隐私保护的不同坐标系两点距离计算

王涛春 罗永龙 左开中 杜安红
(安徽师范大学数学计算机科学学院 芜湖 241003)

摘 要 坐标系变换是合作完成某项测绘作业过程中经常遇到的问题,但因为关系到自身的安全与利益,合作双方都不希望泄露各自的输入信息。首次提出保护私有信息的坐标系变换问题,同时设计了相应的变换协议,并以此协议为基础,进一步设计了不同坐标系下两点距离计算协议,分析了两协议的正确性、安全性及复杂性。在保护私有信息的条件下,解决了不同坐标系下两点距离计算问题,并将其应用到目标定位准确性判断问题中。

关键词 多方安全计算,坐标变换,两点距离
中图法分类号 TP309 **文献标识码** A

Privacy-preserving Distance Measure of Different Coordinates

WANG Tao-chun LUO Yong-long ZUO Kai-zhong DU An-hong
(College of Mathematics and Computer Science, Anhui Normal University, Wuhu 241003, China)

Abstract Coordinate transformation is a problem which can be frequently encountered during cooperatively completing certain surveying and mapping work. However, as related to their own security and interests, the partners do not want to disclose their input. The paper first proposed privacy preserving coordinate transformation and designed corresponding transformation protocol. Based on the above protocol, a protocol for Distance Measure of Different Coordinates was developed and the two's correctness, security and efficiency were analyzed further. In preserved privacy, the problem of privately determining polygonal similarity was successfully solved in the paper, which was also applied to the judgment of target positioning accuracy.

Keywords Secure multi-party computation, Coordinate transformation, Distance measure

1 引言

随着网络技术的发展,不同机构或部门合作完成某项测绘作业变得越来越普遍和便捷,而在合作过程中经常存在着坐标系变换问题[1,2]。例如在目标定位上,合作双方都希望参考对方的数据来判断定位的准确性,但双方探测出的目标数据是相对于自己的距离与方位,即合作双方采用不同的坐标系。因此,为了完成合作,计算双方涉及如何统一坐标系以及对双方的数据进行相应处理的问题。然而由于关系到自身的安全与利益,任何一方都希望在完成合作的同时不向对方泄露自身坐标体系和目标点坐标数据等信息。如何保证双方在合作完成该类任务的同时不向对方泄露自身的任何信息是一个亟待解决的问题。

上述问题是一类特殊的安全多方计算(Secure Multi-party Computation, SMC),是由 Yao 在文献[3]中首次提出的,后来 Goldreich 等进一步推广了这个问题[4]。虽然理论上已经有一些解决该问题的通用方法,但这些方法应用到具体的例子中,在计算效率上是不可行的[5]。对于具体问题需要研究具体的解决方案,因此,高效实用的安全多方计算协议是当前研究的热门课题[6-10]。上面提出的问题,即为在保护隐私的情况下,判定探测的目标坐标数据是否准确,这类问题也称为保护隐私的计算几何(Privacy-Preserving Computational Geometry, PPCG),由文献[7]首先提出。本文首次提出了秘密进行坐标系转换并设计了相应的协议,基于该协议,设计了不同坐标系下的两点距离计算协议,再利用已有的秘密比较协议判定两点距离与某个设定值之间的大小关系,从而解决在不泄露自身信息的情况下评定探测的目标坐标数据的准确性等问题。

2 预备知识

假设参与各方都处于半诚实模型下,所提出的协议主要用到加法同态加密技术和秘密技术,先给出这几个基本概念和问题的定义。

定义 1(半诚实模型) 要求参与各方能够严格、正确地执行协议,不会中途强行退出协议或恶意输入虚假信息,但他们可能会保留能收集到其他参与方的所有信息,并期望通过这些信息推断出其他参与方的输入信息。半诚实模型适用于很多实际的应用环境,所以对半诚实模型下安全协议的研究

到稿日期:2010-09-25 返修日期:2010-12-07 本文受国家自然科学基金项目(60703071),安徽省自然科学基金项目(070412043)资助。
王涛春(1979—),男,硕士,讲师,主要研究方向为安全多方计算、移动计算,E-mail:taochunwang@gmail.com;罗永龙(1972—),男,博士,教授,主要研究方向为信息安全、可信计算、安全计算;左开中(1974—),男,博士,副教授,主要研究方向为可信计算、信息安全、三值光计算机;杜安红(1972—),男,硕士,讲师,主要研究方向为科学计算可视化、可信计算。

是有意义的，且任何半诚实模型下的安全多方计算协议均能够转换成恶意模型下的协议[5]。

定义 2(加法同态加密) 同态加密是一种在不需要解密的情况下，可以允许直接对密文进行操作的加密变换技术。$E(\cdot)$和$D(\cdot)$分别表示加密和解密，k为公钥，x、y为明文，如果根据密文$E(x)$和$E(y)$可以直接计算出$E(x+y)$，即当且仅当$E_k(x)\otimes E_k(y)=E_k(x+y)$时，称其为加法同态加密。同时，根据加法同态加密特性可得出对于任何n有$E(nx)=E(x)^n$成立[11]。

定义 3(秘密比较) 秘密比较是指计算双方在不泄露自己私有输入信息的情况下判断出双方输入数据的大小关系。即假设 Alice 与 Bob 各有一个私有数据，计算双方希望秘密比较这两个私有数据的大小关系。Yao 在文献[3]中提出了一个趣味的“百万富翁”问题，并给出了一个比较大小问题的协议。文献[12]给出了一个有效且公平的比较大小的协议。文献[7]设计了一个基于可交换的双重加密方案的比较相等的协议。文献[13]提出了一个基于 Φ-HA 及同态加密方案的无信息泄漏的秘密比较协议。

3 坐标系变换协议

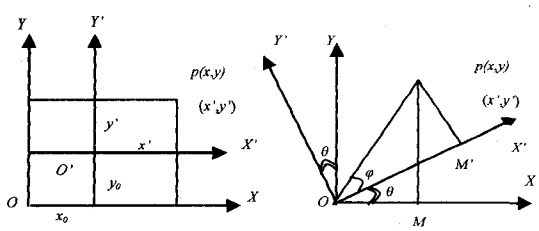
在计算几何中，若计算双方采用不同的坐标系，则进行各种运算之前需要对这两个不同的坐标系进行变换，使计算几何中的对象在同一坐标系下进行运算。本节提出并设计了隐私保护的坐标系转换协议，即计算双方在不泄露自己坐标系信息的情况下，实现坐标系的转换，使计算双方的几何对象在同一坐标系下进行运算。

3.1 有关坐标系转换的基础知识

本文讨论的是平面的坐标变换，平面上一般的坐标变换可视为平移与旋转两种坐标变换连续进行的结果，平移指的是两坐标系XOY和$X'O'Y'$的坐标轴有相同的方向，那么容易得出平面上任一点P在坐标系XOY中的坐标(x,y)和在坐标系$X'O'Y'$中的坐标(x',y')之间的关系为式(1)，如图 1(a)所示。旋转指的是坐标原点O相同，将x轴和y轴绕坐标原点O同时旋转角度θ得到的一新坐标系$X'OY'$(不失一般性，是按逆时针旋转，下同)，那么平面上任一点P的新、旧坐标之间的关系为式(2)，如图 1(b)所示。

$$\begin{cases}x=x'+x_0\\ y=y'+y_0\end{cases}\quad\begin{cases}x'=x-x_0\\ y'=y-y_0\end{cases}\tag{1}$$

$$\begin{cases}x=x'\cos\theta-y'\sin\theta\\ y=x'\sin\theta+y'\cos\theta\end{cases}\quad\begin{cases}x'=x\cos\theta+y\sin\theta\\ y'=-x\sin\theta+y\cos\theta\end{cases}\tag{2}$$



(a) 坐标系平移　　(b) 坐标系旋转

图 1

3.2 坐标系变换

Alice 有私有坐标系$X_aO_aY_a$，Bob 有私有坐标系$X_bO_bY_b$，双方希望在不向对方泄露自身信息的同时，实现两坐标变换，使计算几何中的对象在同一坐标系下进行运算。

Alice 与 Bob 将X_a、X_b轴分别绕点O_a、O_b旋转角度θ_1、θ_2得到新坐标系$X_a'O_aY_a'$和$X_b'O_bY_b'$，使得新坐标系$X_a'O_aY_a'$和$X_b'O_bY_b'$的坐标轴有相同的方向，这时只需要平移即可转换为同一坐标系，即利用坐标平移变换公式得出坐标系$X_a'O_aY_a'$和$X_b'O_bY_b'$的平移量，其中 Alice 得到式(3)，其中v_1，v_2是 Bob 选取的随机数，同时满足：①Alice 不能从坐标转换公式中得到坐标系$X_bO_bY_b$的信息；②Bob 不能得到坐标变换公式，也不能得到任何坐标系$X_aO_aY_a$的信息。坐标系变换协议描述具体如下：

$$\begin{cases}x'=x_a'-(x_b'+v_1)\\ y'=y_a'-(y_b'+v_2)\end{cases}\tag{3}$$

协议 1　坐标系转换协议

Alice 有私有坐标系$X_aO_aY_a$，Bob 有私有坐标系$X_bO_bY_b$，Alice 得到两坐标系变换式(3)，其中(x_a',y_a')和(x_b',y_b')分别是平面上同一个点在新坐标系$X_a'O_aY_a'$和新坐标系$X_b'O_bY_b'$中的坐标，$(x'+v_1,y'+v_2)$是两新坐标系$X_a'O_aY_a'$和$X_b'O_bY_b'$的位移量，这里v_1，v_2是 Bob 选取的一个随机数。

Step1　Alice 与 Bob 共同选择相同的两点P_1、P_2，由于 Alice 与 Bob 采用不同的坐标体系，因此P_1、P_2在两个坐标系有不同的坐标，如图 2(a)所示，旋转 Alice 与 Bob 的坐标系，使得 Alice 与 Bob 的坐标系的X轴都与直线P_1P_2平行，如图 2(b)所示，旋转的度数分别为θ_a和θ_b，根据旋转坐标变换公式分别得到 Alice 与 Bob 的坐标变换公式。

Alice 旋转坐标变换公式：

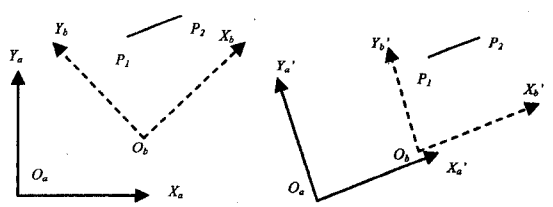
$$\begin{cases}x_a'=x_a\cos\theta_a-y_a\sin\theta_a\\ y_a'=-x_a\sin\theta_a+y_a\sin\theta_a\end{cases}\tag{4}$$

式中，(x_a,y_a)和(x_a',y_a')分别是同一个点在旧坐标系$X_aO_aY_a$和新坐标系$X_a'O_aY_a'$中的坐标。

Bob 旋转坐标变换公式：

$$\begin{cases}x_b'=x_b\cos\theta_b-y_b\sin\theta_b\\ y_b'=-x_b\sin\theta_b+y_b\sin\theta_b\end{cases}\tag{5}$$

式中，(x_b,y_b)和(x_b',y_b')分别是同一个点在旧坐标系$X_bO_bY_b$和新坐标系$X_b'O_bY_b'$中的坐标。



(a) 两坐标系$X_aO_aY_a$和$X_bO_bY_b$　(b) 旋转后的两坐标系$X_a'O_aY_a'$和$X_b'O_bY_b'$

图 2

Step2　Alice 与 Bob 分别根据式(4)、式(5)的坐标变换公式计算P_1在新坐标系$X_a'O_aY_a'$和$X_b'O_bY_b'$的坐标，Alice 与 Bob 分别得出P_1的坐标为$(x_a^{p_1},y_a^{p_1})$和$(x_b^{p_1},y_b^{p_1})$。

Step3　Bob 把坐标$(x_b^{p_1}+v_1,y_b^{p_1}+v_2)$发给 Alice。

Step4　Alice 得到

$$\begin{cases}x'=x_a^{p_1}-(x_b^{p_1}+v_1)\\ y'=y_a^{p_1}-(y_b^{p_1}+v_2)\end{cases}\tag{6}$$

3.3 协议分析

1)协议的正确性

定理 1　协议 1 是正确的。

证明：根据坐标系转换的基础知识可知 Alice 与 Bob 旋

转坐标系得到新坐标系后其点的坐标值也进行了相应的变换是正确的，旋转变换后其新坐标系的坐标轴具有相同的方向，又根据坐标平移变换式(1)将两个新坐标变换在同一坐标系下也是正确的。因此，协议1是正确的。

2)协议的安全性

定理2 协议1是安全的。

证明：

(1)Alice与Bob对坐标系进行旋转变换，转换的角度θ_1、θ_2双方是不知道的，因此计算双方不能通过新坐标系的坐标轴是同方向信息来推断对方原坐标系坐标轴角度的任何信息。

(2)Alice与Bob进行平移变换时，Alice得到式(6)，由于式(6)中有随机数v_1，v_2，Alice不能通过式(6)推断Bob坐标系原点位置的任何信息，Bob也不能得到任何Alice坐标系原点的任何信息。

综合(1)和(2)可知协议是安全的。

3)协议的复杂度

协议1中Alice与Bob通信1次，计算的代价为执行了2次坐标旋转变换1次坐标平移变换。

4 两点距离计算协议

两点之间的距离可以用公式$d=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}$来表示，其中$P_1(x_1,y_1)$和$P_2(x_2,y_2)$是同一平面下的两点。本节在坐标系转换协议的基础上，提出并设计了在保护自身信息的同时计算处于不同坐标系两点之间的距离。

4.1 问题描述

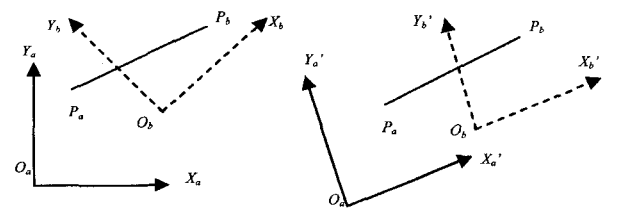
假设Alice在私有坐标系$X_aO_aY_a$下有坐标点$P_a(x_a,y_a)$，Bob在私有坐标系$X_bO_bY_b$下有坐标点$P_b(x_b,y_b)$，Alice与Bob在不泄露自身坐标系和点坐标信息的同时共同协作计算，Alice得到$u=|P_aP_b|^2+v$，其中v是Bob选取的随机数。

4.2 距离计算协议

Alice与Bob执行坐标系转换协议，使得他们各自坐标系的坐标轴有相同的方向，如图3所示，Bob得P_b的新坐标为(x_b',y_b')和随机值v_1，v_2，Alice得P_a的新坐标为(x_a',y_a')以及两新坐标系的位移式(7)，再通过坐标系平移变换公式把点P_a转换到新坐标系$X_b'O_bY_b'$中，设其坐标为(x_a'',y_a'')，则$x_a''=x_a'-x'-v_1$，$y_a''=y_a'-y'-v_2$，即$x_a'-x'=x_a''+v_1$，$y_a'-y'=y_a''-v_2$，最后利用平面两点之间距离公式使Alice得到$u=|P_aP_b|^2+v$，其中v是Bob选取的随机数。

$$\begin{cases} x'=x_{ab}-v_1 \\ y'=y_{ab}-v_2 \end{cases} \tag{7}$$

式中，x_{ab}和y_{ab}是两新坐标系$X_b'O_bY_b'$到$X_a'O_aY_a'$的实际平移量。



(a) 初始坐标系　　(b)x轴与直线P_aP_b平行的坐标系

图3

两点距离计算协议具体描述如下：

协议2 两点距离计算协议

Step1 Alice与Bob执行坐标系转换协议，P_a、P_b的坐标变换为(x_a',y_a')和(x_b',y_b')。

Step2 Alice随机产生一对同态加密的公钥私钥对(E,D)，并计算$E(x_a'-x')$，$E(y_a'-y')$。

Step3 Alice把E，$E(x_a'-x')$，$E(y_a'-y')$发送给Bob。

Step4 Bob选取两个随机数v_3，v_4，并计算$t=E(x_a'-x')^{(x_b'+v_1)}\cdot E(y_a'-y')^{(y_b'+v_2)}\cdot E(v_3)$

$u_1=(x_b')^2+(y_b')^2+2(v_1x_b'+v_2y_b')+v_1^2+v_2^2+v_4$，发送$t$，$u_1$给Alice。

Step5 Alice计算$u_2=D(T)$和$u=(x_a'-x')^2+(y_a'-y')^2-2u_2+u_1$，协议结束。

4.3 协议分析

1)协议的正确性

定理3 距离计算协议是正确的。

证明：

计算

$$\begin{aligned} t&=E(x_a'-x')^{(x_b'+v_1)}\cdot E(y_a'-y')^{(y_b'+v_2)}\cdot E(v_3)\\ &=E((x_a''+v_1)*(x_b'+v_1)+(y_a''+v_2)*(y_b'+v_2)+v_3) \end{aligned}$$

因此

$$\begin{aligned} u_2&=(x_a''+v_1)*(x_b'+v_1)+(y_a''+v_2)*(y_b'+v_2)+v_3\\ &=(x''x_b'+y''_ay'_b)+(x''_av_1+y''_av_2)+(v_1x'_b+v_2y_b')+v_1^2+v_2^2+v_3\\ u&=(x_a'-x')^2+(y_a'-y')^2-2u_2+u_1\\ &=(x''_a+v_1)^2+(y''_a+v_2)^2-2u_2+u_1(x_a'')^2+(y_a'')^2+2(x_a''v_1+y''v_2)+v_1^2+v_2^2\\ &=-2((x''x_b'+y_a''y_b')+(x_a''v_1+y_a''v_2)+(v_1x_b'+v_2y_b')+v_1^2+v_2^2+v_3)+(x_b')^2+(y_b')^2+2(v_1x_b'+v_2y_b')+v_1^2+v_2^2+2v_3+v_4\\ &=(x_a'')^2+(y_a'')^2-2(x''x_b'+y_a''y_b')+(x_b')^2+(y_b')^2+v_4\\ &=(x_a''-x_b')^2+(y_a''-y_b')^2+v_4 \end{aligned}$$

式中，(x_a'',y_a'')和(x_b',y_b')分别是点P_a和P_b在新坐标系$X_b'O_bY_b'$中的坐标，定理得证。

2)协议的安全性

定理4 协议2是安全的。

证明：

(1)Alice与Bob执行坐标系转换协议，由定理2知是安全的。

(2)Alice发送信息$E(x_a'-x')$，$E(y_a'-y')$给Bob，由于Bob不知道Alice的密钥D，因此Bob不能得出$x_a'-x'$，$y_a'-y'$信息。

(3)Bob发送t，u_1给Alice，由于有随机数v_3，v_4，因此Alice不能得到任何x_b'或y_b'的信息。

综合(1)、(2)和(3)可知协议是安全的。

3)协议的复杂度

协议2中Alice与Bob通信代价为交换信息3次。计算的代价为产生一对同态加密的公钥私钥对，加密3次，解密1次，1次模块化的乘法，2次坐标旋转变换，1次坐标平移变换。

通过两点距离计算协议得出不同坐标系两点之间的距离值，并用该值与合作双方设定的某个确定准确度阈值ϕ进行

比较，即 Alice 用值 u 与 Bob 的 $v4+\varphi$ 进行比较，如果 $u \leqslant v4+\varphi$ 则目标定位比较准确，否则准确度有待提高。

结束语 不同机构或部门合作完成某项测绘作业时经常需要对各自的坐标系进行转换，为了保证合作双方的安全与利益，双方都不希望泄露各自的输入信息。本文首次提出并设计了保护私有信息的坐标系变换协议，并在该协议的基础上设计了保护私有信息的不同坐标系两点距离计算协议。解决了在不向对方泄露自身私有信息的情况下计算不同坐标系两点之间的距离问题，并通过秘密比较得出两点距离与某个设定阈值 ϕ 的大小关系，从而解决了对目标定位准确性的判定问题。

参 考 文 献

[1] 刘宗泉，贾志强，邢诚，等. GPS 网 WGS-84 平差坐标向地方独立坐标转换[J]. 测绘信息与工程，2007，32(1)：33-35

[2] 雷伟伟，姜斌. 国家坐标系与城市坐标系转换方法的探讨[J]. 测绘科学，2010，35(1)：22-23

[3] Yao A C. Protocols for secure computation[C]// Proc. of the 23rd IEEE Symp. on Foundation of Computer Science. Chicago: IEEE Computer Society，1982：160-164

[4] Golderich O，Micali S，Wigderson A. How to play any mental game[C]// Proceedings of the 19th Annual ACM Symposium on Theory of Computing. New York，1987：218-229

[5] Goldreich O. Foundations of cryptography，basic applications [M]. Cambridge：Cambridge University Press，2004：233-278

[6] Du W L，Atallah M J. Privacy-preserving cooperative scientific computations [A]// Proceedings of the 14th IEEE Computer Security Workshop[C]. Nova Scotia，Canada：IEEE Computer Society Press，2001：273-82

[7] Mikhail J，Atallah，Du W L. Secure multi-party computational geometry[C]// Lecture Notes in Computer Science 2125. Berlin：Springer，2001：165-179

[8] Lindell Y，Pinkas B. Privacy preserving data mining [J]. Journal of Cryptology，2002，15(3)：177-206

[9] 罗永龙，黄刘生. 空间几何对象相对位置判定中的私有信息保护[J]. 计算机研究与发展，2006，43(3)：410-416

[10] Luo Yong-long，Huang Liu-sheng，Zhong Hong. Secure two-party point-circle inclusion problem[J]. Journal of Computer Science and Technology，2007，22(1)：88-91

[11] Paillier P. Public-key cryptosystems based on composite degree residuosity classes [A] // Advances in Cryptology—EUROCRYPT'99，Lecture Notes in Computer Science 1592 [C]. Springer-Verlag，1999：223-238

[12] Cachin C. Efficient private bidding and auctions with an oblivious third party[C]// Proc. of the 6th ACM Conf. on Computer and Communications Security. Assn for Computing Machinery，1999：120-127

[13] 秦静，张振峰，冯登国，等. 无信息泄漏的比较协议[J]. 软件学报，2004，15(3)：421-427

(上接第 57 页)

法降低$\frac{1}{2}$，经统计 ECAM 算法的通信开销能够比 CAM 算法节省 35%～48%。对于实际的大规模非结构化 P2P 网络，其节点开启发现算法的方式基本是间隔开启的状态，因此 ECAM 算法对通信开销的降低是非常有实际意义的，对提升 P2P 网络的可靠性与可用性有着很重要的帮助。

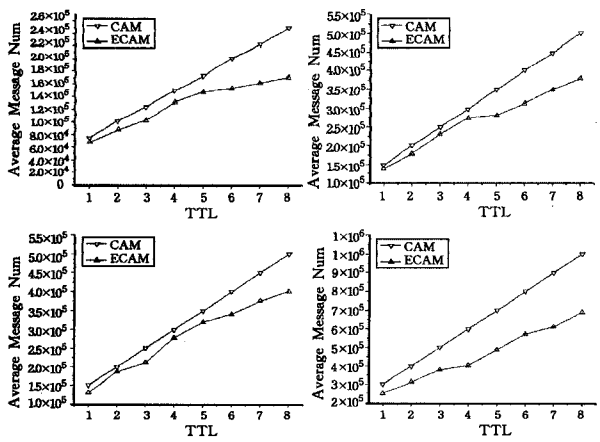


图 9 节点以 0.01s 的间隔依次开启发现算法时的通信开销

结束语 本文对非结构化 P2P 网络下的拓扑优化进行了研究，从拓扑网络中最薄弱的环节——拓扑关键点出发，深入探讨了拓扑关键点的发现算法与消除算法，为保证网络的可靠连通提供了有效手段。总结了非结构化 P2P 网络拓扑优化的研究现状与发展趋势，综述了拓扑关键点的相关技术和应用，分析了众多研究中存在的不足和主要问题。对 CAM 拓扑关键点发现算法进行仿真分析，针对其存在的发现效率低、网络消耗大的问题，提出基于扩展式 CAM 的拓扑关键点发现算法 ECAM，并对其进行模拟仿真。实验结果表明，ECAM 算法在保证发现准确率的同时，大大降低了网络消耗，提高了发现效率。且本算法可应用到实际网络中，与拓扑关键点的消除算法相结合，提高网络可靠性。

参 考 文 献

[1] Saroiu S，Gummadi P，Gribble S. Measuring and analyzing the *characteristics of napster and gnutella hosts*[M]. Multimedia Systems 9，Berlin：Springer-Verlag，2003：170-184

[2] Liu X，Xiao L，Kreling A，et al. Optimizing overlay topology by reducing cut vertices[C]// Proc. of the ACM Int'l Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV). Newport：ACM Special Interest Group on Multimedia. http://portal. acm. org/citation. cfm? id=137821 3&jmp=references&coll=ACM&dl=ACM，2006

[3] Chawathe Y，Ratnasamy S，Breslau L，et al. Making gnutella-like P2P systems scalable[C]// Proc. of the Annual Conf. of the Special Interest Group on Data Communication (SIGCOMM). Karlsruhe：ACM Special Interest Group on Data Communication，2003：407-418

[4] 任浩. P2P 覆盖网拓扑优化研究[D]. 长沙：国防科技大学，2007

[5] 李振华，陈贵海，邱彤庆. 分点：无结构对等网络的拓扑关键点[J]. 软件学报，2008(9)：2376-2388

[6] 冯国富，张金城，姜玉泉，等. 无结构 P2P 覆盖网络的拓扑优化[J]. 软件学报，2007(11)：2819-2829