一种连续查询事件中基于语义的轨迹 k-匿名方法

何远德[1] 黄奎峰[2*]

[1](西南民族大学语言实验教学中心 四川 成都 610041)

[2](重庆三峡医药高等专科学校 重庆 404120)

摘 要 针对传统的轨迹 k-匿名方法难以防范以连续查询为背景知识的攻击问题,利用事件本体对轨迹连续查询进行形式化表示的优点,提出一种连续查询事件中基于语义的轨迹 k-匿名方法。该方法引入 OWL(Ontology Web Language)形式化表示关于轨迹查询事件,构建基于事件本体的轨迹匿名模型;利用轨迹片段相似度计算和 Jena 推理引擎,给出基于 k-匿名查询事件的轨迹聚类方法,实现关于当前轨迹的虚假匿名组。实验表明,与传统方法相比,该方法的信息损失率降低了 15% ~20%,查询精准率保持在 75% 以上,执行时间减少约 20 秒,较好地维持轨迹数据匿名的有效性和可扩展性。

关键词 轨迹 k-匿名 连续查询事件 事件本体 轨迹聚类

中图分类号 TP391 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.08.052

A TRACK K-ANONYMITY METHOD BASED ON SEMANTIC FOR CONTINUOUS QUERY EVENTS

He Yuande[1] Huang Kuifeng[2*]

[1](*Language Experiment Teaching Center, Southwest University for Nationalities, Chengdu 610041, Sichuan, China*)

[2](*Chongqing Three Gorges Medical College, Chongqing 404120, China*)

Abstract Traditional trajectory k-anonymity method is difficult to prevent attacks by background knowledge of consecutive queries. In the view of this, based on the advantage of event ontology in formalizing continuous trajectory query, we proposed a trajectory k-anonymity based on semantic for consecutive query events. This paper introduced OWL to formulae the data query events about trajectories, and established a trajectory anonymity model based on event ontology. Using the similarity calculation of trajectory fragments and Jena reasoning engine, we gave a trajectory clustering method based on k-anonymity query events to realize the false anonymous group of current trajectories. Experiments show that the proposed method reduces the information loss rate by 15% ~20%, keeps the query precision rate above 75%, reduces the execution time by about 20 s, and maintains the validity and scalability of anonymity of trajectory data.

Keywords Trajectory k-anonymity Consecutive query events Event ontology Trajectory clustering

0 引 言

轨迹匿名隐私保护技术是近年来网络空间安全领域研究的热点问题之一[1-3],常用的轨迹匿名技术主要是基于泛化方法的 k-匿名查询技术[4],该技术要求在发布数据中任一当前轨迹在以半径为 δ 的圆柱范围内,至少包含其他 $k-1$ 条轨迹,生成一个泛化后的数据包,向客户端提交虚假轨迹组,从而降低当前查询轨迹的辨识率。然而当用户在多个不同时刻 k-匿名区域时,例如 3 个连续查询事件,轨迹 $T_1=\{P_1、P_2、P_3、P_4\}$,轨迹 $T_2=\{P_3、P_4、P_6、P_7\}$,轨迹 $T_3=\{P_3、P_8、P_9、P_{10}\}$,攻击者比较容易推断发出查询事件请求的为 P_3 用户。

收稿日期:2018-11-23。中央高校基本科研业务费专项基金项目(2016NZYQN40);四川省科技厅项目(2016ZR0149)。**何远德**,实验师,主研领域:信息安全与理论,计算机网络与应用。**黄奎峰**,讲师。

针对传统的 k-匿名轨迹隐私保护方法不能直接应用于连续查询,学者们提出了不同的研究思路和观点。文献[5]将真实轨迹位置进行模糊处理,根据历史数据生成虚假用户,并提出了虚假轨迹的距离约束和相似性约束。文献[6]通过匿名框的泛化方法将最初在框中的轨迹继续保留在接下来多个连续查询匿名框中,以避免攻击者对数据信息的推断和识别。文献[7]针对关联查询攻击和运动模式推断攻击问题,利用路网顶点作为锚点提出一种路网兴趣点连续 KNN 查询隐私保护方法。以上三种方法都采用了匿名框或路网的方式进行隐私保护,但仅考虑轨迹位置与攻击点的匹配程度,忽略了背景知识的语义信息。通过空间关联因素推断并结合特定的领域背景知识,可以将查询条件作为关联最初匿名框的接口,从而对轨迹数据进行攻击,在语义背景下降低了 k-匿名的效果。文献[8]针对语义位置攻击和最大运行速度攻击,将语义轨迹隐私问题定义为 k-CS 匿名问题,实现基于图上顶点聚类的近似算法,进而对图上顶点进行匿名。但这种方法缺少对位置节点语义解释,缺少一个知识库模型,攻击者可以将查询兴趣点所在特定轨迹片段结构作为背景知识进行隐私攻击,构造出至少相同结构和属性的轨迹作为攻击候选集,使目标轨迹导致隐私泄露的概率大于 $1/k$,从而泄露与目标相关的信息[9]。

针对现有轨迹匿名模型难以防范以连续查询为背景知识的攻击问题,利用事件本体对轨迹连续查询进行形式化表示的优点,提出一种连续查询事件攻击中基于语义的轨迹匿名方法。该方法引入 OWL[10](Ontology Web Language)对轨迹的身份隐私、地理信息和敏感查询事件进行形式化表示,构建基于事件本体的轨迹匿名模型,利用轨迹综合相似性和 Jena 推理引擎,给出基于 k-匿名的轨迹聚类方法,实现关于当前轨迹的虚假匿名组,最后用实验验证本文方法的有效性和可扩展性。

1 问题定义与模型

1.1 连续查询事件

连续查询事件采用面向 Clique Cloaking[11-12]的方法,当前轨迹数据动态更新中发出连续查询事件时,攻击者通过快照 cm 列表的形式计算概率 $P(u_i \longrightarrow T_j)$ $(i,j=1,2,\cdots,k)$,找出可能发送的用户,其中 u_i 表示当前查询轨迹事件,T_j 表示当前用户的轨迹。对于每个轨迹的连续查询事件分为内容关联查询和结构相似查询。

定义 1 内容关联查询:存在一条轨迹 T 映射 F,当满足 $F:[(Q_i,\varepsilon_{Qi}),(loc_1,loc_2,\cdots,loc_n),Contex]\longrightarrow u_k$,则当前轨迹受到内容关联攻击,其中 Q_i 为查询内容,ε_{Qi}为 Q_i 的关联强度,$Contex$ 为背景知识。攻击者将查询内容 Q_i 作为轨迹 λ 中位置序列($loc_1,loc_2,\cdots,loc_n$)的关联因素,利用每一个位置 loc_i 发出的查询内容作为相同查询请求,ε 取值越大,位置间的关联程度越高,攻击者对构造 F 的可能性越高。

定义 2 结构相似查询:存在一条轨迹 T 映射 F,对于轨迹结构的每一个属性,诸如采样点序列、速度、形状、转角、加速等,攻击者通过对轨迹 T 的相似结构发现隐私数据。从结构相似性带来的轨迹攻击表示为:

$$F:[(S_i,\varepsilon_{Si}),(loc_1,loc_2,\cdots,loc_n),Contex]\longrightarrow u_k$$

其中:ε_{Si}强度由结构向量集合 S_i 一致性等因素决定,$Contex$ 包含攻击者通过结构属性获取轨迹知识,结构属性的一致性越高,攻击者构造出 F 的可能性越高。

1.2 事件本体[13]

事件本体技术能够描述某个事件行为的概念及概念之间的关系,形式化表示事件行为的语义逻辑,共享、集成、推理的性能,形成相互连接的无环超图。事件本体在特定的领域本体内,对某个特定时间或环境下发生的表现出的动作特征的形式化描述。通常用 <ECS,R,Rules> 表示,ECS 表示事件类集合,包含动作(Action)、对象(Objects)、时间(Time)、地点(Place)、内部状态(Status)和语言表现(Expression)6 个要素的知识单元。R 表示事件关系集合,Rules 采用描述逻辑语言表示事件之间的规则集合。本文针对用户在连续查询事件中存在被攻击者通过内容关联、结构特性和连续查询获取隐私问题,构建基于事件的本体模型 E-Ontology,用于抵御攻击者对轨迹数据的隐私窃取。

2 连续查询事件本体建模

2.1 连续查询事件本体模型

事件本体能够对轨迹连续查询进行可共享的明确的形式化规范化说明,本文根据事件本体定义,结合实际研究需求,扩展 <ECS,R,Rules> 模型,将其逻辑结构定义为一个五元组 E-Ontology = {Contexts, Events, Relations, Rules},其中:

(1) Contexts 是查询事件本体中的背景知识与概念分类集合,每个 Context 表示一个背景概念分类,包括轨迹位置信息、地理环境信息、用户身份和社交关系

信息等,所有 Context 构成一个查询事件背景知识的树形分类结构。

(2) Events 是查询攻击事件行为本体分类集合,存储各类攻击事件行为的实例及其属性。本文所述查询攻击事件行为包含内容集、对象集、时间段集、内部状态集和语言描述集等 5 个要素,其中,内部状态集包括触发条件集和结果集。

(3) Relations 表示概念与概念之间的关系集合,不同的事件之间通过关系,形成具有图结构的事件类网络。关系集合包括包含关系(is_a)、组成关系(isComposed of)、因果关系(causal)、并发关系(concurrence)、跟随关系(follow)。

(4) Rules 是由逻辑描述语言表示的规则集合,可以通过 Contexts、Events、Relations 的分类形成推理规则。

2.2　E-Ontology 构建

如图 1 所示,采用 OWL 对查询事件本体进行构建,OWL 具有较强的语义性和知识表达能力,可较好地支持 Jena 推理引擎。具体构建步骤如下:

(1) 定义基础信息类:基础信息类包括背景知识类和环境信息类,背景知识类(Contexts Class)为一定区域内的地理信息,包含路网顶点、区域、路段、标识、结构等要素,环境信息类包含气象环境(降水数据、能见度)和物理环境(压强、磁场)等要素,这些要素作为基础数据导入本体结构中形成离线的本体结构。从事件本体中自上而下抽象基本类及其层次关系,class 表示类中的本体概念,SubClass 表示子类,instance 表示查询事件的实例,例如 Channel 是 Line 的子类,Position1是 Channel 的实例。

(2) 定义事件类:不同的本体存在不同的抽象类,从多个事件类中抽取事件要素和事件关系,表示事件当前的状态信息和行为特征。例如"Move"是当前查询事件中轨迹的一个状态,它包括从当前路网顶点移出和移入的行为特征,用"InMove"和"OutMove"表示。当多次查询一条轨迹上的路网顶点($P_1, P_2, P_3, \cdots$)时,触发事件本体类中各项子类,遍历 $P_1, P_2, P_3, \cdots$在事件类中位置,若存在当前查询轨迹在 k 个匿名范围实例内的轨迹结构关系或关联因果关系,则进行报警请求。

(3) 设置事件实例:事件实例作为事件类和事件要素的扩充,包含事件发生的具体内容和属性,包含类型、关联强度、因素及约束条件阈值,用 Datatype Property表示,细化查询事件内容。当连续查询某个轨迹上的路网顶点时,将这些查询事件存入匿名集,并不断扩展事件实例库。

(4) 定义事件关系:① 包含关系,存在事件类 $EC_1 = \{E_1, C_{1A}, C_{1O}, C_{1T}, C_{1P}, C_{1S}, C_{1E}\}$ 和 $EC_2 = \{E_2, C_{2A}, C_{2O}, C_{2T}, C_{2P}, C_{2S}, C_{2E}\}$,存在 $EC_1 \in EC_2$,当且仅当 $C1F \wedge C2F \wedge C1I \in C2I \wedge C1A \wedge C2A$。包含关系存在于事件类之间,如查询路网线段事件与查询路网顶点事件属于包含关系,通常用 $R_{\text{is\_a}}$ 表示;② 组成关系,轨迹事件行为类 EC_1 中的一个实例由事件行为类 EC_2 中的某个实例组成时,则该事件行为类 EC_1 由事件类 EC_2 组成,如"敏感位置查询"由"身份信息查询事件"、"停留查询事件"、"离开查询事件"等组成。组成关系形式化为 R_{comp}。③ 因果关系,事件类 EC_1 的实例事件发生以一定的概率导致了事件类 EC_2 的实例事件发生,如果发生的概率大于某一阈值,则该两类事件类存在因果关系,形式化为 R_{cause}。例如恶意者攻击发现一条轨迹 T 上的某个位置 P 在连续查询事件出现,用户位置 P 的泄露导致身份隐私被获取,则该事件发生的实例为因果关系。④ 跟随关系,随着数据流的时间推移,事件类 EQ_1 实例和 EQ_2 实例先后发生,则为该两类事件存在跟随关系,形式化表示为 R_{follow}。例如查询轨迹中位置 P_1 的事件实例 EQ_1 后,进而查询位置 P_1 的事件实例用户出入信息动态 EQ_2。⑤ 并发关系,在一定时间段内,存在两个攻击事件同时发生或攻击事件发生重合,形式化为 $R_{\text{concurrence}}$。

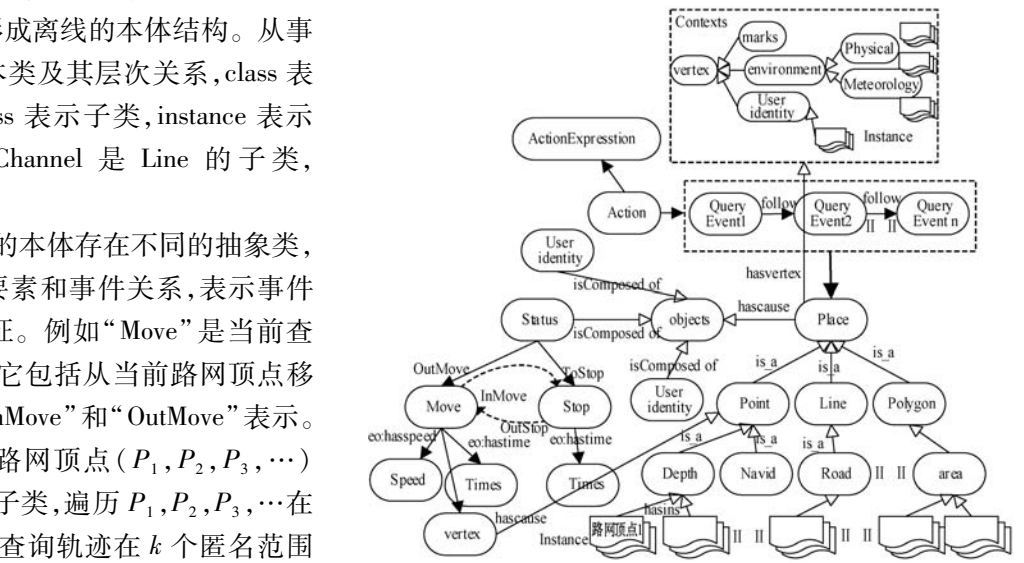

图 1　基于事件本体的轨迹匿名模型

3　基于 k-匿名查询的轨迹聚类方法

由于构建的事件本体模型 E-Ontology,在知识推理与服务方面建立在描述逻辑基础上,对动态事件特征的知识无法应用推理,而基于原子动作的动态描述

逻辑推理对本体事件要素的概念、关系、实例和公理的可满足性推理没有相关的系统框架可参照。因此,本文提出了一种基于 k-匿名查询的轨迹聚类算法,在计算轨迹片段相似度基础上,利用 KNN 在获取邻近轨迹的优点以及 Jena 引擎的推理能力,将与当前轨迹相似的 k 条轨迹进行聚类,从而形成关于当前轨迹的虚假轨迹匿名组。

3.1 轨迹片段相似度计算

(1) 内容关联强度计算:当前查询轨迹内容与 E-Ontology中属性及实例之间的近似度。取当前查询轨迹 $T=\{(T_{v1},T_{v2}),(T_{v2},T_{v3}),\cdots,(T_{vi},T_{vj})\}$,针对集合中的每个路网位置节点 T_{vi} 名称对应的本体与 E-Ontology中实体名称的文本相似性(Jaccard 相似性[14]),并选择文本相似性最大的实体作为该位置节点匹配的实体,记内容关联强度为 ε,扩充到当前轨迹片段记为:

$$A=\lim_{i,j\to n}\sum_{i,j=1}^{n}\varepsilon(T_{v_i},T_{v_j})/n \tag{1}$$

(2) 结构相似度计算:当前攻击查询轨迹结构属性及其实例与 E-Ontology 中属性及实例的相似程度。取当前查询轨迹 $T=\{(T_{v_1},T_{v_2}),(T_{v_2},T_{v_3}),\cdots,(T_{v_i},T_{v_j})\}$,遍历 E-Ontology,当内容关联命中 E-Ontology 实体名称时,进一步向子节点属性扩展同时获取叶节点的实例描述,在 E-Ontology 中选择与当轨迹片段实例最相似的文本作为学习节点,并记为 η:

$$\eta(T_{v_i},T_{v_j})=\left|\frac{(T_{v_i})\cap(T_{v_j})}{(T_{v_i})\cup(T_{v_j})}\right| \tag{2}$$

扩展到当前轨迹片段则计算为:

$$S=\lim_{i,j\to n}\sum_{i,j=1}^{n}\eta(T_{v_i},T_{v_j})/n \tag{3}$$

定义 3(综合相似度) 为结构相似度和内容关联度的权重求和,记为:

$$\mathrm{Sim}(v_i,T_{v_j})=\theta\times A+(1-\theta)\times S \tag{4}$$

按上述方法,对于任意轨迹的综合相似度,构成一个 k 阶相似度矩阵 $R_{\mathrm{Sim}}=(r_{i,j})_{k\times k}$。

3.2 基于 k-匿名聚类的轨迹查询事件服务

为实现当前查询的轨迹与 E-Ontology 实例相似度最高的 $k-1$ 条轨迹,形成一个关于当前轨迹的匿名组,本节在语义本体模型和轨迹相似度的基础上,实现轨迹的 k-匿名。算法的基本思路是:在以半径为 δ 的区域内,截取当前查询轨迹片段,采用综合相似度计算当前轨迹片段与 E-Ontology 实体、属性和实例,选取最大的 $k-1$ 条轨迹,并遍历整条轨迹,生成关于当前轨迹的虚假轨迹组。最后将学习到的知识更新到语义本体库中,作为新的相似匿名实例,从而增强轨迹匿名的语义性。如算法 1 所示。

算法 1 基于 k-匿名聚类的轨迹查询事件服务

输入:当前查询轨迹 T_q,轨迹位置节点 $V(T_q)$,参数 k 表示 k 条轨迹,参数 θ 表示相似权重,T_{ont} 表示 E-Ontology

输出: 匿名轨迹组 T_p

步骤:

1. Init $\theta=0.5$, $V(T_q)$, V_i, T_{ont}, $i=0$;
2. OntModel T_{ont} = ReasonerFactory. CreateReasoner( )
   //通过 Jena 推理引擎获取 E-Ontology 实体
3. For Each $V(T_q)<n, i<n$ and $|T_{\mathrm{ont}}|>0$
   $V_{i++}=\{V(T_q)\}$ //通过参数 V_i进行增量存储
   //当前轨迹位置节点 $V(T_q)$
   R_{sim} = calculating(V_i, T_{ont}, θ) //计算当前查询轨迹片段
   //与 E-Ontology 形成的 k 阶矩阵
   min = MinDistance(R_{sim})
   //取输入轨迹点距离最小间隔的轨迹
   $V_{ij}=\varnothing, j=0$ //初始化 k 阶矩阵的列 j
   For $|R_{\mathrm{sim}}|<=k$ and $j<k$
   V_{ij} += max(T_{ont}. Reasoner(V_i), min)
   //通过 Jena 的 Reasoner API 获取相似度最大的轨迹
   $T_p[\,]=V_{ij}$ //最终结果存入 $T_p[\,]$
   End For
   End For
Return T_p

算法 1 中,步骤 1 有关参数选取:给定当前查询轨迹 T_q,选取相似权重 $\theta=0.5$,主要是平衡结构相似度和内容关联度的权重,参数 k 表示从当前区域内获取的 k 条轨迹,$V(T_q)$ 表示轨迹的位置节点编码,初始化为 0,通过参数 V_i进行增量存储,并可以调用 R_{sim}求出 k 阶相似度矩阵,时间复杂度为 $O(n^2)$;步骤 2 通过 Jena推理引擎生成 E-Ontology 模型库;步骤 3 先计算当前查询轨迹片段与 E-Ontology 形成的 k 阶矩阵,然后实时泛化当前轨迹结点的 k 匿名数据,将相似度最大的 k 条轨迹存入当前匿名组,形成关于当前轨迹的虚假轨迹。算法根据轨迹片段相似度将当前查询轨迹片段将和 E-Ontology 的实体、属性和实例相似的轨迹片段进行聚类,进而扩充到整条轨迹。

4 实验结果分析

4.1 实验数据

为了验证本文方法的有效性,考虑经典匿名聚类

算法 NWA[15] 和(k, δ) – anonymity[15] 在信息损失、近邻查询准确度、执行效率三个方面与本文方法的可比性,由此进行实验对比分析。实验数据采用 Thomas Brinkhoff 基于路网的移动对象生成器和和 AIS 信息服务平台共同合成的上海近岸地区移动对象的数据集生成的网络,包括查询范围 δ、对象数、轨迹点和数据量,如图 2 所示。

查询半径（m）	对象数（个）	轨迹点（个）	数据量（MB）
100	136	588	180
200	265	760	366
300	390	890	511
400	425	1360	860
500	485	1599	997
600	566	1724	1215

图 2　系统中生成的数据集网络

实验环境在 Intel Core 2 Quad 2.4 GHz Windows 10 系统上运行,服务器架构在 IBM 3650xm 上,采用 Linux Asia 3x 版本,系统数据库为 IBM DB2,算法采用 Java 语言和 Jena 推理包实现。考虑算法在随机选取轨迹初始节点会导致匿名结果的差别,实验重复不少于 5 次,结果取平均值。

4.2　性能分析

本次实验从信息损失、查询准确率和执行效率三个方面与不同的 k-匿名方法进行性能比较,通过实验讨论算法的性能。

(1) 信息损失比较。本文方法构成的信息损失来自查询事件轨迹位置节点的匿名聚类造成的内容泛化和结构隐匿的信息损失。因此,采用用户错误访问子空间轨迹片段数与当前轨迹片段数之比作为度量轨迹信息损失的标准。

图 3 给出了不同方法随着 k 值的增加信息损失量的变化,实验表明:与 NWA 和(k, δ)-anonymity 相比,在 k 值为 8 ~ 10 时本文方法降低了 15% ~ 20%,因为本文方法构建了基于事件本体的匿名模型,针对轨迹信息的语义知识不足进行扩展改进,对输入轨迹动态判断,采用 Jena 推理引擎将当前轨迹与历史轨迹存储与一个匿名组保证匿名信息的相对完整性。

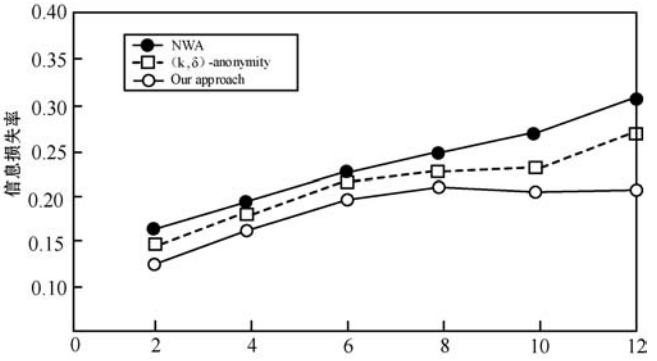

图 3　随着 k 值增大,三种方法的信息损失率

(2) 查询精准率。在使轨迹数据匿名隐私保护的同时,又保证用户查询的精准性。以基于 k-匿名查询的轨迹聚类方法生成的匿名组 T_p 与当前真实查询轨迹 T_q 为中心进行近邻查询,查询内容为用户提交的 LBS 轨迹位置节点请求;T_p 和 T_q 为结果集数量,使用查询准确率 POI 来衡量服务质量,其计算方式如下所示:

$$POI = \frac{|T_p \cap T_q|}{|T_p|} \times 100\% \tag{5}$$

如图 4 所示,随着 k 值的增加,在半径 δ 为 100 ~ 600 m 的范围内查询精准率保持在 65% 以上,实验表明:本文方法通过 Jena 引擎将当前轨迹与 E-Ontology 匹配,使得在轨迹距离上的划分粒度更为精细,因此在当前匿名轨迹与实际轨迹的距离较小,误差在半径范围较大时保持平衡。

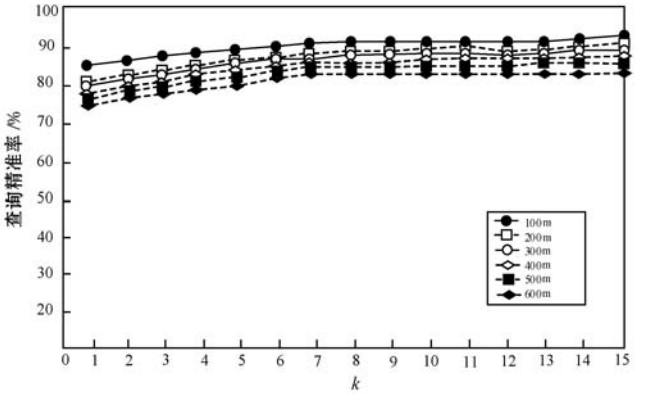

图 4　不同距离下近邻查询精准率

(3) 执行效率。为考察本文算法的执行效率,采用运行时间作为执行效率的度量标准。图 5 给出了随着 k 的增大,相对于 NWA 和(k, δ)-anonymity,本文方法的运行时间相对减少并且平均低于 20 秒。实验表明:本文对内容和结构独立计算且只进行一次就生成了 k 阶矩阵,而基于事件本体的匿名模型的计算深度通过 Jena API 直接调用,效率较高,因此开销时间较小。

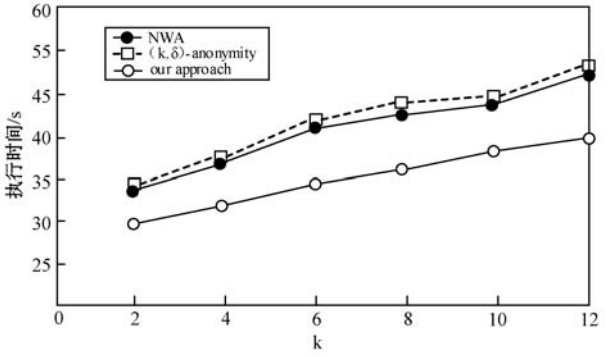

图 5 随着 k 值增大,执行时间的变化

5 结 语

本文采用 OWL 形式化表示轨迹数据及查询事件,提出一种连续查询事件中基于语义的轨迹 k-匿名方法,构建事件本体模型,并结合轨迹片段相似度计算和 Jena 推理引擎,提出基于 k-匿名查询的轨迹聚类方法。该方法可以防止攻击者窃取用户轨迹数据,维护公共安全。然而数据规模扩大伴随着 k 值的增大,轨迹数据的不确定性可能影响推理的准确性,后续工作将在原始数据采集和提高匿名质量及匿名算法方面做深入研究。

参 考 文 献

[1] 霍峥,孟小峰. 轨迹隐私保护技术研究[J]. 计算机学报, 2011, 34(10): 1820 - 1830.

[2] 朱麟, 黄胜波. 不确定环境下轨迹 k-匿名隐私保护[J]. 计算机应用,2015,35(12):3437 - 3441.

[3] 王爽, 周福才, 吴丽娜. 移动对象不确定轨迹隐私保护算法研究. 通信学报,2015,36(S1):94 - 102.

[4] Sweeny L. K-anonymity: a model for protecting privacy[J]. International Journal on Uncertainty, Fuzziness and Knowledge based Systems, 2002, 10(5):557 - 570.

[5] 胡德敏, 郑霞. 基于连续查询的用户轨迹 K-匿名隐私保护算法[J]. 计算机应用研究, 34(11):3421 - 3427.

[6] Kim H I, Shin Y, Chang J W. A grid-based cloaking scheme for continuous queries in distributed systems[C]// Proceedings of the 11th IEEE Int Conf on Computer and Information Technology(CIT). Los Alamitos, CA: IEEE Computer Society,2011: 75 - 82.

[7] 周长利, 马春光, 杨松涛. 路网环境下保护 LBS 的位置隐私的连续 KNN 查询方法[J]. 计算机研究与发展, 2015,52(11):2628 - 2644.

[8] 霍峥, 崔洪雷,贺萍. 基于语义位置保护的轨迹隐私保护的 k-CS 算法[J]. 计算机应用,2018,38(1):182 - 187.

[9] Liu X Y, Wang X C. Survey on privacy preserving techniques for publishing social network data[J]. Journal of Software, 2014,25(3): 576 - 590

[10] OWL Web Ontology Language Overview [EB/OL]. [2004 - 02 - 10]. https://www.w3.org/TR/owl-features/.

[11] Peng T, Liu Q, Meng D C, et al. Collaborative trajectory privacy preserving scheme in location-based services [J]. Information Sciences, 2017, 387: 165 - 179.

[12] Yan Y S, Pei Q Q, Wang X, et al. Probability-based prediction query algorithm [J]. Ad Hoc Networks, 2017, 60: 52 - 65.

[13] Ma M, Wang P. On the Consistency of Event Processing: A Semantic Approach[J]. Knowledge-Based Systems, 2017, 137:29 - 41.

[14] Raff E, Nicholas C. Lempel-Ziv Jaccard Distance, an effective alternative to ssdeep and sdhash[J]. Digital Investigation, 2018, 24:34 - 49.

[15] Gao S, Ma J, Sun C, et al. Balancing trajectory privacy and data utility using a personalized anonymization model[J]. Journal of Network and Computer Applications, 2014, 38: 125 - 134.

(上接第 267 页)

[8] 管军, 周家胜, 易文俊, 等. 基于自适应混沌变异粒子群优化算法的旋转弹丸气动参数辨识[J]. 兵工学报, 2017(1):76 - 83.

[9] 李建美, 高兴宝. 基于自适应变异的混沌粒子群优化算法[J]. 计算机工程与应用, 2016, 52(10):44 - 49.

[10] 陈寿文. 基于质心和自适应指数惯性权重改进的粒子群算法[J]. 计算机工程与应用, 2015, 51(5):58 - 64.

[11] 肖红, 李盼池. 改进的量子行为粒子群优化算法及其应用[J]. 信息与控制, 2016, 45(2):157 - 164.

[12] 章国勇, 伍永刚, 顾巍. 基于精英学习的量子行为粒子群算法[J]. 控制与决策, 2013, 28(9):1341 - 1348.

[13] Cotler J, Hunter-Jones N, Liu J, et al. Chaos, complexity, and random matrices[J]. Journal of High Energy Physics, 2017, 2017(11):48.

[14] Cheng Y H, Kuo C N, Lai C M. Comparison of the adaptive inertia weight PSOs based on chaotic logistic map and tent map[C]// IEEE international Conference on information and Automation. IEEE, 2017:355 - 360.

[15] 韩忠华, 孙越, 史海波. 基于改进 ICA 算法的 LBFFSP 问题研究[J]. 信息与控制, 2017,46(4):474 - 482.

[16] 韩忠华, 朱伯秋, 史海波, 等. 基于改进蝙蝠算法的柔性流水车间排产优化问题研究[J]. 计算机应用研究, 2017,34(7):21 - 24.

[17] 朱雅敏, 薛鹏翔. 基于学习因子自适应改变的粒子群算法研究[J]. 陕西科技大学学报, 2015(4):172 - 177.

[18] 李国晓, 韦世丹. 基于改进 Tent 映射的自适应变尺度混沌粒子群算法[J]. 水力发电, 2017(2):89.