DOI: 10.3785/j.issn.1008-973X.2012.04.020

动态 P2P 网络中基于匿名链的位置隐私保护

徐 建[1], 黄孝喜[1], 郭 鸣[2], 金正平[1], 郑 宁[1]
(1.杭州电子科技大学 计算机学院,浙江 杭州 310018;2.浙江大学城市学院 计算机与计算科学学院,浙江 杭州 310015)

摘 要: 为了解决动态 P2P 环境中的位置隐私保护问题,提出基于匿名链的位置隐私保护算法. 不同于一般的 K-anonymity 方法,通过在用户查询信息转发的过程中构造一条匿名链来混淆身份信息与位置信息的一一对应关系,在完成查询的同时保护用户位置的隐私. 针对一般 P2P 匿名存在的匿名组稳定性问题,该算法根据路网环境中移动对象的动态性,通过计算相邻移动用户之间的连通性对匿名链中间节点的选择进行优化. 讨论匿名链构造的方法和中间节点优化选择的标准,对算法的安全性展开理论分析. 通过实验验证了算法的可行性. 实验结果表明,该算法在不同用户密度下都能够较好地完成匿名链的构造,保护用户位置隐私;同时,中间节点的优化方法可以在一定时间内显著提高匿名链的有效性.

关键词: P2P 网络;位置隐私;匿名链;基于位置的服务(LBS)
中图分类号: TP 391 **文献标志码**: A **文章编号**: 1008-973X(2012)04-0712-07

Location privacy through anonymous chain in dynamic P2P network

XU Jian[1], HUANG Xiao-xi[1], GUO Ming[2], JIN Zheng-ping[1], ZHENG Ning[1]
(1. *College of Computer, Hangzhou Dianzi University, Hangzhou* 310018, *China*; 2. *School of Computer and Computing Science, Zhejiang University City College, Hangzhou* 310015, *China*)

Abstract: An anonymous chain based privacy protection algorithm was presented to solve the problem of location privacy protecting in dynamic peer-to-peer (P2P) network. Different from the general K-anonymity method, anonymous chain was constructed to break the one-to-one correspondence between the user identity and location information during the forwarding process of query message, and the location privacy was protected with the completion of the query. The algorithm optimizes the selection of intermediate nodes according to the stability of linkage between two nodes in order to deal with the dynamic issues in P2P environment. A connectivity matrix was introduced for the chain constructing algorithm and the security of anonymous chain was proved. A simulation on a real city map for the algorithm showed the effectiveness. The results prove that anonymous chain can be constructed in different density of moving nodes and the optimal intermediate nodes selecting method obviously improves the stability of the chain.

Key words: P2P network; location privacy; anonymous chain; location-based service

基于位置的服务(LBS)依赖于移动对象准确、实时的位置信息,但如果向不可信的第三方披露这些信息,用户将面临巨大的风险[1-2],所以用户的位置隐私成为研究者讨论的一个重要话题. Gruteser 等[3]将数据库信息发布中的 K-anonymity 模型引入位置隐私保护研究领域. 其他位置隐私保护方法还有使用假数据[4]、基于空间变换的匿名[5]等.

传统的 K-anonymity 模型面临连续查询攻击、

收稿日期: 2011-10-08. 浙江大学学报(工学版)网址: www.journals.zju.edu.cn/eng
基金项目: 国家自然科学基金资助项目(61003195, 61070212, 61103101); 中国博士后科学基金特别资助项目(201104743).
作者简介: 徐建(1975—),男,副教授,从事分布式计算机系统的研究. E-mail:jian.xu@hdu.edu.cn

最大速度攻击和异常点攻击威胁. Bamba 等[6]在位置隐私保护中使用了 l-diversity 思想. Gedik 等[7]介绍一种可提供差别服务的匿名模型并开发了相应的算法. Xu 等[8]提出基于圆形匿名空间的匿名算法，圆形的匿名空间能够生成较小的查询结果集，从而提高算法的精度. Kyriakos 等[9-10]讨论了路网限制环境下基于道路路段和交叉点的匿名查询处理.

在分布式结构的隐私保护模型[11]中，用户通常需要维护一个复杂的数据结构对位置进行匿名处理. 但是这种依赖固定基础通信设施的模式不适合高度动态的 LBS 应用. Chow 等[12]提出一种基于 K-anonymity 模型的 P2P 解决方案. 但 Chow 主要考虑欧几里德平面空间用户位置的匿名，在匿名组选择组成员时没有考虑用户的移动性. Amir 等[13-14]讨论了分布式环境中移动用户的近邻检测和选择问题.

本文讨论动态 P2P(peer-to-peer)网络中、路网环境下的用户位置隐私保护问题. 动态 P2P 网络是指在一个缺乏固定通信基础设施的环境中，移动用户只能通过互相协作、经过多跳的路由进行通信的网络. 在这样的环境中用户位置隐私保护的问题有一些独特性，例如需要考虑用户的移动性、受限的传输范围和带宽、多跳的通信以及受限的移动路径.

保护用户的位置隐私是保护用户身份信息与位置信息的关联性[15]. 基于以上认识，本文提出一种基于匿名链的位置隐私保护思路. 该模型通过在信息转发的过程中构造一条匿名链来混淆身份信息与位置信息的一一对应关系. 匿名链的构造过程使用私有通信(即加密)，以提高链路的安全性. 匿名链基于关联保护的模型只隐藏了身份信息与位置信息的对应关系，保留了精确的位置数据. 同时，在选择匿名链成员时比匿名区域更充分地考虑了用户的移动性，因此在保护位置隐私的同时具有较高的服务质量.

1　系统模型

如图 1 所示，系统由 2 个部分组成：移动用户和 LBS 服务器，根据移动用户在算法中扮演的不同角色可以分为查询节点、中间节点和代理节点. 查询用户通过中间节点组成一条匿名链通向代理节点，由代理节点向 LBS 服务器发起查询，并由代理节点返回查询结果.

定义 1　移动用户　移动用户是具有查询需求、并有无线通讯和计算能力的移动对象.

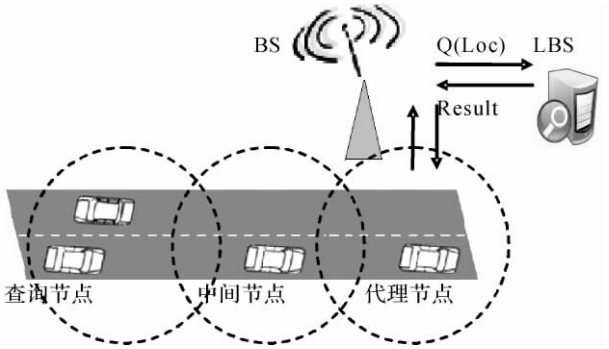

图 1　匿名链查询示意图

Fig. 1　Query through anonymous chain

假设每个移动用户都装备有 2 种无线接口卡：其中一个接口卡用于通过移动基站与 LBS 服务器的通信，另一个用于在缺乏足够固定通讯基础设施时移动用户之间的 P2P 通信. 在许多 LBS 服务和 P2P 应用中都采用这种多接口卡的策略[16]. 事实上现在市场有许多智能无线终端都具有这种能力，例如配备有 GPRS/CDMA 数据通信模块、同时具有 802.11b/g 能力的 iphone、Android 手机. 假设用户都装备了无线定位装置，例如 GPS，用于确定用户的平面坐标. 每个移动用户都有使用自身位置信息进行查询的需求，并且愿意帮助其他人进行匿名及查询处理.

定义 2　查询节点　查询节点是一个移动用户，它根据自身对匿名质量的要求，例如匿名链长度的要求和查询的时间限制，发起匿名查询.

定义 3　中间节点　中间节点是一个移动用户，它根据相邻节点发出的查询请求，判断自身能否帮助查询节点建立匿名链. 若确定自身成为查询节点匿名链的成员，则需要帮助寻找匿名链中的下一节点. 中间节点只了解与其相连的上一节点与转发的下一节点，不能确定查询节点的身份.

定义 4　代理节点　代理节点是一个移动用户，它根据相邻节点转发的查询请求，判断自身能否帮助查询节点完成查询请求. 若确定自身成为代理节点，则需要完成查询并返回相关结果.

定义 5　LBS 服务器　接受代理节点的查询请求，并返回相关结果. 由于 LBS 服务器收到的查询请求虽然包含查询节点的具体位置，但不包含该节点的身份信息，恶意用户不能通过 LBS 获得用户的位置隐私.

定义 6　匿名链　由查询节点、若干个中间节点、代理节点构成的，与 LBS 服务器通信的链路，本文称为匿名链.

2 算法和分析

2.1 算法介绍

查询节点初始化一个查询请求消息,定义该消息为QM(Pseudonym, TTL, HTL, Loc, Query),请求消息包括一个全局唯一的假名标识Pseudonym,该标识与查询节点的身份无关.生存时间(time to live, TTL)为该查询的有效时间,用于限定查询的有效性与清理超时的查询记录和转发记录.生存跳数(hop to live, HTL)表示匿名链的长度,即该请求至少需要流经的中间节点数目,显然HTL越大,匿名的效果越好.Loc是查询的位置信息.Query是查询的内容.通常匿名链算法由以下3个步骤组成.

1)相邻节点搜索.在这一步中,移动用户U将所有愿意帮忙的相邻节点信息收集起来组成一个列表.首先,移动用户向它的邻居广播请求消息.热心的相邻节点将自己的身份ID、位置、当前的运动速度信息反馈给U.为了提高匿名链构造的安全性,可以使用公钥机制对通信的内容进行加密,那么需要反馈相邻节点的公钥.用户U接着将接收到的邻居节点信息存储在一个列表List中.为了提高匿名链构造的效率,U可以周期性地检查该列表,尽量保证列表不为空.

2)选择下一中间节点.这一步移动用户在列表中选择合适的下一中间节点(HTL>1)或是代理节点(HTL=1),并转发查询请求.不管是自己发出的查询请求,还是从相邻节点接收到的查询消息,移动用户U检查消息的HTL和TTL字段,进行相应的处理.当TTL晚于系统的当前时间,并且HTL≥1时,从列表List中选择合适的节点,与之建立连接,将HTL减1,转发查询消息.

每一个节点都建立一张转发表,表中存储接收、转发消息的相邻节点身份ID与查询消息Pseudonym的对应关系以及该消息的TTL.当接收到一个查询结果时,通过查找该表,找到一中间节点并转发.当接收到一个过时的查询结果时,丢弃该结果,并删除表中的相应记录.在每次接到消息时,都对转发表进行清理,删除过时的转发记录,以提高系统转发的效率.

理论上,TTL应该大于实际的查询/返回的往返时延(round trip time, RTT).但是在动态的无线网络中,测量实际的RTT时间有困难,另本文建议采用的匿名链长度是小于最大长度的一个随机数,因此发送节点TTL设置为2×匿名链长度×单跳网络传输的最大延迟(例如IEEE802.11传输上限300 m的延迟).

3)代理节点查询结果.在这一步中,代理节点完成查询,并转发查询结果.移动用户U检查消息的HTL和TTL字段,当HTL=0时,向LBS发起查询.接收LBS的查询结果,并向该消息匿名链的上一中间节点转发结果.查询结果沿着匿名链,返回给查询节点,算法结束.

整个过程如算法1所示.

Algorithm 1 Peer-to-Peer Anonymous Chain

```
function P2PAnonymousChain (Message QM)
// Step 1: Peer Search Step
if called first time then
List ←{Ø}
end if
while NumUser(List) < 1 do
  Broadcast a request to the peers around myself
  List ←List ⋃ {the received peer information}
end while
if QM. HTL > 0 and QM. TTL< current time then
  // Step 2: Chain Setup
   C-next ← function FindNext(List)
  QM. HTL ← QM. HTL—1
  Insert forward record and Forward QM to C-next
  forward connect message to C-next
else
  // Step 3: Query
       initialize a query and return the result
end if
return
```

2.2 中间节点选择优化

2.2.1 匿名链的稳定性 与一般的移动网络不同,路网环境中节点的移动是受限的.节点之间的移动可以分为:1)同向运动;2)背向运动;3)交叉运动.一般来说,2个同向运动节点间建立的通信链路比2个背向运动节点建立的匿名链生存的时间长.在链路中间节点的选择过程中,不同的匿名链具有不同的稳定性.

从分析可知,移动节点之间通信的稳定性受到两点之间的距离、两点运动方向与运动速度的影响.本文使用连通性表示2个节点通信的稳定性.

定义7 连通性 连通性是移动节点通信最大距离与2个节点之间距离的比值,记为 $S_t=R/d$.其中 R 为通信的最大距离,d 表示在 t 时刻两节点之间的距离.

节点之间的连通性用来衡量某一时刻2个节点

之间保持通信的能力. 在不考虑障碍物的情况下，距离近的 2 个节点比距离远的 2 个节点拥有更强的通信能力. 当 $d>R$ 时，$S_t<1$，那么在 t 时刻两点之间由于处于可通信的范围之外而无法建立匿名链路.

记 $S_{t'}$ 为两节点在 t' 时刻的连通性，要使得节点在经过一段时间 $\tau=t-t'$ 之后继续能够保持通信并且通信能力最强，则在 t 时刻必须选择一个在经过 τ 时间后仍将以较大概率继续保持连通性的节点，这个概率记为 P.

路网结构中节点移动的模型都可以整合为以某一角度相对运动的交叉运动模型. 图 2 给出了这一运动模型中运动情况的详细分析. 2 个节点起始位置分别为 m_1、m_2，相距为 d，分别以 v_1、v_2 的速度运动，两个速度成一定角度运动. 经过 τ 段时间之后，运动至 m_1'、m_2'，两点距离变为 d'. 在运动过程中，若将 2 个节点的运动看成是一个整体，则只需考虑运动组的状态改变.

对于 2 个移动节点，改变它们运动状态的是节点的速度差，$v=v_1-v_2$. v、v_1、v_2 都是速度矢量，包含了方向的信息.

两点之间的距离也可以看作是一个距离的向量（m_1 到 m_2 的向量）. 从几何意义上分析，速度向量的作用效果一共有两部分：一部分改变了距离向量的大小，另一部分改变了距离向量的方向. 若记合速度向量与距离向量之间的夹角为 θ，则改变距离大小的部分为 $|v|\cos\theta$，改变距离方向的部分为 $|v|\sin\theta$. 在经过 τ 时间后，距离变换的关系可以表示为

$$|d'|=|d|+|v|\tau\cos\theta. \tag{1}$$

若以在 t' 时刻继续保持通信连通的概率来评估各点的可连通性，即计算在 t' 时刻连通性 $S_{t'}\geqslant 1$ 的概率，记为 $P(S_{t'}\geqslant 1)$，则

$$P(S_{t'}\geqslant 1)=P\left(\frac{R}{d+|v|\tau\cos\theta}\geqslant 1\right)=P\left(|v|\leqslant\frac{R-d}{\tau\cos\theta}\right). \tag{2}$$

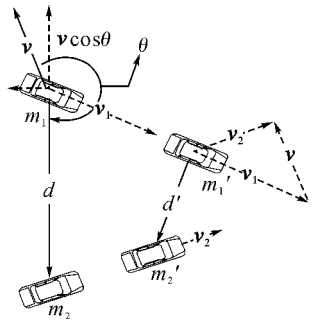

图 2　移动位置分析

Fig. 2　Location analysis of moving peers

假设移动节点的速度值，服从均值为 μ、方差为 σ 的正态分布，即 $|v|\sim N(\mu,\sigma)$，则

$$P(S_{t'}\geqslant 1)=P(|v|\leqslant\frac{R-d}{\tau\cos\theta})=\frac{1}{\sqrt{2\pi}\sigma}\int_0^{\frac{R-d}{\tau\cos\theta}}\exp\left(-\frac{(|v|-\mu)^2}{2\sigma^2}\right)\mathrm{d}|v|. \tag{3}$$

从式(3)可以看出，影响概率 $P(S_{t'}>1)$ 的主要参数是距离 d、速度 $|v|$、时间 τ 以及速度与距离向量的夹角 θ. 因此，概率 $P(S_{t'}>1)$ 是由一个关于 d、$|v|$、τ、θ 的函数决定的：$P(S_{t'}\geqslant 1)=f(d,|v|,\tau,\theta)$. 本文将该函数定义为连通稳定度.

定义 8　匿名链的连通稳定性　匿名链的连通稳定性是衡量匿名链路中多个节点之间通信保持连通的概率. 该概率是由链路上两两相邻节点关于 d、$|v|$、τ、θ 的函数 $P(S_{t'}\geqslant 1)=f(d,|v|,\tau,\theta)$ 决定的.

通过计算邻居节点的连接稳定度，可以评估出各节点在未来时间 τ 内的连通性，并以此为指标选择下一个节点来构造通信链路. 与一般随机形式的节点选择算法相比，考虑节点移动性的算法所构造出的通信链路显然拥有更强的稳定性. 此外，通信链路的稳定性也与链路的长度有关，链路越长，稳定性越差. 若通信链路稳定性的概率为

$$P_{(0,1)}=f(d,|v|,\tau,\theta), \tag{4}$$

则长度为 K 的通信链路稳定性的概率为

$$P(K)=P_{(0,1)}\times P_{(1,2)}\times\cdots\times P_{(K-1,K)}=\prod_{i=1}^{K}P_i. \tag{5}$$

2.2.2　匿名链的空间覆盖度　通过构造匿名链路来保证位置信息，当查询节点与中间节点或者代理节点的位置十分相近时，保护的隐私效果降低. 因为观察攻击者可能把代理节点所发布的查询位置信息当成是查询节点的位置信息，而当查询节点与代理节点的位置信息相近时，查询节点的位置隐私有泄漏的风险. 在考虑系统连通稳定性的同时，必须考虑隐私保护效果.

定义 9　空间覆盖域　空间覆盖域是指匿名链内所有节点的最大通信范围在消除重叠区域后所覆盖的空间之和.

在匿名链路构造的过程中，选择距离现有节点集合越远的节点能够更大程度地增加空间覆盖域，以增强匿名效果. 在选择中间节点时，通过计算各临近节点的距离来评估构造匿名链时空间覆盖域的增长程度.

在匿名链构造时，节点的选择既需要考虑通信的稳定性，又需要考虑系统的匿名性. 相对地，距离

相近的节点之间通信稳定性较强,但会降低系统的匿名性;距离较远的点尽管通信稳定性较弱,但能够增强系统匿名性.因此,算法的实施必须作出一个折中的选择.本文在优先考虑连通稳定性的前提下,选择空间覆盖域较大的节点.

匿名链构造过程中的中间节点选择过程如算法 2 所示.

Algorithm 2 Mobile-Aware peer Selecting

1: function FindNext (Loc, List)

2: for all new peers in List do

3: $p_i = f(d, v, \tau, \theta)$

4: end for

5: sort List with p_i

6: for top 3 peers in List do

7: l_i = Distance(Loc, peer_i. Loc)

8: end for

9: next = the second distance peer

10: return next

2.3 安全性分析

在本文的模型中,LBS 服务器收集了位置数据和用户的查询记录,但是身份数据与位置数据的对应关系却被保护了.因此,攻击者的目标是获得这种对应关系.

攻击者假设:攻击者是一个全局的攻击者,即攻击者可以获取 LBS 服务器数据,并且在移动节点内有同伙恶意节点.攻击者以获取查询发起者的身份为目标,获取位置数据与身份数据的关联关系.

攻击环境假设:在网络中,假设有移动节点集合 N,N 包含 n 个移动用户.攻击者恶意节点集合 C,C 包含 c 个为恶意节点,$c<n$.仅考虑一种静态的模型,即在算法进行过程中没有移动用户退出,也没有新节点的加入.在匿名链的构造过程中,查询节点构造的匿名链长度最大取值为 K.同时,一些恶意节点可能被选为中间节点.恶意节点可以根据本地转发表的查询记录构造匿名链中节点的顺序,根据系统允许的匿名链最大长度 K 值推测查询节点的身份.

显然,查询节点在不知情的条件下选择了恶意的节点作为中间节点,则隐私信息会被恶意节点窃听到然后告知攻击者.因此,攻击者成功窃听到隐私信息的概率是恶意节点推测到查询节点的概率.若使用 H_1 表示第一个中间节点是恶意节点的事件,则

$$P(H_1) = c/n. \tag{6}$$

显然,第一个中间节点是恶意节点的事件发生概率与 Chow 等[12]使用匿名组头节点来代理查询的 K-anonymous 模型相等.

在匿名链保护模型中,查询消息是通过一条长度不超过 K 的匿名路径传播的.假设匿名路径上的第 $j(j \leqslant K)$ 个节点是恶意节点,则该节点会以一定的概率去推测自它开始的第 $i(i \leqslant j)$ 个节点是查询节点.令 $\rho(i)$ 表示推测第 i 个节点为查询节点的概率,$\varphi(i)$ 为该节点确为查询节点的概率,如下:

$$\rho(i) = 1/j, \tag{7}$$

$$\varphi(i) = \left(\frac{n-c}{n}\right)^{i-1}\frac{c}{n}. \tag{8}$$

使用 H_j 表示位于匿名链上第 j 节点的攻击者成功地推测出初始节点的事件,则该概率为

$$P(H_j) = \sum_{i=1}^{j}\varphi(i)\rho(i) = \sum_{i=1}^{j}\frac{1}{j}\left(\frac{n-c}{n}\right)^{i-1}\frac{c}{n}. \tag{9}$$

对于最大长度为 K 的匿名链,较大的 K 值将增大 j 的取值范围,提高查询节点的匿名程度,从而增加恶意节点的攻击难度.由以上分析可知,查询节点匿名的效果与恶意节点集合 C 的大小以及匿名链的长度相关,在恶意节点数目一定的情况下,根据用户可接受的查询时间和系统开销限制,系统可以增加匿名链的最大长度来增加匿名效果.

3 实验模拟

实验使用德国 Oldenburg 实际的道路地图,包含 6 105 个节点和 7 035 条边,如图 3 所示.在 Brinkhoff[17]研发的模拟器基础上,使用 Java 语言开发实现本文算法,模拟不同交通状况条件下的查询.同时假设移动用户之间 P2P 通信的协议为 IEEE802.11a/b/g.模拟硬件平台为 TyanPSC 桌面高性能计算系统.

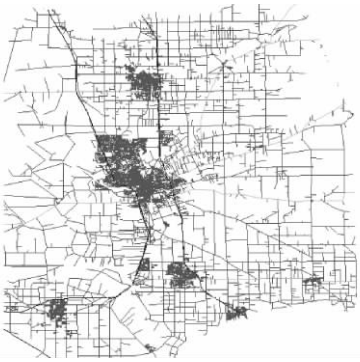

图 3 San Joaquin 地图

Fig. 3 Map of San Joaquin

3.1 成组匿名的稳定性

实验设置为总共 11 000 个移动用户,初始移动用户数为 1 000,以 100 个/模拟时间单位的速度进入路网.移动节点的运动路径是随机的,在节点生成时随机选择的起始路网结点间使用 Dijkstra 算法确定.

运动的速度是由所经路段允许的最大速度和通过该路段的移动节点数共同确定的. 平均路径长度约为 16 km. 假设用户在移动过程中以某个固定的概率发起查询，匿名成组区域范围为3 hops. 随机跟踪 500 个用户的匿名组，统计在 1、2、3、4 单位时间内匿名组初始成员数目的变化. 实验结果如图 4 所示. 图中，p 为匿名组初始成员数目与匿名组总成员数目的比值.

由图 4 可以发现，随着时间的推移，匿名组初始成员数目呈下降趋势，从平均 70% 下降到 54%、45%、38%. 结果表明，匿名组随着时间的推移，初始成员快速离开，新成员快速加入. 系统需要不断地进行匿名组的重组以保证稳定性.

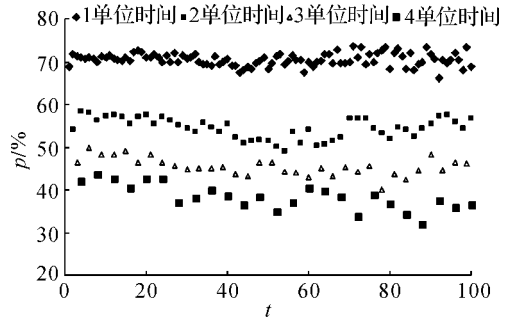

图 4　成组匿名的稳定性

Fig. 4　Stability of spatial cloaking

3.2　中间节点选择优化效果

在这个实验中，对中间节点的随机选择方法和优化选择方法进行比较实验，研究优化选择对匿名链稳定性的影响. 在不同节点规模的条件下，使用 3 hops的匿名链路长度，统计匿名链在一个模拟时间单位后的有效比例.

如图 5 所示，随着环境中移动用户数目 N_s 的增加，匿名链的总体有效率逐步提高. 但是在不同用户数目的条件下，优化选择的稳定性都优于随机选择，结果平均提高了约 9.24%，因此表明了算法 2 的有效性.

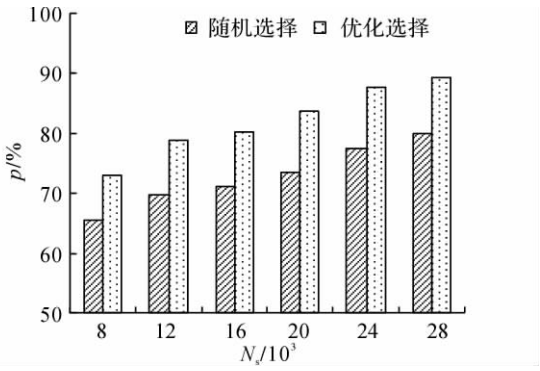

图 5　中间节点选择优化效果

Fig. 5　Effects of optimal node selecting

3.3　匿名链连接的可扩展性

使用一次匿名链的连接成功率来衡量系统的连通性，以评价匿名链保护模型的可扩展性. 主要从 2 个方面分析：规模的可扩展性和匿名链路长度的可扩展性.

规模的可扩展性是指当网络规模确定、移动用户数目增加时系统的稳定性. 如图 6 所示为在 Oldenburg 路网环境中，不同节点规模下的系统稳定性. 在不同节点规模下分别统计系统内连接成功的比率. 可以看出，匿名链路的成功率受到用户密度的显著影响. 当用户密度提高时，中间节点的选择空间扩大，匿名链的一次连接成功率会提高.

匿名链路是一条多跳的通信链路，在高度动态的路网环境中多跳的通信链路会受到跳数的直接影响. 如图 6 所示为多跳匿名链路的扩展性. 实验结果表明，匿名链的长度对系统可扩展性的影响显著，当匿名链路增长时，系统一次连接成功率降低. 但是随着环境中用户数目的增加，可选中间节点增多，较长匿名链的连接成功率也随之提高.

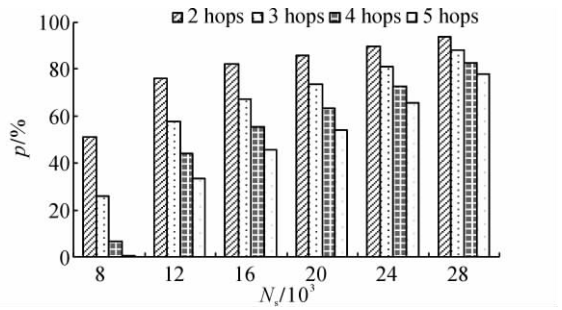

图 6　匿名链的成功率

Fig. 6　Success rate of anonymous chain

3.4　匿名链查询节点的匿名效果

在 11 000 个移动用户的模拟环境中，依次增加恶意用户的比例. 记录在匿名链最大长度为 2、3、4、5 hops 的实验条件下，出现恶意节点的匿名链数目及第一个恶意节点的位置，计算系统中成功推测查询节点的平均概率. 实验结果如图 7 所示.

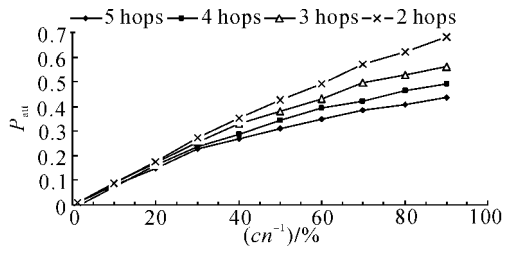

图 7　攻击成功概率

Fig. 7　Probability of successfully attacking

图7中,c/n为系统中恶意节点占移动用户总数的比例,P_{att}为系统中恶意节点攻击成功的概率.较大的概率表示较差的匿名性.从图7可以看出,随着系统中恶意节点数目的增加,系统整体的攻击成功概率增加.当恶意节点比例<10%时,匿名链长度对攻击成功概率的影响不显著.但当恶意节点比例>10%时,匿名链长度的增加,可以显著降低攻击成功的概率,提高查询节点的匿名性.

4 结 语

在动态P2P网络环境中,移动用户向不可信的LBS提供自身位置信息获取服务的时候面临攻击而导致位置隐私泄漏的风险.一般的P2P位置隐私保护算法仅考虑在欧几里德空间内用户的移动问题,匿名组成员的选择也没有考虑路网限制的移动特性.本文提出基于匿名链的P2P结构位置隐私保护方法,通过匿名链保护用户身份信息和位置信息的关联,讨论了动态环境中匿名链中间节点的优化选择方法.本文对算法进行理论分析,并通过实验验证了可行性.

下一步的研究中项目组将对算法进一步完善,并对其在实际应用中可能产生的问题进行研究.例如匿名链空间覆盖问题的量化分析和研究;基于关联性的匿名链位置隐私保护模型在传感器网络中的应用;从动态移动网络中不同的应用情景出发,对匿名链位置隐私保护技术应用进行深入研究等.

参考文献(References):

[1] KARIM W. Privacy implications of personal locators: why you should think twice before voluntarily availing yourself to GPS monitoring [J]. **Journal of Law and Policy**, 2004, 14(1): 485-515.

[2] BARKHUUS L, DEY A. Location-based services for mobile telephony: a study of users's privacy concerns [C] // **Proceedings of Interact**. Zurich: IOS, 2003: 709-712.

[3] GRUTESER M, GRUNWALD D. Anonymous usage of location based services through spatial and temporal cloaking [C] // **Proceedings of Mobile systems, Applications and Services**. San Francisco: ACM, 2003: 31-42.

[4] KIDO H, YANAGISAWA H. A anonymous communication technique using dummies for location-based services [C] // **Proceedings of ICPS**. Santorini: IEEE, 2005: 88-97.

[5] GHINITA G, KALNIS P, KHOSHGOZARAN A, et al. Private queries in location based services: anonymizers are not necessary [C] // **Proceedings of the ACM International Conference on Management of Data**. Vancouver: ACM, 2008: 121-132.

[6] BAMBA B, LIU L, PESTI P. Supporting anonymous location queries in mobile environments with privacy grid [C] // **Proceedings of World Wide Web**. Beijing: IEEE, 2008: 237-246.

[7] GEDIK B, LIU L. Protecting location privacy with personalized k-anonymity: architecture and algorithms [J]. **IEEE Transactions on Mobile Computing**, 2008, 7(1): 1-17.

[8] XU J, TANG X, HU H, et al. Privacy-conscious location-based queries in mobile environments [J]. **IEEE Transactions on Parallel and Distributed Systems**, 2010, 21(3): 313-326.

[9] KYRIAKOS M, YIU M. Anonymous query processing in road networks [J]. **IEEE Transactions on Knowledge and Data Engineering**, 2010, 22(1): 2-15.

[10] BALAJI P, LIU L. MobiMix: protecting location privacy with mix zones over road networks [C] // **Proceedings of IEEE International Conference on Data Engineering (ICDE)**. Hannover: IEEE, 2011: 11-16.

[11] GHINITA G, KALNIS P, SKIADOPOULOS S. PRIVE: anonymous location-based queries in distributed mobile systems [C]// **Proceedings of World Wide Web**. Banff: ACM, 2007: 371-380.

[12] CHOW Chi-yin, MOHAMED M, XUAN L. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments [J]. **GeoInformatica**, 2011,15(2): 351-380.

[13] AMIR A, EFRAT A, MYLLYMAKI J, et al. Buddy tracking: efficient proximity detection among mobile friends [C] // **Proceedings of IEEE INFOCOM**. Hong Kong: IEEE, 2004: 7-11.

[14] YIU M L, YU L H, SALTENIS S, et al. Efficient proximity detection among mobile users via selftuning policies [C]// **Proceedings of VLDB**. Singapore: ACM, 2010: 13-17.

[15] HUBAUX J P, CAPKUN S, LUO J. The security and privacy of smart vehicles [J]. **IEEE Security and Privacy**, 2004(3): 49-55.

[16] KU W S, ZIMMERMANN R, WANG H. Location-based spatial query processing with data sharing in wireless broadcast environments [J]. **IEEE Transactions on Mobile Computing**, 2008, TMC 7(6): 778-791.

[17] THOMAS B. Generating network-based moving objects [C] // **Proceedings of International Conference on Scientific and Statistical Database Management**. Berlin: IEEE, 2000: 253-256.