)11 - 2578 - 05

RAP2P:一种基于资源广告的非结构化 P2P 系统

罗绪成,耿 技,刘 峤
(电子科技大学 计算机科学与工程学院,四川 成都 610054)
(xucheng@uestc.edu.cn)

摘 要:研究了非结构化 P2P 系统的数据管理和相应的资源查询算法。提出了基于资源广告的非结构化 P2P 系统,即 RAP2P。设计了一种类似谣言传播机制的资源信息广告算法 AdGossip 来传播共享资源广告,并且通过共享资源广告缓存限制机制来保证局部区域缓存空间对共享资源节点的最大覆盖率。分析和模拟结果表明,在获得 100% 查询命中率的条件下,RAP2P 的资源定位消息开销约为泛洪查询的 25%,查询的时延为泛洪查询的 30% ~50%,并且远远低于 k-random walks。

关键词:非结构化 P2P;资源定位;资源广告;谣言传播;Bloom 过滤器
中图分类号: TP393 **文献标识码**:A

RAP2P: a resource advertising-based unstructured P2P system

LUO Xu-cheng, GENG Ji, LIU Qiao
(*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan* 610054, *China*)

Abstract: The data management and resource locating algorithms of unstructured P2P system were studied. The proposed system was called RAP2P. The system simulated the marketing behavior, and shared the resource of advertised information to improve the resource locating performance. A gossiping-based resource advertising algorithm was proposed to propagate the resource information. By constraining the caching of resource information, the 2-hop search space stored the largest percent of all information. To exploit such resource layout, a dynamic shadow flooding search algorithm was presented. The analysis and simulation show that RAP2P requires about 25% message overhead of flooding algorithm and 30% to 50% query delay of flooding algorithm with 100% query hit rate, and its query delay is also far below that of k-random walks.

Key words: unstructured P2P; resource locating; resource advertising; gossip propagation; Bloom filter

0 引言

Gnutella 网络是一种非结构化 P2P 网络,节点之间的连接是随机的,共享资源和节点之间没有确定的关系,因此,最初的查询方式是基于泛洪的查询算法。由于基于泛洪的查询算法盲目地向邻居节点转发查询请求,这些查询请求中存在大量的冗余查询请求,造成大量的网络开销,特别是在网络规模扩大的情况下,这种现象更为严重。虽然泛洪查询的效率较低,但是泛洪查询能够穷尽搜索系统中的所有节点,因此所得的结果是最好的。为了解决基于泛洪查询的 Gnutella 网络可扩展性差的问题,提出了多种改进方案,主要目的是降低资源定位的消息开销。Edith Cohen 等从数据管理方面出发,提出了多种复本策略来提高 Gnutella 网络的查询性能[1]。Qin Lv 等采用综合的方法来提高非结构化 P2P 网络的资源定位性能,研究了 P2P 网络的拓扑结构特点、复本策略和相应的查询算法,提出了扩展环、k-random walks 算法来提高非结构化 P2P 网络的查询性能[2]。Christos Gkantsidis 等组合现有的解决方案,如 flooding,random walks,look ahead 查询机制和复本策略来解决非结构化 P2P 系统的性能优化问题[3]。另一种解决 Gnutella 网络可扩展性问题的方案是将网络中的节点划分为超级节点和叶子节点,后者与一个或者多个超级节点相连,并将共享资源在所连接的超级节点上作索引,由超级节点代理其叶子节点完成资源定位的功能。在这种体系结构中,由于叶子节点不参与资源定位的消息路由功能,因此,降低了消息路由网络的规模,从另一个角度降低了 Gnutella 网络的可扩展性要求。虽然上述解决方案提高了 Gnutella 网络的某些主要性能指标,如查询的成功率和查询时延等,但是都不能得到与泛洪查询相近的查询结果。最近的测量研究表明 P2P 文件共享系统中存在大量的污染文件[4],声誉机制是解决该问题的方法之一,需要对查询结果进行排等级,因此,查询的命中率越高,声誉机制越有效。为了快速下载大文件,用户需要多源并行下载支持,因此,需要提供优质(如高带宽等)节点选取的功能,同样需要对查询结果进行排等级。总之,如果需要获得更好的共享性能,P2P 共享系统需要得到泛洪查询的结果,同时又需要降低泛洪查询的消息开销,即高命中率、低时延、低消息开销。

现有的 P2P 共享系统中,资源定位基本是通过传播查询请求来完成的。为了获得好的查询结果,需要系统中每个节点均能够接收到该查询请求,因此,基于泛洪的查询算法成为 Gnutella 网络的基本查询算法。这种资源定位方式可以看作是查询请求广告模式,即向所有节点广告自己的需求,但是这种方式只能为查询的发起者服务。相反地,如果共享资源的节点广告自己所共享的资源,则这种信息能够为系统中所有节点服务,降低资源定位的开销。

本文提出一种基于共享资源广告的非结构化 P2P 系统(Resource Advertising-based unstructured P2P, RAP2P)。通过

收稿日期:2006 - 08 - 22 **基金项目**:国家自然科学基金资助项目(60473090,60573129)
作者简介:罗绪成(1974 -),男,四川彭州人,博士研究生,主要研究方向:分布式系统、对等计算、网络安全; 耿技(1963 -),男,安徽合肥人,教授,主要研究方向:计算机网络、信息安全; 刘峤(1974 -),男,四川成都人,博士研究生,主要研究方向:信息安全、分布式计算.

所设计的广告信息发布算法将资源广告分布到系统中的不同节点。RAP2P 中的每个节点分配一个缓存空间用于存储资源广告信息。通过适当的控制算法,使得在每个节点的局部(2-hop)范围内,具有较高的广告信息覆盖率。在这种资源布局的条件下,资源定位能够在局部范围内完成,既提高了资源查询的命中率,同时降低了资源查询的时延。

1　RAP2P 的系统结构

RAP2P 中,每个节点共享多个文件或者共享文件数目为零。为了提高共享资源的查询性能,每个节点广告其共享的资源并且缓存所接收到的一定数量的共享资源广告。通过适当的控制策略,保证共享资源广告的合理分布及其新鲜性,提高资源查询的性能。对每个节点来说,该节点和其 k-hop(k =2 或者 3)范围内的节点构成一个局部范围(Local Domain,LD)。一个 LD 中的所有节点的缓存的总和构成一个大的存储空间 LDC(Local Domain Cache)。每个节点缓存所接收到的广告信息,并且在其 LD 中的节点之间限制所存储广告信息的差异性,即最大程度限制在一个 LDC 中不存在多份相同的广告信息。为了降低广告信息的存储开销和传输所需的网络带宽,RAP2P 采用 Bloom Filter[5](简称 BF)来表示节点的共享资源。为了保证共享资源广告的快速传播和新鲜性,RAP2P 设计了基于谣言传播机制的广告算法进行共享资源广告信息的维护,即 AdGossip。在广告信息达到良好分布的情况下,每个 LDC 保存了尽可能多的共享资源广告,达到较大的广告覆盖率。通过一个 LDC 泛洪查询,就能够达到较高的共享资源节点命中率,2 个 LDC 泛洪查询通常能够达到 100% 的节点覆盖率,获得高命中率、低时延和低消息开销的系统性能。RAP2P 的系统结构如图 1 所示。

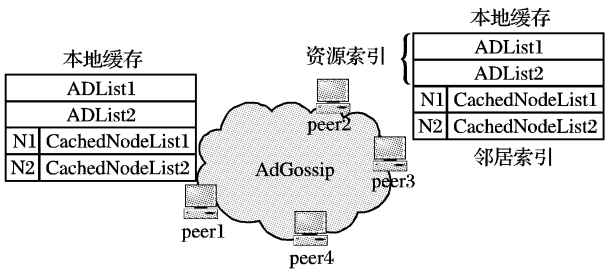

图 1　RAP2P 的系统结构

1.1　资源广告

共享资源的节点向其他节点广告自己的资源信息需要解决两个问题,广告信息的构造和广告信息的传播与缓存。系统中的节点传播广告信息,满足条件的节点缓存所接收到的广告信息,因此,需要紧凑的广告消息表示方法,既能减少存储的空间,又能够降低传播的网络带宽需求。在大规模、动态网络中,资源广告需要能够合理分布到某些节点,最终形成的资源布局具有在小范围内,高覆盖率的特征。

节点所共享资源的集合用 BF[6,7] 表示。BF 是一种空间有效的随机化数据结构,用于表示一个集合,并支持集合的成员关系查询。BF 采用长度为 m 的比特向量 V 来表示一个集合。设所要表示的集合为 $S = \{s_1, s_2, \cdots, s_n\}$。初始化时,向量 V 中的每一位均设为 0。选取 k 个相互独立的哈希函数 $H = \{h_1, h_2, \cdots, h_k\}$,且满足 $h_i \in \{0, 1, 2, \cdots, m-1\}$。集合的表示算法和成员查询算法分别为算法 1 和 2。根据算法 1 和 2,比特向量中被置为 1 的位置的 k-组合可能大于插入的成员数,因此,可能造成误称(false positive),即某个元素不属于集合 S,但是被错误地认为属于集合 S。假设所有的哈希函数是完全随机的,在 $k = \ln 2 \cdot (m/n)$ 的条件下,这种误称率可以近似表示为 $f = (1/2)^k \approx (0.6185)^{m/n}$。在很多应用中,适度小的误称概率不会给系统的功能和性能带来负面影响,反而能够明显提高系统的性能。根据具体的需求,所要求的误称概率可以通过对参数 n, m, k 的调节来达到。在 RAP2P 系统中,采用 BF 来描述节点所共享的资源的集合,结合节点的身份(如 IP 地址)等其他信息构成该节点的资源广告信息。以这种方式来构造资源广告,能够大量减少传输的网络带宽和相应节点的缓存空间。

算法 1

```
Bit_string BF_present( S, H )
  For( int i =1; i <| S |+1; i ++)
  {
    For( int j =1; j <| H |+1; j ++)
    V [ h_j ( x_i ) ] =1;
  }
  Return V;
```

算法 2

```
Boolean BF_membership( V, x )
  For( int j =1; j <| H |+1; j ++)
  {
    If V [ h_j ( x ) ] =0
    then Return FALSE;
  }
  Return TRUE;
```

Gossiping 算法是对社会群体中谣言传播方式的模拟,每个节点周期性地与随机选取的系统成员(一个或者多个)交换信息,从而在达到适度开销的条件下快速传播信息。该算法常用于解决网络系统中的通信和计算问题,主要包括复本维护[8]、消息传播[9~11]、成员关系维护[12]等。由于 Gossiping 算法能够适应网络的动态变化,并且在大规模网络计算中,以相对较小的消息开销能够获得较高的性能指标,因此,RAP2P 采用一种基于 Gossiping 的算法来进行共享资源广告的传播,即 AdGossip 算法。本文假定随机的成员选择[13~15]是已经具有的基本服务,RAP2P 系统建立在该服务的基础之上。通过 AdGossip 算法,节点广告自己的共享资源信息,这种共享资源广告具体表示为:ID:BF:tm:ttl,其中 ID 为该广告信息属主的 ID 号,BF 为共享资源信息的 BF 表示,tm 为该广告信息创建的时间戳,ttl 为该广告信息的生命期。采用 AdGossip 算法,经过一定的 Gossiping 轮数,共享资源广告能够在整个系统中快速分布。另一方面,为了保证共享资源分布的合理性,还需要节点对共享资源广告的存储的限制机制。在 RAP2P 中,每个节点除了存储共享资源广告,还需要保存邻居节点所缓存的节点列表,以此来保证 LDC 中共享资源广告的最大覆盖率。根据所获得的资源分布模式,资源定位能够通过 2-hop 泛洪查询达到对共享资源节点的较大覆盖率,提高资源定位的性能。RAP2P 中节点的数据结构如图 1 所示,每个节点分配一个缓存空间,用于存放共享资源广告和其邻居所缓存的节点摘要。共享资源广告索引分为两类,分别用列表 ADList1 和 ADList2 来存储。ADList1 为新发布广告列表,如果一个广告信息在当前的 LDC 中第一次出现并且该广告的广告生命期尚未结束(ttl >0),则被当前 LDC 中的节点视为新广告,需要进行 AdGossip 操作;ADList2 为旧广告列表,如果一个广告信息在当前 LDC 中第二次出现或者该广告信息的生命期结束(ttl =0),则该广告被视为旧广告,当前 LDC 对其免疫,该广告被插入到 ADList2,并从 ADList1 删除,不再进行 AdGossip 操作。

P2P 文件共享系统是一个不断动态变化的系统,在运行过程中节点自主地加入和退出系统,下面对这些行为进行分别说明。

节点初始化 分配缓存空间,如果当前节点无共享文件,则缓存空间为空;如果有共享文件,则生成当前节点的共享资源索引广告。

节点加入系统 采用 Gnutella 协议规定的算法来获取邻居节点,加入到网络中,同邻居节点交换邻居信息,启动 Active thread 和 Passive thread。

节点意外退出系统 由于节点意外退出,造成所广告的资源信息失效,这种失效只有在该节点被访问时才能够检测到,RAP2P 系统对这种失效不进行特别处理,当检测到这种情况时,删除 LDC 中失效节点的广告信息。

节点正常退出系统 在正常退出的情况下,为了维护 LDC 的覆盖率,节点执行退出操作,随机分发本地缓存的表项给邻居节点,并通知邻居节点删除退出节点的表项。

在节点加入系统后,需要周期性地进行共享资源维护操作,即运行 AdGossip 算法进行共享资源的广告。AdGossip 算法的 active thread 和 passive thread 分别为算法 3 和 4。

算法 3

```
AdGossip: Active thread
  do forever
  wait t time_unit;
  {
    for (int i=0; i<ADList1.length; i++)
    {
      r←random_select_peer();
      ADList1[i].ttl--;
      push(r, ADList1[i]);
    }
  }
```

算法 4

```
AdGossip: Passive thread
do forever
AD←waitMessage();
if (AD in LDC)
then
  Update_LDC(AD);
else if LDC not full then
{
  if(AD.ttl! =0)
  then
    Add_LDC_ADList1(AD);                    //insert into ADList1
  else
    Add_LDC_ADList2(AD);
}
else
{
  r←Select_Random_Peer();
  push(r, AD);
}
Update_LDC(AD)
{
  If (AD is the same as Stored_AD)
  then
    Immune(AD);   //当前 LDC 中的缓存节点不再 gossip 此 AD
  else if (AD.tm > Stored_AD.tm) then
  {
    Remove_LDC(AD);                         //删除旧的 AD
    Insert_LDC(AD);     //将新的 AD 插入到空闲的 ADList1 中
  }
```

1.2 资源定位

在 RAP2P 系统中,由于在一个 LDC 中,已经保证了较大的节点覆盖率,因此采用 2-hop 泛洪查询算法就能够保证较大的命中率。另一方面,由于每个节点缓存空间大小的限制,如果系统中的广告信息过多,就不能够保证 1-LDC 对系统中所有共享资源节点的覆盖,因此,可能存在 1-LDC 搜索无法找到系统中存在资源的情况。RAP2P 采用动态反馈查询算法,即动态浅层泛洪查询资源定位算法(Dynamic Shadow Flooding Query,DSFQ)来解决该问题。在 DSFQ 中,节点首先进行本地 2-hop 浅层泛洪查询操作,根据反馈信息,如果对这次搜索算法的结果不满意,则随机选择一个系统成员,后者代理前者作本地浅层泛洪操作。一般情况下,最多操作 2 次就能够达到对共享资源节点的高概率覆盖。

2 RAP2P 的性能评估

2.1 RAP2P 的性能分析

非结构化 P2P 系统 RAP2P 所构成的网络用图 $G=(V,E,R)$ 表示,其中 V 为节点集合,$|V|=n$;$E=V\times V$ 为边的集合,$|E|=m$;R 为系统中所共享资源的集合,$R=\bigcup_{i=1}^{n}R_i$,R_i 为某个节点所共享的资源的集合。对任意节点 $v\in V$,$\Gamma(v)$ 表示节点 v 的邻居节点集合,$|\Gamma(v)|=d$。以节点为索引,采用 BF 来描述节点所共享的资源集合,即 R_i 用 BF_i 表示,则系统中节点共享的资源可以采用 $ID_i:BF_i:tm_i:ttl$ 为表项的列表 L 来描述。从列表 L 中选取表项,并将这些表项缓存到不同的节点,这就是资源广告过程。

对于同一 Gnutella 网络,如果不采用基于广告的资源管理算法,要达到 100% 的命中率,有效的查询算法是泛洪查询。如果查询消息的生命期设为 T,则一个资源定位的消息开销为 $M_F=\sum_{i=0}^{T}d^i$,查询时延为 $D_F=T$,通常 $T=6$ 或者 7。采用 k-random walks 进行查询,如果 $k=1$,根据 random walks 在覆盖一个图的时间为 $C_G\leqslant 2m(n-1)$,则定位一个资源的消息开销为 $M_R\leqslant 2m(n-1)$,查询时延为 $D_R\leqslant 2m(n-1)$。

在 RAP2P 网络中,采用 AdGossip 算法进行共享资源信息的传播,在 n 个节点的网络中,AdGossip 算法收敛的时间为 $O(\log n)$,但是并不需要达到收敛的 Gossiping 轮数,广告信息在网络中就有很好的分布,则 AdGossip 算法对一个广告信息进行传播所需要的消息开销为 $M_G\leqslant\sum_{i=0}^{\log n}2^i$。如果有 x 个查询命中该广告信息,则分摊到一个查询的广告成本为 M_G/x。在 RAP2P 网络中,查询通常在 2-hop 的邻居范围内完成,则一个查询所需的消息开销为 $M_A=M_G/x+\sum_{i=0}^{2}d^i$,查询时延为 $D_A=2$。RAP2P 系统中的其他维护开销相对很小,并且是为整个共享过程服务,因此,可以不计入一个查询所需的消息开销。

根据上述分析,显然 D_A 介于 $30\%D_F$ 和 $50\%D_F$ 之间。在规模为 90000 节点的网络中,设 $d=5$,$x=10$,则:$M_A=M_G/x+\sum_{i=0}^{2}d^i\leqslant 26246$,$M_F=\sum_{i=0}^{6}5^i=97656$,因此 $M_A\approx 25\%M_F$。实用的 k-random walks 中,通常 k 在 16 ~ 64 时能够获得好的查询结果[5]。k-random walks 的消息开销在系统模拟中进行分析。

根据所设计的广告信息分布算法,系统中的共享资源广告信息分布到系统中不同的节点进行缓存,通过这种方法来优化共享资源信息在系统中的分布。假设系统中有 r 个节点共享资

源,则需要 r 个广告信息来描述共享资源。如果每个节点缓存的表项的最大长度为 l,则 LDC 中至少需要 r/l 个节点才能够完全覆盖整个共享资源广告。由 $r/l = \sum_{i=0}^{h} d^i$ 可得:$l = r/\sum_{i=0}^{h} d^i$。对于 $n = 90000$ 的网络,如果 $h = 2$, $d = 5$,假设有 1/2 的节点共享资源,则缓存空间的大小 $l \approx 1452$,就可以获得接近 100% 的查询命中率。如果一个广告信息的存储空间大小为 1K 字节,则缓存空间的大小约为 2M 字节就可以满足需求,而这种空间开销对当前的个人电脑来说,是很小的开销。节点还可以根据自己的功能强弱,设定缓存空间的大小,高性能节点可以缓存更多的广告信息,功能较低的节点可以减小缓存空间的大小,还可以通过激励机制鼓励节点共享缓存空间。

2.2　系统模拟与结果分析

Peersim 是一个大规模 P2P 系统的模拟平台,其灵活的框架支持开发各种 P2P 系统的模拟程序,已用于多个 P2P 算法的性能评估[13]。因此,采用 Peersim 来模拟所设计的算法。在模拟过程中,所需要分析的量包括 AdGossip 的收敛规律和 RAP2P 系统的资源定位性能。

模拟过程分别在不同规模的幂率随机图上进行,采用了 10 000,30 000,50 000,70 000,90 000 个节点的网络规模。用 Brite 拓扑生成器生成相应的拓扑数据。RAP2P 系统不考虑优化的复本算法,因此不需要相应的复本维护开销。系统中只考虑自发的复本配置情况,采用随机分布的方式配置复本,分别模拟了复本量为 1, 2, 3, …, 10 的配置情况。

2.2.1　AdGossip 的收敛规律和参数确定

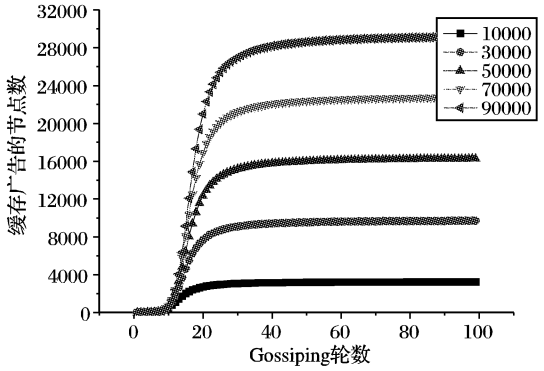

图 2　节点的收敛趋势

首先,不考虑 ttl 对广告消息的传播限制,观察分析 AdGossip 的广告信息传播效果。采用同步的模拟方式,在一轮中,具有广告信息的节点只进行一次广告信息转发操作。分析经过多少轮之后,被广告的资源在系统的节点中有较好的分布和相应的消息收敛情况,轮数分别为 1, 2, 3, …, 100 等。随机选择 50% 的节点具有共享资源,在共享资源广告的每一轮中观察具有广告信息的节点数。同时,在每一轮中,观察该轮中所传播的广告消息。节点的收敛趋势如图 2 所示。根据图 2,在 20 轮时,具有广告信息的节点基本保持稳定,而且这些具有广告信息的节点的数量约为网络规模的 1/3,即对于一个资源广告来说,如果系统中 1/3 节点知道该广告信息,则系统中的每个节点均可以通过其所在的 LDC 知道该资源广告。上述无 ttl 限制的广告传播算法所需的消息开销比较大,广告信息在系统中的分布密度也比较大,降低了缓存空间的利用率。考虑 ttl 限制的情况,在消息广告的同时进行资源查询操作,该过程如图 3 所示。当 Gossiping 轮数在 10 至 15 之间时,在模拟所给定的几种网络规模中,命中率达到 100%。因此,在实际系统中,可以根据网络的规模设定 ttl,降低资源广告的消息开销,同时提高缓存空间的利用率。

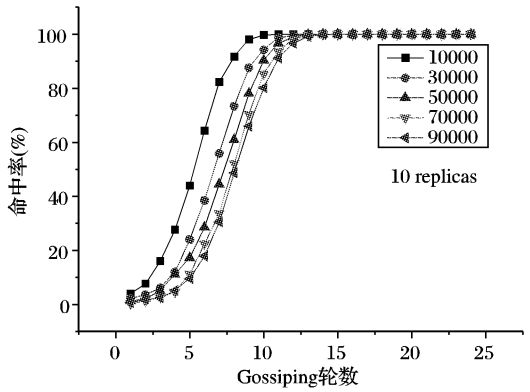

图 3　查询命中率与 Gossiping 轮数

2.2.2　消息开销和查询时延的对比

RAP2P 系统的运行过程中所产生的消息量包括 AD 广告的消息量、1-LDC 查询的消息量和 LDC 的维护消息量。因为一个广告信息通常包括了多个文件,而且这个广告可以为多个查询服务,因此,计算在一个资源查询请求中所占的消息开销为 M_A/k,其中 k 与一个广告中所描述的资源数和该广告被命中的次数有关。LDC 的维护消息通常比较小,并且用于系统运行的整个过程中,因此可以忽略。模拟的结果如图 4 和图 5 所示。在查询命中率较低的条件下,RAP2P 的消息开销低于泛洪,高于 k-random walks;查询命中率增高的条件下,RAP2P 的消息开销低于 k-random walks,远低于泛洪查询。RAP2P 的查询时延低于泛洪查询,而 k-random walks 的查询时延远高于泛洪和 RAP2P,因此,没有在图中标出。

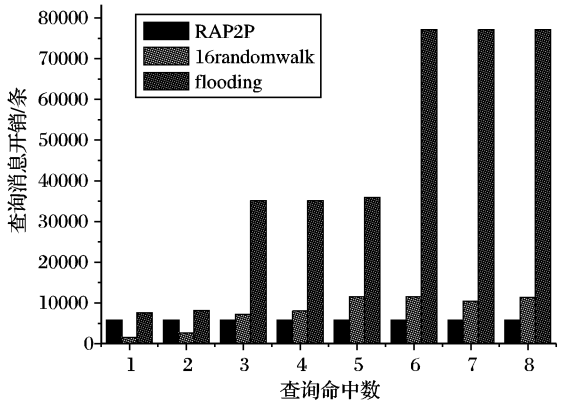

图 4　查询命中率与查询消息开销

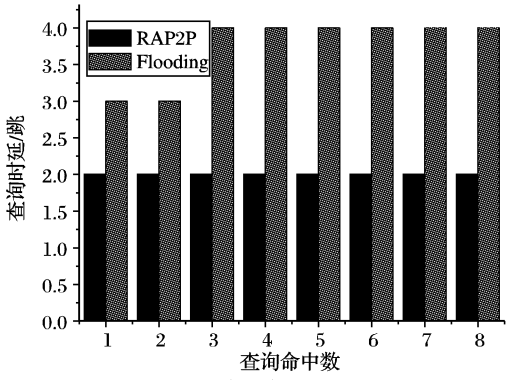

图 5　查询命中率与查询时延

3　结语

RAP2P 通过资源广告的方式达到共享资源信息在整个共享网络中的合理分布,每个节点和其直接邻居的缓存空间

所构成的局部区域缓存中保存了尽可能多的广告信息。AdGossip 算法保证了共享资源广告信息的快速传播和新鲜性。根据共享资源管理算法所形成的共享资源布局设计了动态浅层泛洪查询的资源定位算法,节点首先进行本地 2-hop 泛洪查询请求,如果对查询结果不满意,可以再次执行查询操作,节点随机选择一个系统成员,该成员代理前者执行本地 2-hop 查询请求泛洪。分析和模拟结果均表明:RAP2P 对非结构化 P2P 系统的资源定位性能有较大提高,能够在低消息开销和低查询时延的条件下,获得与泛洪查询接近的查询结果。

参考文献:

[1] COHEN E, SHENKER S. Replication strategies in unstructured peer-to-peer networks[A]. ACM SIGCOMM[C]. New York: ACM Press, 2002. 177 - 190

[2] LV Q, CAO P, COHEN E, *et al.* Search and replication in unstructured peer-to-peer networks [A]. Proceedings of the 16th international conference on Supercomputing (ICS'02) [C]. New York: ACM Press, 2002. 84 - 95.

[3] GKANTSIDIS C, MIHAIL M, SABERI A. Hybrid search schemes for unstructured peer-to-peer Networks[A]. Proceedings of the INFOCOM[C]. New York: IEEE Computer and Communications Societies, 2005. 1526 - 1537.

[4] LIANG J, KUMAR R, XI Y, *et al.* Pollution in P2P file sharing systems[A]. Proceedings of the INFOCOM[C]. New York, USA: IEEE Computer and Communications Societies, 2005. 1174 - 1185.

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

[6] BYERS JW, CONSIDINE J, MITZENMACHER M, *et al.* Informed content delivery across adaptive overlay networks[J]. IEEE/ACM Transactions on Network Parallel Distributed Systems, 2004, 12(5): 767 - 780.

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

[8] AGRAWAL D, ABBADI AE, STEINKE RS. Epidemic algorithms in replicated databases (extended abstract)[A]. Proceedings of the Sixteenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems[C]. New York, USA: ACM Press, 1997. 161 - 172.

[9] MOSK-AOYAMA D, SHAH D. Information dissemination via gossip: applications to averaging and coding[EB/OL]. http://arxiv.org/abs/cs.NI/0504029, 2005.

[10] KERMARREC A-M, MASSOULIÉL, GANESH AJ. Probabilistic reliable dissemination in large-scale systems[J]. IEEE Transactions on Parallel Distributed Systems, 2003, 14(3): 248 - 258.

[11] JUN S, AHAMAD M, JUN XU. Robust information dissemination in uncooperative environments[A]. Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)[C]. Washington, DC, USA: IEEE Computer Society, 2005. 293 - 302.

[12] GANESH AJ, KERMARREC A-M, MASSOULIÉ L. Peer-to-peer membership management for gossip-based protocols[J]. IEEE Transactions on Computers, 2003, 52(2): 139 - 149.

[13] JELASITY M, GUERRAOUI R, KERMARREC A-M, *et al.* The peer sampling service: experimental evaluation of unstructured gossip-based implementations[A]. Proceedings of the 5th ACM/IFIP/USENIX international conference on Middleware[C]. New York, USA: Springer-Verlag, 2004. 79 - 98.

[14] AWAN A, FERREIRA RA, JAGANNATHAN S, *et al.* Distributed uniform sampling in unstructured peer-to-peer networks[A]. Proceedings of the 39th Annual Hawaii International Conference on System Sciences [C]. Washington, DC, USA: IEEE Computer Society, 2006. 223.

[15] GANESH AJ, KERMARREC A-M, MASSOULIÉ L. SCAMP: peer-to-peer lightweight membership service for large-scale group communication [A]. Proceedings of the Third International COST264 Workshop on Networked Group Communication (NGC'01) [C]. London, UK: Springer-Verlag, 2001. 44 - 55.

(上接第 2577 页)

$Z_{n^2}^*$ 上的 n 次剩余问题是困难的条件下,Paillier 加密体制具有很好的安全性能。

3.2.3 执行效率分析

从 3.1 协议描述可知,协议在执行过程中,如果议价失败共需要进行 4 轮通信和 5 次 Paillier 加密算法的加/解密运算;如果议价成功共需要 6 轮通信和 7 次 Paillier 加密算法的加/解密运算,协议的通信复杂度和计算复杂度均为常数阶。因此适合于较大数值的秘密比较,具有很好的实用性。

4 结语

本文提出的基于加同态公钥加密体制的两方议价协议,是高效的实用安全多方计算协议研究工作的组成部分之一。该协议具有较高的执行效率,其通信复杂度和计算复杂度均为常数阶,因此该协议在电子商务中具有较好的实用价值。除了 Paillier 加密算法,其构造方法也适用于其他的加同态公钥加密体制。

参考文献:

[1] GOLDREICH O. Secure Multi-Party Computation(Draft, Version 1.4)[EB/OL]. http://www.wisdom.weizmann.ac.il/ oded/pp.html, 2002.

[2] YAO AC. Protocols for Secure Computations[A]. 23rd IEEE Symposium on Foundations of Computer Science (FOCS)[C], 1982.160 - 164.

[3] GOLDREICH O, MICALI S, WIGDERSON A. How to Play Any Mental Game[A]. 19th Annual ACM Symposium on Theory of Computing[C]. New York: ACM Press, 1987. 218 - 229.

[4] GOLDREICH O, MICALI S, WIGDERSON A. Proofs That Yield Nothing About Their Validity -or- All Languages in NP Have Zero-Knowledge Proof Systems[J]. Journal of the ACM, 1991, 8(1): 691 - 729.

[5] FISCHLIN M. A Cost-Effective Pay-Per-Multiplication Comparison Method for Millionaires[A]. RSA Security 2001 Cryptographer's Track at RSA Conference, LNCS2020[C], 2001. 457 - 471.

[6] SCHNEINIER B. Applied Cryptography: Protocols, Algorithms, and Source Code in C[M]. 2nd ed. New York: John Wiley & Sons, 1996. 334 - 340.

[7] PAILLIER P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes[A]. STERN J, ed. Eurocrypt'99, LNCS 1592[C]. Berlin: Springer-Verlag, 1999. 223 - 238.

[8] BRESSON E, CATALANO D, POINTCHEVAL D. A Simple Public Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications [A]. LAIH CS, ed. Asiacrypt 2003, LNCS2894[C]. Berlin: Springer-Verlag, 2003.37 - 54.

[9] CATALANO D, GENNARO R, GRAPHAMN H. The Bit Security of Paillier Encryption Scheme and Its Applications[A]. Advances in Cryptology - Eurocrypt'01, LNCS2045[C]. Berlin: Springer-Verlag, 2001.229 - 243.

[10] CRAMER R, SHOUP V. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption[A]. Advances in Cryptology - Eurocrypt'02, LNCS 2332[C]. Berlin: Springer-Verlag, 2002.45 - 94.