文章编号:1007-5321(2018)06-0097-06 DOI:10.13190/j.jbupt.2018-046

基于 DTW 交换查询的轨迹隐私保护方案

宋 成, 张亚东, 王 磊, 刘志中, 晁 浩
(河南理工大学 计算机科学与技术学院, 河南 焦作 454003)

摘要: 针对轨迹数据的攻击性推理可能导致个人隐私信息泄露的问题,提出了一个基于动态时间归整(DTW)交换查询的轨迹隐私保护方案. 通过对基于位置的服务(LBS)请求的用户及候选者身份进行匿名化处理,利用 DTW 算法依次计算出所有候选者与发起者在一定时间间隔内的轨迹相似值,从中选出最优相似轨迹的候选者替代真实用户请求 LBS 服务,从而实现用户身份与位置的隐私保护. 经过安全性分析,所提方案不仅满足匿名性和不可伪造性等安全特性,而且能够抵抗窃听攻击和连续查询服务追踪攻击. 仿真实验结果表明,所选候选者轨迹的相似度有明显提高.

关 键 词: 基于位置的服务; 动态时间归整; 轨迹隐私保护; 交换查询
中图分类号: TP309 **文献标志码**: A

Trajectory Privacy Protection Scheme Based on DTW Exchange Query

SONG Cheng, ZHANG Ya-dong, WANG Lei, LIU Zhi-zhong, CHAO Hao
(College of Computer Science and Technology, Henan Polytechnic University, Henan Jiaozuo 454003, China)

Abstract: In order to solve the problem of personal privacy information disclosure caused by aggressive reasoning of the trajectory data, based on dynamic time warping (DTW) exchange query, a trajectory privacy protection scheme is proposed. Through anonymizing the identities of user and candidates who request location-based service (LBS), and calculating the trajectory similarity between all candidates and the initiator within acertain period of time by using the DTW algorithm, then choosing the candidate with the optimal trajectory similarity to replace real user in requesting LBS, the real user privacy information about identity and location is effectively protected. Security analyses prove that this scheme not only satisfies the security characteristics such as privacy, anonymity, and unforgeability, but also can resist query service tracking attack. Simulation experiments show that the optimal trajectory similarity is significantly improved.

Key words: location based services; dynamic time warping; trajectory privacy protection; exchange query

随着无线通信、全球定位系统和智能移动终端的迅猛发展,用户能够随时随地享受基于位置的服务(LBS, location based services)[1-3]带来的各种便利. 然而,在传统 LBS 请求中,移动终端用户请求信息若被攻击者窃听,相关隐私信息[4-5]将会泄露. 当前,尽管一些学者针对用户位置隐私问题做了一些研究[6-8],但深入研究发现,仅防止位置信息泄露已不能满足用户的需求. 因此,在保护用户位置隐私的基础上,如何防止攻击者根据位置时空的关联性推断用户隐私信息成为亟待解决的问题[9-10]. 针对该问题,笔者提出了一个基于动态时间归整(DTW, dynamic time warping)交换查询的轨迹隐私保护方

收稿日期: 2018-03-20
基金项目: 国家自然科学基金项目(61300124, 61300216, 61772159); 河南省科技攻关计划项目(172102310677, 182102110333)
作者简介: 宋 成(1980—), 男, 讲师, 硕士生导师, E-mail:songcheng@hpu.edu.cn.

案. 该方案在匿名 LBS 请求用户及候选者身份基础上,采用 DTW 算法,计算所有候选者与发起者一定时间间隔内的轨迹相似值,并由相似度最高的最优候选者替代真实用户请求 LBS 服务.

1 相关工作

近年来,一些学者在移动终端用户轨迹隐私保护方面做了大量的研究工作. Gruteser 和 Liu[11] 根据区域内对象多少将其划分为敏感区域和非敏感区域,通过对敏感区域内的用户进行抑制或延迟位置更新的方法来保护其轨迹隐私. Terrovitis 和 Mamoulis[12] 通过迭代抑制的方法从轨迹中选择满足隐私约束的位置,由于轨迹被抑制造成信息大量受损,导致服务质量下降. Chen 等[13] 通过量身定制的隐私模型局部抑制方法减少信息受损. 赵婧等[14] 通过向敏感轨迹数据集中添加假数据或局部抑制的方法,提出一种基于轨迹频率抑制的隐私保护方案. 随后,Dai 和 Hua[15] 提出一种基于分段假弹道的虚拟轨迹生成方案. 以上方案均基于虚拟轨迹模糊和抑制思想,尽管实现简单,效率较高,但隐私级别相对较低. 针对此问题,学者们又提出了一些基于轨迹匿名的方案. Chow 和 Mokbel[16] 提出一个 k-匿名区域共享方案,通过包含其他 $k-1$ 个相同用户连续查询,LBS 服务器无法辨别真实用户. Kato 等[17] 以用户移动特征信息预知为前提,提出一种虚拟匿名化轨迹隐私保护方案,但轨迹相似度有待进一步提高. 2014 年,Hwang 等[18] 提出一种基于用户隐私信息的综合弹道隐私方案,通过预处理一组类似轨迹来模糊用户的真实轨迹,同时引入时间模糊技术,由于每次预处理计算量较大,导致效率偏低. Schlegel 等[19] 提出一个用户自定义的隐私网格系统,满足了快照和持续 LBS 查询隐私保护的基本要求,但需要第三方辅助实现. 李凤华等[20] 提出一种高效的轨迹隐私保护方案,基于地图背景信息、轨迹相似性以及用户行动模式等特征来构建 $k-1$ 条虚假轨迹,以致攻击者无法分辨出其真实轨迹,进而保证终端轨迹隐私安全. Peng 等[21] 提出一个基于连续查询的协作轨迹隐私保护方案. 以上 3 个方案均未考虑通信保密问题.

2 预备知识

2.1 轨迹隐私保护系统模型

如图 1 所示,轨迹隐私保护系统模型主要由移动终端、可信匿名服务器和 LBS 服务器 3 部分实体组成. 每部分实体的功能如下.

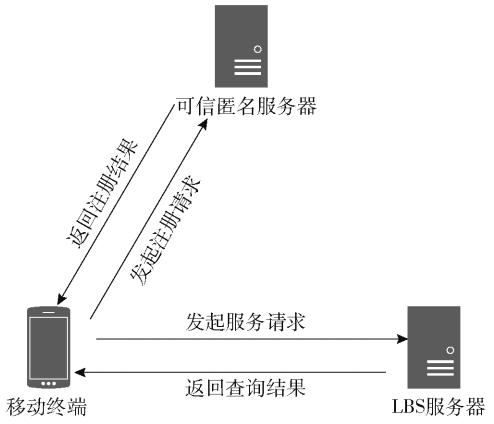

图 1 轨迹隐私保护系统模型

1) 移动终端. 移动终端具有 2 个功能:一是向可信匿名服务器发送匿名化请求并验证匿名的有效性;二是发送 LBS 请求,并接收服务查询的结果.

2) 可信匿名服务器. 在匿名位置隐私保护中,通常需配置一个可信匿名服务器. 可信匿名服务器保存用户属性矩阵信息,并处理移动终端请求,为移动终端寻找最优候选者,发布系统参数等.

3) LBS 服务器. LBS 服务器是轨迹隐私保护系统的核心部分,负责处理来自移动终端的匿名化查询,并将查询结果反馈给移动终端.

2.2 轨迹数据集

对于一个运动对象 A,其运动轨迹 T_A 是一组在采样时间内的离散位置,而轨迹数据集 T 是所有用户轨迹序列的集合,表示为:$T=\{T_k\},k=1,2,\cdots$. 其中,T_k 为用户 i 的运动轨迹. 每个用户 k 的运动轨迹 T_k 是由 n 个不同时刻 t_i 的位置序列组成,表示为:$T_k=\{\mathrm{ID}_k,(x_1,y_1,t_1),(x_2,y_2,t_2),\cdots,(x_n,y_n,t_n)\}$. 其中,$t_1<t_2<\cdots<t_n$,$\mathrm{ID}_i$ 表示用户的匿名身份,(x_i,y_i) 为对象在 t_i 时刻的位置,t_i 为采样时的时间.

2.3 动态时间归整算法

DTW 算法是针对传统算法对采样过于苛刻的问题而设计的,通过采用重复之前的记录点填补对应空缺的方式,求出最小距离作为轨迹的相似性度量. 设序列 $L=\{l_1,l_2,\cdots,l_m\}$ 和序列 $H=\{h_1,h_2,\cdots,h_n\}$ 分别表示两条轨迹的空间域离散采样,其中,$m>1,n>1$. 为了对齐 L 和 H 内的元素,需要构造一个 $m\times n$ 的矩阵,矩阵元素 (i,j) 分别表示 l_i 和 h_j 2 点的欧氏距离 $\mathrm{Dist}(l_i,h_j)$,即欧几里得距离. 2 条

轨迹间的相似度表示为:$\mathrm{DTW}(L,H)=D(m,n)$. 其中 $D(i,j)$ 满足:$D(i,j)=\mathrm{Dist}(i,j)+\min\{D(i-1,j),D(i-1,j),D(i-1,j-1)\}$. $D(i,j)$ 表示序列 L 与 H 之间的规整路径距离.

3　轨迹隐私保护方案

3.1　系统初始化

系统初始化阶段主要生成系统参数,具体步骤如下.

第 1 步　G_1、G_2 分别为 2 个阶为素数 q 的加法循环群和乘法循环群,P 是为 G_1 的生成元. $e:G_1\times G_1\rightarrow G_2$ 表示一个双线性映射. Z_q^* 表示模 q 的整数乘法群.

第 2 步　定义 2 个安全哈希函数:$H_1:\{0,1\}^*\rightarrow G_1^*$,$H_2:\{0,1\}^*\rightarrow\{0,1\}^k$. 其中,$\{0,1\}^*$ 表示任意长度的二进制串,k 为一个整数.

第 3 步　可信匿名服务器选取系统主密钥 $s\in Z_q^*$,计算其公钥为 $\mathrm{PK}_{\mathrm{anon}}=sP$.

第 4 步　可信匿名服务器保存系统主密钥 s,公开系统参数:$\{G_1,G_2,e,k,n,P,\mathrm{PK}_{\mathrm{anon}},H_1,H_2\}$.

3.2　注册

注册阶段主要实现身份匿名化,具体步骤如下.

第 1 步　移动终端将其真实身份 ID 作为注册请求消息发送给可信匿名服务器.

第 2 步　可信匿名服务器随机生成一个 $m\times n$ 矩阵 $\boldsymbol{Z}(2\leqslant m<n)$ 和一个 m 维的列向量 $\boldsymbol{p}$,满足 $R(\boldsymbol{Z})=R(\overline{\boldsymbol{Z}})$,且 $R(\boldsymbol{Z})<n$.

第 3 步　可信匿名服务器为每个用户生成一个唯一 n 维列向量 $\boldsymbol{d}_i$,且满足 $\boldsymbol{Z}\boldsymbol{d}_i=\boldsymbol{p}$,并随机选取一个 n 维列向量 $\boldsymbol{D}$,计算用户 u 的假身份 $\mathrm{PID}_u=\boldsymbol{D}^{\mathrm{T}}\boldsymbol{d}_i$,参数 $Q_u=H_1(\mathrm{PID}_u)$ 和 $X_u=sQ_u$,然后将 $\{\mathrm{PID}_u,X_u,\boldsymbol{d}_i\}$ 通过安全信道返回给用户.

第 4 步　用户 u 收到消息后,计算 $\widetilde{Q}_u=H_1(\mathrm{PID}_u)$,并判断 $e(X_u,P)\stackrel{?}{=}e(\widetilde{Q}_u,\mathrm{PK}_{\mathrm{anon}})$ 若等式成立,用户 U 将 X_u 作为其部分私钥,并随机选择 $r_u\in Z_q^*$,计算其私钥 $\mathrm{SK}_u=r_uX_u$ 和公钥 $\mathrm{PK}_u=\langle V_u,Y_u\rangle$,其中,$V_u=r_uP$,$Y_u=r_u\ \mathrm{PK}_{\mathrm{anon}}$;否则,返回第 1 步.

3.3　DTW 轨迹相似度计算

设 $L_u=\{l_u^1,l_u^2,l_u^3,\cdots,l_u^m\}$ 和 $H_c=\{h_c^1,h_c^2,h_c^3,\cdots,h_c^n\}$ 分别为发起者和候选者运动轨迹的离散采样. 可信匿名服务器通过 DTW 算法依次计算出发起者与候选者的轨迹相似值,步骤如下.

第 1 步　根据点间的欧氏距离,生成序列距离矩阵 $\boldsymbol{M}_{n\times m}$,其中行对应 L_u,列对应 H_c,矩阵元素为对应 L_u 和 H_c 中对应点的欧氏距离.

第 2 步　根据 $\boldsymbol{M}_{m\times n}$ 计算损失矩阵 $\boldsymbol{M}_c$,$\boldsymbol{M}_c$ 第 1 行第 1 列元素为矩阵 $\boldsymbol{M}_{m\times n}$ 第 1 行第 1 列的元素. 其余位置元素的计算方法为:$M_c(i,j)=\min\{M_c(i-1,j),M_c(i-1,j-1),M_c(i,j-1)\}+M(i,j)$. 元素 $\boldsymbol{M}_c(m,n)$ 为 L_u 与 H_c 的轨迹相似度.

第 3 步　利用同样方法分别求出真实轨迹与其他候选轨迹相同时间间隔 Δt 内轨迹的相似度.

3.4　查询交换的位置服务请求

查询交换的位置服务请求阶段主要挑出最优候选者,由候选者替代用户请求 LBS 服务. 具体步骤如下.

第 1 步　终端用户 u 发起广播,获取一定范围内候选用户匿名身份 $\{\mathrm{PID}_{n1},\mathrm{PID}_{n2},\mathrm{PID}_{n3},\cdots,\mathrm{PID}_{nk}\}$,计算 $\mathrm{MEG}_{\mathrm{uo}N}=\{E_{\mathrm{PK}_{\mathrm{anon}}}(\mathrm{PID}_u,\mathrm{PID}_{n1},\mathrm{PID}_{n2},\cdots,\mathrm{PID}_{nk}),E_{\mathrm{PK}_S}(\mathrm{Loc}_u,Q_u,K_s)\}$ 并发送给可信匿名服务器. 其中,$E_k(\ )$ 为加密函数,PK_s 为 LBS 服务器公钥,Loc_u、Q_u、K_s 分别表示位置、请求内容、用户与 LBS 服务器的会话秘钥.

第 2 步　可信匿名服务器接收到请求后,随机选择 $i\in Z_q^*$,计算 $\boldsymbol{I}=i\boldsymbol{Z}$ 和 $\boldsymbol{r}=i\boldsymbol{p}$,并将消息 $\{t_1,\boldsymbol{I},H_2(\boldsymbol{r}\parallel\mathrm{ID}_{\mathrm{Tu}}\parallel t_1\parallel t_2)\}$ 发送给终端用户 u,其中 $\mathrm{ID}_{\mathrm{Tu}}$ 为可信匿名服务器的身份标识,t_1 表示时间戳.

第 3 步　用户 u 接收到消息后,计算 $\boldsymbol{R}=\boldsymbol{I}\boldsymbol{d}_i$,验证等式 $H_2(\boldsymbol{R}\parallel\mathrm{ID}_{\mathrm{Tu}}\parallel t_1)\stackrel{?}{=}H_2(\boldsymbol{r}\parallel\mathrm{ID}_{\mathrm{Tu}}\parallel t_1)$,若等式成立,计算 $\{t_2,H_2(\boldsymbol{R}\parallel\mathrm{ID}_{\mathrm{Tu}}\parallel t_1\parallel t_2)\}$,并将其发送给可信匿名服务器,$t_2$ 表示时间戳.

第 4 步　可信匿名服务器接收到消息后,验证等式 $H_2(\boldsymbol{R}\parallel\mathrm{ID}_{\mathrm{Tu}}\parallel t_1\parallel t_2)\stackrel{?}{=}H_2(\boldsymbol{r}\parallel\mathrm{ID}_{\mathrm{Tu}}\parallel t_1\parallel t_2)$,若成立,则解密消息 $E_{\mathrm{PK}_{\mathrm{anon}}}(\mathrm{PID}_u,\mathrm{PID}_{n1},\mathrm{PID}_{n2},\cdots,\mathrm{PID}_{nk})$;然后基于轨迹相似度挑出最优候选者 B,计算 $\mathrm{MEG}_{\mathrm{NoB}}=\{E_{\mathrm{PK}_B}(\mathrm{PID}_u),E_{\mathrm{PK}_S}(\mathrm{Loc}_u,Q_u,K_s)\}$,其中 PK_B 表示候选者 B 的公钥;最后将数据包 $\mathrm{MEG}_{\mathrm{NoB}}$ 发送给 $\mathrm{MEG}_{\mathrm{BoS}}$ 并告之替代用户 u 发起 LBS 请求.

第 5 步　B 收到消息后通过解密获取 PID_u,并计算 $\mathrm{MEG}_{\mathrm{BoS}}=\{E_{\mathrm{PK}_S}(\mathrm{PID}_B),E_{\mathrm{PK}_S}(\mathrm{Loc}_u,Q_u,K_s)\}$,然后将 $\mathrm{MEG}_{\mathrm{BoS}}$ 发送给 LBS 服务器.

第 6 步　LBS 服务器收到数据包后解密 $\mathrm{MEG}_{\mathrm{BoS}}$,获取查询请求内容,并计算 $\mathrm{MEG}_{\mathrm{SoB}}=$

$\{E_{PK_B}(PID_B), En_{K_S}(MEG)\}$,其中$En_{K_S}(\ )$表示对称加密函数;然后将$MEG_{SoB}$发送给 B.

第7步 B 收到消息后,计算$MEG_{Bou}=\{E_{PK_u}(En_{K_S}(MEG))\}$,其中$PK_u$表示用户 u 的公钥,然后将MEG_{Bou}发送给 u.

第8步 用户 u 接收到信息后解密MEG_{Bou}获取查询结果 MEG.

4 安全性分析

4.1 匿名性

定义1 匿名游戏.

第1步 攻击者发起询问获取系统公共参数:$\{G_1, G_2, e, k, n, P, PK_{anon}, H_1, H_2\}$和必要的参数信息.

第2步 攻击者选取2个完全不同的LBS服务请求加密信息 m_0 和 m_1.

第3步 选取随机位 $b\in\{0,1\}$,并将 m_b 和 m_{1-b}随机发送给两个最优候选者 B_1 和 B_2,b 对于攻击者是保密的.

第4步 LBS服务器分别为 B_1 和 B_2 查询所请求的信息结果MEG_b 与MEG_{1-b}.

第5步 如果 B_1 与 B_2 输出2个加密的查询结果MEG_b 与MEG_{1-b}分别与加密信息 m_0 与 m_1 所请求的内容相对应,然后将MEG_b 与MEG_{1-b}按照随机顺序发送给攻击者;否则,返回$\perp$给攻击者.

第6步 攻击者对 MEG_b 进行解密输出真正发出LBS服务请求的用户信息,则攻击者赢得这场游戏.

定理1 假设在轨迹隐私保护方案中攻击者 A 在匿名游戏中以可以忽略的概率赢得游戏,则该方案满足匿名性.

证明 攻击者 A 作为定义1中匿名游戏的攻击者,如果在第5步中收到是$\perp$,则表明攻击者 A 不能获取任何有用的信息. 考虑另一种情况,假设攻击者 A 获取了2个加密后的请求查询结果:

$$MEG_{SoB_1}=\{E_{PK_{B_1}}(PID_{B_1}), En_{K_S}(MEG_b)\}$$

$$MEG_{SoB_2}=\{E_{PK_{B_2}}(PID_{B_2}), En_{K_S}(MEG_{1-b})\}$$

由于本文方案中所有参与者之间的通信进行了加密处理. 若攻击者 A 预通过解密数据包MEG_{SoB_1}来获取用户的身份信息,需要通过计算 $X_{B_1}=sQ_{B_1}$ 和$SK_{B_1}=r_{B_1}X_{B_1}$得到其解密密钥SK_{B_1},而该计算过程将面临求解椭圆曲线离散对数难题,即攻击者 A 通过解密方式获取请求结果信息等价于破解椭圆曲线离散对数难题,其在计算上是不可行,故攻击者 A 赢得游戏的概率:$Adv(A)=|Pr[A]|$ 是可以忽略不计的. 因此攻击者 A 在匿名游戏中以可忽略的概率赢得游戏. 方案中每次LBS请求均由不同的最优的候选者替代,隐藏了发起者的身份信息,因此进一步提高方案的匿名性.

4.2 不可伪造性

用户注册阶段,可信匿名服务器为用户的真实身份进行匿名化,生成可验证性的假身份PID_u,注册用户获取信息$\{PID_u, X_u, \boldsymbol{d}_i\}$后,用户计算 $\widetilde{Q}_u=H_1(PID_u)$并判断等式 $e(X_u,P)\stackrel{?}{=}e(\widetilde{Q}_u, PK_{anon})$. 若攻击者冒充可信匿名服务器伪造用户注册信息,在没有获得可信匿名服务器私钥 s 的情况下,该等式无法成立. 如果攻击者设法获取可信匿名服务器私钥 s,则需要通过可信匿名服务器公钥信息(P, PK_{anon}),根据等式$PK_{anon}=sP$ 推导私钥 s,即面临求解椭圆曲线离散对数难题.

4.3 防窃听攻击

用户和LBS服务器之间的无线通信容易被攻击者监视和窃听,本文方案通过加密方式来解决窃听攻击. 当最优的候选者与LBS进行通信时,最优候选者 B 的PID_B 和发起者 u 的请求信息(Loc_u, Q_u, K_s)使用LBS服务器的公钥PK_S 加密,确保请求信息和会话秘钥 K_s 的保密性. 当LBS返回查询结果时,使用会话秘钥 K_s 对查询结果加密,并使用LBS服务器的公钥PK_S 对最优候选者 B 的PID_B 进行加密处理,确保用户的信息和身份不被泄露.

4.4 抵抗查询追踪攻击

查询追踪攻击也称为连续查询攻击. 本文方案通过最优候选者替代发起者请求LBS服务,发起者的身份完全由候选者的身份替代. 在LBS服务器的查询记录信息中,仅记载了最优候选者的身份信息;同时,用户移动轨迹上不同时间间隔内代替其发出LBS服务请求的最优候选者是不固定,攻击者无法通过查询用户交集推断其关联性. 设用户在移动轨迹上连续查询的次数为 k 次,每次参入请求的候选者个数为 n_i,其中 $1\leqslant i\leqslant k$,由于每次查询过程中最优候选者不同,即不同的匿名区域候选者相互独立. 设攻击者截获用户 u 和候选者之间的通信并解密消息的概率为 $Pr(E)$,根据PID_u 求解 d_i 的概率为 $Pr(ID)$,假设攻击者获取移动终端用户向匿名服务

器注册请求消息，那么连续查询过程中实现用户追踪的概率为 $\prod_{i=1}^{k}\frac{1}{n_i}\Pr(E)\Pr(\mathrm{ID})$. $\Pr(E)$ 等价于破解椭圆曲线密码体制，在计算上是不可行. $\Pr(\mathrm{ID})$ 等价于已知 PID_u，根据等式 $\mathrm{PID}_u=\boldsymbol{D}^{\mathrm{T}}\boldsymbol{d}_i$ 求解 $\boldsymbol{d}_i$，而 $\boldsymbol{D}$ 是可信匿名服务器随机选取的一个 n 维列向量，求解 $\boldsymbol{d}_i$ 的概率可忽略，同时方程 $\boldsymbol{Zd}=\boldsymbol{p}$ 有无穷解，攻击者也无法通过矩阵方程确定 $\boldsymbol{d}_i$. 综上分析，攻击者获取请求者真实身份的概率可忽略.

5　仿真结果

仿真实验在 Intel i5 CPU 处理器、8 GB 内存、Windows7 64 位操作系统、Matlab 仿真软件和移动对象生成器 Thomas Brinkhoff 环境下进行 . 假设具备一个理想的网络环境，Thomas Brinkhoff 首先生成大量的移动对象的轨迹数据，然后随机选取某一移动对象作为发起者，通过 DTW 相似轨迹求解算法和交换查询算法来实现用户轨迹的混淆，进而保护用户的轨迹隐私. 为了确保实验结果的真实性，以下所有的实验结果均为 1 000 次运行的平均值. 如图 2 所示，在候选者一定的情况下，处理时间开销随着用户和轨迹段点数的增加而增加. 例如，当候选者 $K=5$ 时，轨迹段的点数 N 从 2 增加到 10，算法的处理时间从 18 ms 增加到 41 ms，这表明处理时间与轨迹段上的点的数量成正比关系. 在轨迹段点数一定的情况下，处理时间随着候选者个数的增加而增加，如当 $N=3$ 时，候选者个数为 5、10 和 15，所需要的处理时间分别为 21 ms、25 ms 和 31 ms. 由于增加用户的候选者个数或者轨迹段内点数，用户需要匹配一定范围内的更多的候选者用户，导致增加一定的时间开销. 需要注意，本文方案在实际应用场景中需要满足候选用户个数 $K\geqslant 2$ 和轨迹段上的点数 $N\geqslant 2$. 如果请求用户所在环境过于稀疏，如 $K=0$，周围无候选者；若 $K=1$，无需调用 DTW 算法，直接替代用户请求服务，攻击者可以通过候选者的连续查询进行跟踪. 如果轨迹段上的采样点数 $N=1$，那么该轨迹段由该采样点来替代，显然，一个点无法确定轨迹段的相似性.

实验结果如图 3 所示，3 个方案中，候选者个数 K 对最优轨迹相似度影响均不大. 在候选者个数 K 相同的情况下，随机选择方案的相似度效果最差，文献[17]次之，本文方案相似程度最高. 因为随机方案不考虑用户的行动模式和趋势等因素，仅随机地

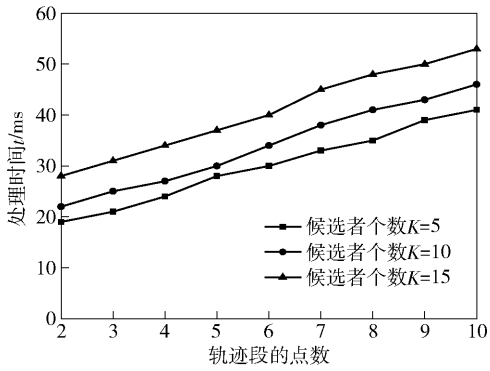

图 2　候选者个数和轨迹段的点数与时间的关系

生成虚假轨迹；文献[17]中在生成虚假轨迹时考虑了用户在每一次停顿后继续行进的方向和可达性等因素，使得所生成虚假轨迹与用户真实的轨迹的相似度有所提高；本文方案通过轨迹采样，然后根据 DTW 算法选择最优相似轨迹，该算法采用重复之前的记录点填补对应空缺位置的方式来计算两条轨迹间的相似度，参与计算的两条轨迹的采样点不需在时间间隔和采样点数一一对应，避开了传统的基于欧式距离轨迹相似度算法，同时，由于该方案采样时间间隔较短，采样点数较多，所以所选最优候选者轨迹相对于文献[17]的方案更接近用户的真实轨迹.

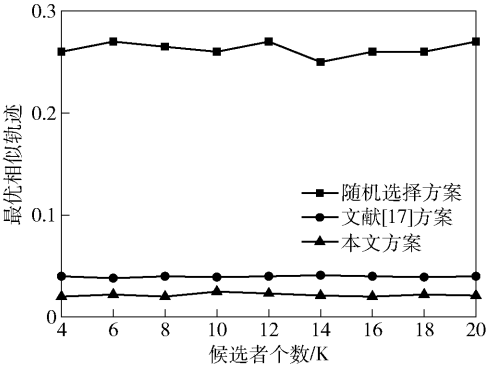

图 3　最优轨迹相似度比较

6　结束语

针对攻击者根据用户运动轨迹数据进行逻辑性推理可能造成个人隐私信息泄露的问题，提出了一个基于 DTW 交换查询的轨迹隐私保护方案. 通过对 LBS 服务请求的用户及候选者身份进行匿名化处理，并采用 DTW 算法挑选最优相似轨迹候选者替代真实用户进行 LBS 服务请求，从而解决用户的身份和位置隐私问题. 通过安全性分析，本文方案不仅满足匿名性和不可伪造性等安全特性，而且还

能抵抗窃听攻击和连续查询攻击. 对本文方案候选者个数和轨迹段的点数对算法所需时间以及不同方案相似度进行仿真实验,结果表明,本文方案所选最优候选者与真实用户在一定时间间隔内轨迹相似程度明显优于其他方案. 因此,本文方案在移动用户隐私保护环境中有着重要的理论意义和应用价值.

参考文献:

[1] Gartner G, Huang Haosheng. Progress in location-based services 2014[M]. Berlin: Springer International Publishing, 2015.

[2] Sun Yanming, Chen Min, Hu Long, et al. ASA: against statistical attacks for privacy-aware users in location based service[J]. Future Generation Computer Systems-the International Journal of eScience, 2017(70): 48-58.

[3] Li Xinghua, Miao Meixia, Liu Hai, et al. An incentive mechanism for *K*-anonymity in LBS privacy protection based on credit mechanism[J]. Soft Computing, 2017, 21(14): 3907-3917.

[4] Huo Zheng, Meng Xiaofeng. A survey of trajectory privacy-preserving techniques[J]. Chinese Journal of Computers, 2011, 34(10): 1820-1830.

[5] He Wen. Research on LBS privacy protection technology in mobile social networks[C]//IEEE Advanced Information Technology, Electronic and Automation Control Conference. New York: IEEE Press, 2017: 73-76.

[6] Khoshgozaran A, Shahabi C, Shirani-Mehr H. Location privacy: going beyond *K*-anonymity, cloaking and anonymizers[J]. Knowledge and Information Systems, 2011, 26(3): 435-465.

[7] Zhang Yuan, Chen Qingjun, Zhong Sheng. Privacy-preserving data aggregation in mobile phone sensing[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(5): 980-992.

[8] 万盛, 李凤华, 牛犇, 等. 位置隐私保护技术研究进展[J]. 通信学报, 2016, 37(12): 124-141.
Wan Sheng, Li Fenghua, Niu Ben, et al. Research progress on location privacy-preserving techniques[J]. Journal on Communications, 2016, 37 (12): 124-141.

[9] Lee K C K, Zheng Baihua, Chen C, et al. Efficient index-based approaches for skyline queries in location-based applications[J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(11): 2507-2520.

[10] Tai F Y, Song Jiankai, Tsai Y C, et al. Cloaking sensitive patterns Td preserve location privacy for LBS applications[C]//IEEE International Conference on Consumer Electronics-Taiwan. New York: IEEE Press, 2016: 1-2.

[11] Gruteser M, Liu Xuan. Protecting privacy in continuous location-tracking applications[J]. IEEE Security and Privacy, 2004, 2(2): 28-34.

[12] Terrovitis M, Mamoulis N. Privacy preservation in the publication of trajectories[C]//International Conference on Mobile Data Management. New York: IEEE Press, 2008: 65-72.

[13] Chen Rui, Fung B C M, Mohammed N, et al. Privacy-preserving trajectory data publishing by local suppression[J]. Information Sciences, 2013(231): 83-97.

[14] 赵婧, 张渊, 李兴华, 等. 基于轨迹频率抑制的轨迹隐私保护方法[J]. 计算机学报, 2014, 37(10): 2096-2106.
Zhao Jing, Zhang Yuan, Li Xinghua, et al. A trajectory privacy protection approach via trajectory frequency suppression[J]. Chinese Journal of Computers, 2014, 37(10): 2096-2106.

[15] Dai Jiazhu, Hua Liang. A method for the trajectory privacy protection based on the segmented fake trajectory under road networks[C]//International Conference on Information Science and Control Engineering. New York: IEEE Press, 2015: 13-17.

[16] Chow C Y, Mokbel M F. Enabling private continuous queries for revealed user locations[C]//International Symposium on Advances in Spatial and Temporal Databases. Berlin: Springer, 2007: 258-275.

[17] Kato R, Iwata M, Hara T, et al. A dummy-based anonymization method based on user trajectory with pauses[C]//International Conference on Advances in Geographic Information Systems. New York: ACM, 2012: 249-258.

[18] Hwang R H, Hsueh Y L, Chung H W. A novel time-obfuscated algorithm for trajectory privacy protection[J]. IEEE Transactions on Services Computing, 2014, 7(2): 126-139.

[19] Schlegel R, Chow C Y, Huang Qiong, et al. User-defined privacy grid system for continuous location-based services[J]. IEEE Transactions on Mobile Computing, 2015, 14(10): 2158-2172.

[20] 李凤华, 张翠, 牛犇, 等. 高效的轨迹隐私保护方案[J]. 通信学报, 2015, 36(12): 114-123.
Li Fenghua, Zhang Cui, Niu Ben, et al. Efficient trajectory privacy protection scheme [J]. Journal of Communications, 2015, 36(12): 114-123.

[21] Peng Tao, Liu Qin, Meng Dacheng, et al. Collaborative trajectory privacy preserving scheme in location-based services[J]. Information Sciences, 2017(387): 165-179.