级联加密技术及其在安全电子邮件中的应用

黄涵淇 刘明华 胡 健 尹燕伟 冯久超
(华南理工大学电子与信息学院 广州 510641)

摘 要 为了保护电子邮件传输的安全性,提出了一种级联加密的保密通信技术。基于预处理和量化处理对超混沌系统产生的序列进行了改进,改进后的序列通过了NIST随机性测试,具有更理想的相关性、更强的伪随机性及不可逆性。级联加密技术可发挥两者各自的优势,提高电子邮件传输的安全性。分析和应用表明了该级联加密系统的可靠性。

关键词 级联加密,电子邮件加密,超混沌序列,预处理,量化处理
中图法分类号 TP309 **文献标识码** A

Study on Application of Hyperchaotic Encryption Combined with 3DES in Secure E-mail System

HUANG Han-qi LIU Ming-hua HU Jian YIN Yan-wei FENG Jiu-chao
(School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China)

Abstract The security problem of email transmission on the Internet was considered. A scheme of cascade cipher based on improved hyperchaotic sequences combined with 3DES algorithm was proposed. Based on hyperchaotic system, the real chaotic sequences were pretreated and quantified. The improved sequences, which have stronger pseudo-random, better correlation and irreversible characteristics were validated by the NIST test. An example of email transmission using the cascade cipher system was presented to demonstrate its performance.

Keywords Cascade cipher, E-mail encryption, Hyperchaotic sequences, Pretreatment, Quantification

1 前言

随着计算机网络和通信技术的快速发展,越来越多的信息通过网络进行传输,因此确保通信双方的信息安全已成为愈来愈重要的问题。DES加密体制是目前在商业领域比较重要而流行的一种加密体制,它广泛应用于大量数据的保密传输、加密存储等应用场合。但DES算法的缺点是密钥较短(56位),随着计算机处理能力的不断提高,实时破译DES已经实现,为此人们提出了保密性能更好的3DES加密算法,使密钥扩展到112位。

混沌是指由非线性确定性系统产生的一种复杂类随机行为。利用混沌系统,可以产生数量众多、非相关、类似噪声、又可以再生的混沌序列,这种序列难以重构和预测,从而使密码分析者难以破译[1]。序列密码的安全性在很大程度上取决于伪随机序列的随机性。混沌序列密码实际上是利用混沌映射产生一个混沌序列,然后使用该混沌序列和明文做某种可逆运算,比如做异或运算,从而完成加密[2]。最近的理论研究结果表明,用相空间重构技术,可以推测出低维混沌系统的性质与特征。要增强系统的抗破译能力,采用超混沌系统是行之有效的解决方法。与一般的混沌系统相比较,超混沌系统具有两个或两个以上正的李雅普诺夫指数,且具有更为复杂的动力学行为,更加难以预测,因此在保密通信、信息安全等工程领域中有广泛的应用前景[3-5]。

综合考虑随机性、快速性、安全性、抗破译性、空间复杂性和易实现等因素,利用超混沌的复杂性,对产生的实值序列进行预处理和量化处理,这样产生的二值序列游程短、均匀分布性好,且具有良好的随机特性、很强的安全性和广泛的实用性。文献[6]提出了将混沌加密技术和传统加密技术相结合的一种新颖的保密通信技术,但只提供了大致的技术框架,并没有具体应用方案及应用实例,为此,结合电子邮件系统,将这种级联加密技术应用其中。通过COM加载项,设计和实现了在Outlook 2007客户端中对电子邮件进行加解密。在发送端,先用改进后的超混沌序列对邮件明文进行加密,然后级联3DES加密技术进一步加密,接收端采用相应的解密技术解密密文,从而实现了对电子邮件的保密通信。

2 超混沌序列的改进

文献[7]提出了一个新的四维超混沌系统,其状态方程表示为:

到稿日期:2011-06-30 返修日期:2011-12-06 本文受国家自然科学基金(60872123,U0835001),广东省高等学校高层次人才项目基金(N9101070)资助。

黄涵淇(1989-),女,硕士生,主要研究方向为信号与信息处理、信息安全,E-mail:huanghanqi.1989@163.com;**刘明华**(1975-),男,博士,主要研究方向为非线性电路;**胡 健**(1986-),女,硕士生,主要研究方向为信号与信息处理、数字家庭;**尹燕伟**(1986-),男,硕士生,主要研究方向为信息与信息处理;**冯久超**(1964-),男,教授,博士生导师,主要研究方向为数字信号处理、数字通信、非线性动力学及混沌理论与应用。

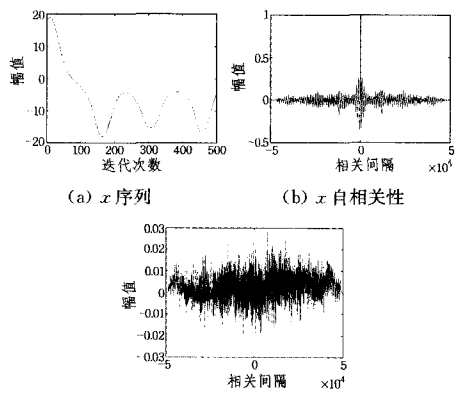
$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=cx-xz+u\\ \dot{z}=xy-bz\\ \dot{u}=-dx\end{cases} \tag{1}$$

式中，a,b,c,d 为系统控制参数。当 $a=35,b=3,c=35,d=8$ 时，4 个 Lyapunov 指数分别为 $\lambda_1=0.2788,\lambda_2=0.1470,\lambda_3=0,\lambda_4=-38.429$，有 2 个正的 Lyapunov 指数，4 个 Lyapunov 指数之和小于零，是一个超混沌系统。

2.1 超混沌序列的预处理

当两个同构系统的初态与参数相差较大时，两混沌系统之间的相应变量是互不相干的浮点数序列。然而，当两个同构系统的初态及参数具有微小差异(10^{-14})时，与单维混沌相比，超混沌得到的两组序列数之间就会存在一定的互相关性，将经过这两组序列量化后得到的 0-1 序列也存在较强的互相关性，因此有必要对超混沌变量进行预处理，来得到更适合产生序列密码的原始浮点数值序列。

本文采用经典的四阶 Runge-Kutta[8] 来求解方程(1)，系统初始值：$x_0=10,y_0=11,z_0=12,u_0=13$，控制参数：$a=35,b=3,c=35,d=8$，积分步长 $h=0.01$，迭代次数 $n=40000$。以 x 序列的特性为例，得到 x 序列的 35400～35900 项、x 的自相关性和 x-z 的互相关性如图 1 所示。



(a) x 序列　(b) x 自相关性

(c) x-z 互相关性

图 1　x 序列、x 自相关性和 x-z 互相关性

按照 Golomb 公设，理想的伪随机序列应具有 3 个特性：均匀分布、自相关是 δ 函数、互相关是零[9]。而在上述条件下，x,y,z,u 实数值混沌序列值域分别为(−28,25)，(−32,28)，(8,61)，(−82,75)，其数学期望分别是 $E_x=0.0602,E_y=0.0515,E_z=33.7305,E_u=-0.0550$。从图 1 中可以看出，序列在局部呈现一定的单调性，其均匀分布较差，序列的自相关不是 δ 函数，互相关也不是理想的零。因此，为了得到更好的伪随机序列，有必要对实数值超混沌序列做如下预处理：

(1)将序列的小数点向右移动 k 位($k=0,1,2,3,4\cdots$)；

(2)将序列映射到值域(−0.5,0.5)；

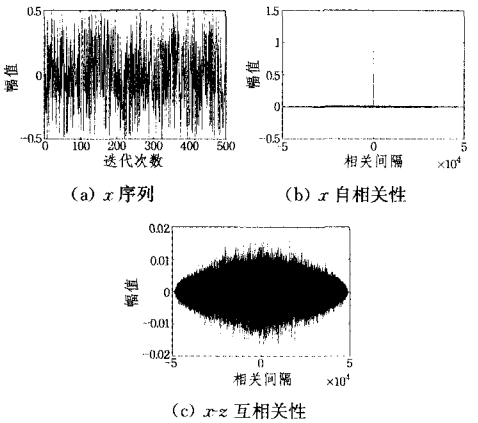
整个预处理过程可由下式实现：

$$x_k(i)=10^k x_k(i)-\mathrm{round}(10^k x_k(i)) \tag{2}$$

式中，round(x)为取最接近整数的运算。

对超混沌序列采用式(2)进行预处理，k 值取 2，改进后的 x 序列的 35400～35900 项、x 的自相关性和 x-z 的互相关性如图 2 所示。

预处理后的结果为：x,y,z,u 实数值混沌序列值域均为(−0.5,0.5)，其数学期望分别为 $E_x=0.0013,E_y=2.2918\mathrm{e}-005,E_z=-0.0014,E_u=8.8572\mathrm{e}-004$，说明序列分布均匀；自相关尖峰值是 1，旁瓣的最大值 $R_{x\max}=0.0162,R_{y\max}=0.0152,R_{z\max}=0.0154,R_{u\max}=0.0163$，说明是自相关较理想的 δ 函数；互相关的最大值 $R_{xy\max}=0.0163,R_{xz\max}=0.0191,R_{yz\max}=0.0161,R_{xu\max}=0.0173,R_{yu\max}=0.0188,R_{zu\max}=0.0163$，说明互相关近似为理想的零。比较图 1 和图 2 可以看出，预处理后的超混沌序列具有良好的均匀分布特性、随机统计特性和相关特性，是非常理想的伪随机序列。



(a) x 序列　(b) x 自相关性

(c) x-z 互相关性

图 2　改进后的 x 序列、x 自相关性和 x-z 互相关性

2.2 量化处理

一般对离散混沌系统的量化方法是设定一个阈值，大于该阈值，量化值取 1，否则取 0。这种量化方法简单，一步就可产生一位二进制数。对于连续混沌系统，由于系统方程的数值算法较复杂，因此采用两分区间量化时，产生序列密码的速度太慢。综合考虑快速性和随机性两个因素，设计了下述量化方法。

将区间(−0.5,0.5)均分为连续的 16 等份，每个区间标号为 0～15，相应区间的二进制值为 0000～1111，如区间 6 对应的二进制序列为 0110。选择序列 x、u，将预处理后的超混沌序列 x'、u' 值映射到相应区间并生成二进制序列 x''、u''，在同一步内产生的二值序列按照(x'',n'')的顺序分别映射到密钥序列的相应位置，最终密钥序列的长度为原序列长度的 8 倍[10]。相比一般离散混沌系统采取的两分区间量化方法，该方法提高了产生序列的速度和随机性。

2.3 伪随机性检验分析

根据 Shannon 理论，若加密密码序列是完全随机的，则该加密系统是不可破解的。在数字实现方式下，由于存在有限精度效应，因此得到的序列并非是完全随机的，而是伪随机序列。为了确保伪随机序列尽量接近真随机序列，本文采用美国国家标准技术研究院开发的 NIST 测试组件，它包括 16 项测试，选取其中相对重要的 5 项[11]：频数测试、分组频数测试、游程测试、频谱测试和近似熵测试。每个被测二进制序列的长度为 10 万位，取 100 组进行测试。每项测试的结果均以 P-value 表示，若 P-value<0.01，则说明该项测试未通过；否则，说明该项测试通过，测试结果如表 1 所列。

表 1　改进后的超混沌序列随机性测试结果

测试类型	频数测试	分组频数测试	游程测试	频谱测试	近似熵测试
P-value 范围(100 组数据)	0.1306～0.9646	0.1551～0.9613	0.1493～0.9963	0.2120～0.9537	0.2670～0.9905

从测试结果可知，超混沌实值序列经过预处理和量化后产生的0～1二进制密钥流完全通过了随机性测试。

3 级联加密技术的电子邮件保密通信

3.1 电子邮件保密通信原理

根据文献[6]的思想，结合常规加密技术，提出本算法的电子邮件保密通信的原理框图，如图3所示。

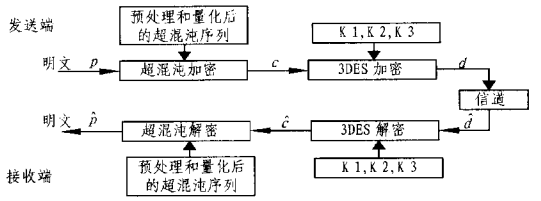


图3 电子邮件保密通信原理框图

3.2 加解密算法

由原理框图3可见，加解密算法按以下几个步骤进行：

(1) 用户输入口令字，使用hash算法将口令字和一段随机数结合生成8个double类型的数字，用其小数点后的部分替换原有超混沌系统初始值和控制参数的小数点后的数字，这样，不同的口令将对应不同的初始参数，从而产生不同的超混沌序列；

(2) 将第(1)步中获取的参数代入超混沌系统，取迭代次数 $n=50000$，舍弃前10000次迭代产生的序列值，将序列值预处理和量化后得到的二进制序列与电子邮件的明文 p 进行按位异或操作，得到异或后的密文 c；

(3) 将最后3次迭代产生的 x 作为3DES加密算法的3个密钥值 $K1,K2,K3$，对密文 c 进行3DES加密得密文 d；

(4) 将 d 送到信道传送；

(5) 接收端收到密文 $\hat{d}$ 后，输入一个与加密相同的口令字，采用相同的算法获得4个初始值和4个控制参数；

(6) 与第(2)步相同，同样进行 $n=50000$ 次迭代，取最后3次迭代产生的 x，即为3DES算法的3个密钥值 $K1,K2,K3$，对密文 $\hat{d}$ 进行解密得密文 $\hat{c}$；

(7) 再将密文 $\hat{c}$ 与二值化处理后的超混沌序列(舍弃前面10000次迭代产生的序列)按位进行异或操作，完成最终解密过程，得到明文 $\hat{p}$。

步骤(1)－(3)是发送端加密过程，步骤(5)－(7)是接收端解密过程，采用因特网传送信号，只要保证加密和解密的密钥相同，迭代次数相同，就能在接收端正确解密出明文。

3.3 级联加密系统在Outlook 2007电子邮件中的应用

Outlook是应用广泛的电子邮件客户端程序，本文通过Outlook COM加载项来实现级联加密系统对电子邮件的加解密功能，软件实现主要包括两个部分：一部分是用Visual Basic开发的ActiveX DLL COM组件，用于加载到Outlook程序中，并通过Outlook的对象模型访问Outlook中的数据；另一部分是用Visual C开发的DLL，包括用于对电子邮件内容进行加密和解密的函数。

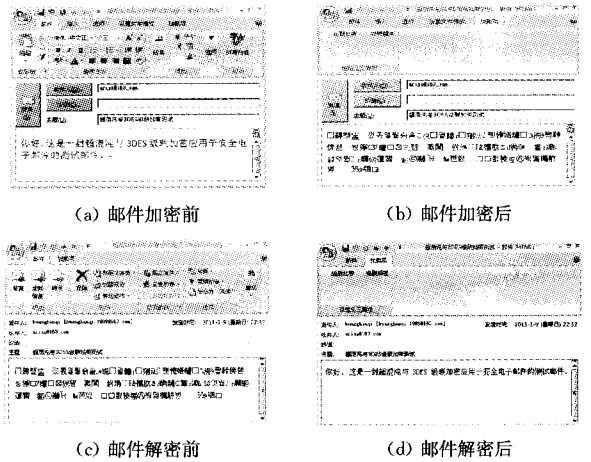
具体实现流程如下：

(1) 在Outlook 2007中新建一封邮件，输入要发送的邮件内容，加密前的邮件如图4(a)所示；

(2) 点击“加载项>>级联加密”按钮，电子邮件内容加密后如图4(b)所示，加密完成后发送电子邮件；

(3) 在接收端，接收到经互联网传输后的加密邮件，解密前的邮件如图4(c)所示；

(4) 点击“加载项>>级联解密”按钮，完成对邮件的解密操作，如图4(d)所示。可以看出，邮件解密后的内容与加密前的内容完全一致。



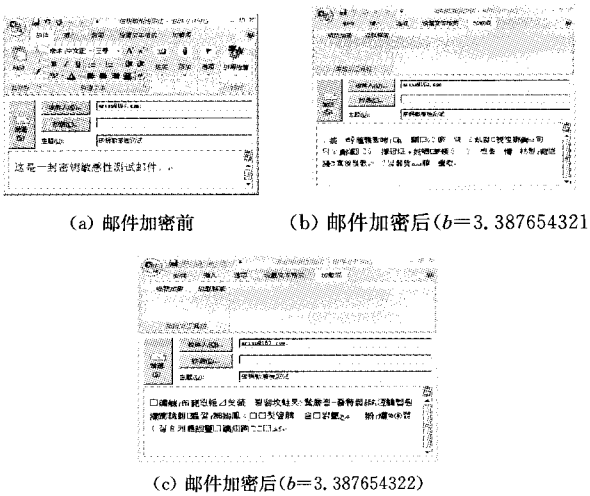
(a) 邮件加密前　(b) 邮件加密后

(c) 邮件解密前　(d) 邮件解密后

图4 电子邮件系统的加解密流程图

3.4 密钥敏感性分析

一个好的加密系统，其密文必须对密钥很敏感，即密钥很小的一点变化，就会导致密文发生很大的变化[12,13]。为了测试密钥敏感性，做了以下对比实验：从超混沌系统的4个控制参数和4个变量中任选一个(本文测试中选择 b)，当参数 $b=3.387654321$ 时，对明文“这是一封密钥敏感性测试邮件”进行加密，如图5(a)所示，加密后的密文如图5(b)所示；其他条件不变，仅将参数 b 改为3.387654322，对同样的明文进行加密，加密后的密文如图5(c)所示。由图5(b)和图5(c)对比可以得出：密钥稍微有点改变后，密文将完全不同。



(a) 邮件加密前　(b) 邮件加密后($b=3.387654321$)

(c) 邮件加密后($b=3.387654322$)

图5 密钥敏感性测试

4 安全性分析

基于文献[7]提出的超混沌系统，其结构较低维混沌系统复杂，产生的实数值序列更不可预测；系统中有4个变量和4个控制参数，这些都可以用来作为序列系统的种子密钥，算法的密钥空间大大高于应用低维混沌方程构造的序列；对系统输出的实值混沌序列进行处理，可采用单变量或多变量组合的加密混沌序列(本文中选取 x 和 u 两个序列进行组合)，这样序列的设计灵活，有更大的设计空间，可以提高安全性，为

改善有限精度造成的短周期效应提供了解决的可能性。

预处理后的超混沌序列是非常理想的伪随机序列，密钥集合中不存在大量的弱密钥(密钥与输出之间存在超出一个好密码所应具有的相关性)和等效密钥(由一个密钥与输出能推导出另一个密钥与输出)。量化处理采用一种通过均分区间一次迭代生成多比特二进制序列的方法，提高了生成序列的速度和随机性。预处理和量化过程是一种不可逆变换，破译者无法根据截取的密文去重构产生序列密码的混沌系统动力学模型、初始状态等，从而基于相空间重构的攻击、基于回归映射的攻击和基于混沌同步的分析方法都将不起作用，这一加密算法有很高的抗破译能力。

本文中的超混沌加密属于流加密，对分组加密的攻击方法是无效的。同时，对选择明文/密文攻击方法，由于混沌的单向性和混沌信号的迭代处理，异或操作后密钥流的推断几乎不可能。该加密算法没有 S-box 空间，临时变量也比较少，而且通过循环产生密钥流，循环过程中需要寄存的变量有限，运行时占用的空间很少，另外，加密和解密过程是可以重用的，这样所占用的空间就大大缩小。

采用 3DES 加密算法，解决了 DES 算法密钥太短的问题，同时也克服了 DES 中存在的弱密钥和半弱密钥的缺陷[14]；另外，将超混沌序列加密后的密文作为 3DES 加密级的输入，使得 3DES 算法的输入和输出间不存在唯一的明文-密文对[6]，从而提高了保密性。在信道中传输的密文是经过双重加密的，可以对抗文献[15]中提出的对混沌系统的识别和对初始值确定的破译方法，从而发挥了两者各自的优势，提高了加密的复杂度。

结束语 提出一种基于超混沌加密技术和 3DES 加密技术相结合的级联加密技术方案。对超混沌实值序列进行了预处理和量化处理，预处理改善了超混沌系统在有限精度实现时的短周期现象，得到了自相关特性良好的输出序列；量化处理提高了序列密码产生的速度和随机性。基于超混沌系统设计的加密算法具有很大的密钥空间、较好的安全性和较强的抗破译能力。该方案利用了超混沌加密技术和 3DES 两者各自的优势，比任意一种加密技术单独使用时的保密性能都好。将这种级联加密技术应用于 Outlook 2007，实现了电子邮件内容的加解密。实验结果表明，这种保密技术可以在网络信息传输中很好地完成加密和解密过程，安全性能好，应用方便简单。

参 考 文 献

[1] Zhou Hong, Ling Xie-ting. Problems with the chaotic inverse system encryption approach[J]. IEEE Trans on Circuits and Systems I: Fundamental Theory and Applications, 1997, 44(3): 268-271

[2] Kanso A, Smaoui N. Logistic chaotic maps for binary numbers generations[J]. Chaos Solitons & Fractals, 2009, 40(5): 2557-2568

[3] Wang Xing-yuan, Yang Lei, Liu Rong, et al. A chaotic image encryption algorithm based on perceptron model[J]. Nonlinear Dynamics, 2010, 62(3): 615-621

[4] Cruz-Hernandez C, Lopez-Gutierrez R M, Aguilar-Bustos A Y, et al. Communicating encrypted information based on synchronized hyperchaotic maps[J]. International Journal of Nonlinear Sciences and Numerical Simulation, 2010, 11(5): 337-349

[5] 赵耿，方锦清. 现代信息安全与混沌保密通信应用研究的进展[J]. 物理学进展，2003，23(2)：212-255

[6] 丘水生，陈艳峰，吴敏，等. 混沌保密通信的若干问题及混沌加密新方案[J]. 华南理工大学学报：自然科学版，2002，30(11)：75-80

[7] 刘明华，冯久超. 一个新的超混沌系统[J]. 物理学报，2009，58(7)：4457-4462

[8] 张池平，施云慧. 计算方法[M]. 北京：科学出版社，2002：371-384

[9] Wang Ying, Han Chun-yan, Liu Yuan-yi. A parallel encryption algorithm for color images based on Lorenz chaotic sequences [C]//Proceeding of the 6th World Congress on Intelligent Control and Automation. Dalian, China, 2006: 9744-9747

[10] 姚洪兴，李萌，杜贤利. 一种基于超混沌的二值序列生成方法[J]. 科学技术与工程，2008，8(13)：3508-3512

[11] 刘金梅. 多个混沌系统构造密码算法的理论及应用研究[D]. 广州：华南理工大学，2009

[12] Shannon C E. Communication theory of secrecy systems[J]. Bell Systems Technical Journal, 1949, 28: 656-715

[13] 潘勃，冯金富，陶茜，等. 基于超混沌映射和加法模运算的图像保密通信方案[J]. 计算机科学，2009，36(8)：273-275

[14] 宋震，等. 密码学[M]. 北京：中国水利水电出版社，2002

[15] Sobhy M I, Shehata A-E R. Methods of attacking chaotic encryption and countermeasures[C]//IEEE International Conference on Acoustics, Speech, and Signal Processing. 2001, 2: 1001-1004

(上接第 61 页)

[12] Shavitt Y, Tankel T. Big-bang simulation for embedding network distances in Euclidean space[J]. IEEE/ACM Transactions on Networking (TON), 2004, 12(6): 993-1006

[13] 黄永生，孟祥武，张玉洁. 基于社会网络特征的 P2P 内容定位策略[J]. 软件学报，2010，21(10)：2622-2630

[14] Zaharia M A, Chandel A, Saroiu S. Finding content in file-sharing networks when you can't even spell[OL]. http://research.microsoft.com/workshops/PTPS2007/paper/ZahariaChandelSaroiuKeshav.pdf, 2007

[15] Gaeta R, Sereno M. Generalized Probabilistic Flooding in Unstructured Peer-to-Peer Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(12): 1-8

[16] BRITE[OL]. http://www.cs.bu.edu/brite

[17] Jovanovic M A. Modeling large-scale peer-to-peer networks and a case study of Gnutella[M]. University of Cincinnati, USA: 2001

[18] Lv Q, Cao P. Search and replication in unstructured peer-to-peer networks[C]//Proc. of the 16th ACM Int'l Conf on Supercomputing(ICS 2002). New York: ACM Press, 2002: 254-261

[19] Gnutella[OL]. http://www.limewire.com/developer/gnutella_protocol_0.4.pdf

[20] Jiang S. LightFlood: Minimizing redundant messages and maximizing scope of Peer-to-Peer search[J]. IEEE Transactions on Parallel and Distributed Systems, 2008, 19(5): 601-614

[21] 孙新，刘玉树，刘琼昕. 具有位置感知和语义特征的 P2P 网络模型[J]. 电子学报，2010，38(11)：2606-2610