CN 43-1258/TP
ISSN 1007-130X

计算机工程与科学
Computer Engineering & Science

第 38 卷第 11 期 2016 年 11 月
Vol. 38, No. 11, Nov. 2016

文章编号:1007-130X(2016)11-2191-06

一种基于 K-匿名聚类的可穿戴设备数据重发布方法*

李　桐,刘　强,蔡志平,周桐庆

(国防科学技术大学计算机学院,湖南 长沙 410073)

摘　要:近年来,可穿戴设备被广泛地被应用于日常生活。用户量增加造成的可穿戴设备数据重发布是导致隐私泄漏的一个重要原因。为此,数据匿名化重发布方法受到了广泛关注。然而,现有的数据匿名化重发布方法存在两个方面的不足:一方面,现有的数据匿名化重发布算法可能会造成严重的信息损失或用户隐私数据的泄漏;另一方面,现有的数据匿名化重发布算法在兼顾保护用户隐私和减少信息损失的情况下会造成较高的发布成本。为了兼顾隐私安全和数据可用性,并且提高数据重发布算法的效率,结合可穿戴设备自身的特点,提出基于聚类的数据匿名化重发布算法,该算法直接对增量数据进行基于聚类匿名化操作,使数据匿名化重发布更为高效。此外,在数据量较大的应用场景中,基于聚类的数据匿名化重发布算法可以有效减少信息损失。实验结果表明,基于聚类的数据匿名化重发布算法能够在保证用户隐私安全的前提下减少信息的损失并且提高执行效率。

关键词:可穿戴设备;K-匿名聚类;数据重发布;隐私保护

中图分类号:TP391.08　　**文献标志码**:A

doi:10.3969/j.issn.1007-130X.2016.11.005

A wearable data re-dissemination method based on K-anonymity clustering

LI Tong, LIU Qiang, CAI Zhi-ping, ZHOU Tong-qing

(College of Computer, National University of Defense Technology, Changsha 410073, China)

Abstract: Nowadays, wearable devices are widespread in our daily life. The rapid growth of users' number results in data re-dissemination by data holders. Nevertheless, improper re-dissemination methods can lead to unacceptable information loss or privacy leakage. In addition to privacy preserving concern, the data republishing methods for wearable devices should also be efficient enough due to the rapid increase of the number of wearable devices. In order to enhance the efficiency under the premise of information security of users and acceptable information loss, we propose a wearable data re-dissemination method based on clustering K-anonymity. The proposed method jointly considers data privacy, information loss and the overheads. Specifically, the proposed method processes the incremental data directly to enhance the efficiency and the clustering K-anonymity can limit information loss. The proposed method can reduce information loss when the amount of the data is huge. Experimental results demonstrate its effectiveness.

Key words: wearable device; K-anonymity clustering; re-dissemination; privacy preserving

* 收稿日期:2016-07-16;修回日期:2016-09-13
基金项目:国家自然科学基金(601379145)
通信地址:410073 湖南省长沙市国防科学技术大学计算机学院
Address: College of Computer, National University of Defense Technology, Changsha 410073, Hunan, P. R. China

1 引言

在过去的几年里,可穿戴设备在其数量以及功能方面都得到了巨大的提升,伴随着可穿戴设备的普及,越来越多的可穿戴设备走进了人们的生活,并且记录了人们日常生活的点点滴滴[1-3]。

在当前的技术背景下,可穿戴设备的作用主要为采集数据,为了充分开发可穿戴设备数据的价值,数据持有者乐意与第三方分享数据,然而事实证明这些数据足以泄漏用户的隐私[2-4,8]。除此之外,可穿戴设备数据发布时还会伴随发布诸如身高、体重、年龄等信息以提升可穿戴设备数据的可用性[9],这些信息以用户自愿的形式收集,其初衷是为用户提供更个性化的服务,但是伴随发布的信息会增加用户隐私泄漏的可能性。因此,如何在隐私安全的前提下分享可穿戴设备数据成为问题的关键。

加密技术和身份认证技术是隐私保护领域中较为常用的技术,但是在数据分享过程中,第三方的可靠性以及获取数据的真实目的难以得到有效证实,因此,身份认证技术和加密技术并不适用于数据分享。只有对原数据做出修改,在一定程度上降低数据的可用性,才能在数据共享时更好地保护用户的隐私。早在1998年,Samarati和Sweeney[10]提出了K-匿名,K-匿名要求每一条记录与同数据集的至少$K-1$条其他记录在准标识符字段保持一致。然而,K-匿名不能防止敏感属性字段造成的信息泄漏,为了解决这一弊端,Machanavajjhala等人[11]在K-匿名的基础上引入了l-多样性,l-多样性要求敏感属性在一个K-匿名的等价类中至少有l个“表现良好”的元素。虽然l-多样性对K-匿名做出了改进,但是l-多样性本身较为复杂,并且也存在弱点。Li Ning-hui和Li Tian-cheng[12]提出了t-closeness,t-closeness要求敏感属性在一个等价类中的分布要尽量趋近于数据表全局的敏感属性分布。

K-匿名的原理是切断准标识符属性(诸如家庭住址、性别、年龄等虽然不能标识出身份,但是却含有一定与身份相关信息的属性)之间的关联,阻止连接攻击的发生。l-多样性和t-closeness是K-匿名的改进,这些方法在K-匿名的基础上改进了数据表中每个等价类敏感属性(诸如病情、工资等个人隐私数据)的分布,使敏感属性的分布更为合理。

然而,以上所有匿名化发布方法所关注的都是数据一次性发布的问题,可穿戴设备近些年来发展势头迅猛,用户数量激增,因此,数据的持有者为了保证数据的时效性,需要多次发布数据。为保护用户隐私在数据重发布的过程中不被泄漏,数据的匿名化重发布成为了数据持有者较为合理的选择。但是,现有的数据匿名化重发布方法在发布数据时可能会造成严重的信息损失,更严重的问题在于,现有的一些重发布方法在匿名化重发布数据的过程中存在隐私泄漏的可能。与此同时,考虑到用户增量规模巨大,匿名化重发布方法的效率也是一个必须考虑的重要问题。

针对可穿戴设备数据重发布过程中所需面临的隐私安全、数据可用性、算法效率等问题,本文根据可穿戴设备目前的发展状况,以K-匿名为基础,提出了基于聚类的数据匿名化重发布算法,并且通过实验验证了该匿名化重发布算法在隐私保护、数据损失控制以及算法效率方面的效果。

本文其余部分组织如下:第2节举例说明了数据重发布时所可能带来的数据损失或隐私泄漏问题,并且介绍了几种已有的数据匿名化重发布的算法;第3节提出了基于聚类的数据重发布算法;随后,第4节给出了实验结果比较,以验证可穿戴设备数据基于聚类重发布方法的效果;第5节对本文工作进行总结。

2 相关工作

随着计算机、物联网技术(可穿戴设备)的飞速发展[2],当前社会个人的数据量、数据多样性以及数据采集手段呈现出飞速增长的趋势。为了挖掘数据所蕴含的价值,数据持有者需要在保证隐私安全的前提下分享数据,数据匿名化发布方法则是相对适宜的选择。之前已有相关工作提出数据匿名化发布的方法,其中K-匿名是其余匿名化发布方法的基础,l-多样性[10]和t-closeness[12]则是K-匿名的进一步发展。

然而,以上所列匿名化方法只关注了数据一次性发布的问题。但是,在大多数情况下数据会发生改变,数据的持有者需要根据数据的动态变化情况,选择在不同时间点发布不同版本的数据,也就是数据的重发布。

较为简单的数据匿名化重发布方法有两种,第一种为直接对增量数据进行诸如抑制(删除)或者泛化(将数据从精确值模糊化为一个取值范围的过

程)等匿名化操作,这种数据重发布的方法较为简单,并且安全性强,但是这种数据重发布方法的缺陷在于其有可能会造成较严重的信息损失,信息损失程度较为严重时会导致数据不可用的后果。

数据匿名化重发布的第二种方法将增量数据与原有数据视为整体,对整体数据进行泛化(或抑制)操作,之后发布匿名化操作的结果。这种重发布算法可以有效减少信息的损失,但是也有以下两点问题:其一,会造成大量的冗余计算;其二,也是更为严重的问题,可能会导致用户隐私的泄漏。例如,表 1 为一个数据集的一部分,表 2 为表 1 所含数据 2-匿名结果,表 3 为增量数据,表 4 为使用第二种匿名化发布方法所产生的 2-匿名结果(所有表格中 Sd 均表示敏感属性的值)。

Table 1　Original data

表 1　原始数据

Age	*Height*	*Weight*	
37	172	70	*Sd*1
22	188	88	*Sd*2
36	171	71	*Sd*3
21	187	86	*Sd*4

Table 2　2-anonymity results of the original data

表 2　原始数据的 2-匿名结果

Age	*Height*	*Weight*	
3*	17*	7*	*Sd*1
3*	17*	7*	*Sd*2
2*	18*	8*	*Sd*3
2*	18*	8*	*Sd*4

Table 3　Incremental updating results

表 3　增量更新数据

Age	*Height*	*Weight*	
37	172	71	*Sd*1
22	185	88	*Sd*2
39	171	71	*Sd*3
23	187	86	*Sd*4。

表 3 与表 1 的数据较为接近,其原因在于,用户量大并且人体的身高数据和对应的体重数据取值范围有限。显然,表 4 中的数据比起表 2 中的数据更为具体,这就使得隐私泄漏的风险增加。

以上两种数据匿名化重发布方法较为简单,然而,K-PPRP 算法[13]是一种不同于以上两种方法的数据重发布算法,K-PPRP 算法使增量数据逐条有选择地(满足单调性原则)插入到最新版本的匿名化发布的数据集中,再对其做泛化操作。这种算法所取得的效果是前两种算法的折衷,K-PPRP 算法相对于第一种算法可以减少信息的损失,但其流程要远复杂于第一种方法。相比于第二种方法,K-PPRP 可以减少冗余计算,并且更安全可靠,但是经过匿名化操作后,数据的可用性要略逊一筹。K-PPRP 算法虽然具有安全可靠、数据损失小等优势,但是就总体而言,其效率较低。在保证隐私安全以及数据可用的前提下,提高匿名化发重布方法的效率是本文所关注的主要问题。

Table 4　Results of 2-anonymity after incremental updating

表 4　增量更新后 2-匿名结果

Age	*Height*	*Weight*	
37	172	7*	*Sd*1
37	172	7*	*Sd*2
22	18*	88	*Sd*3
22	18*	88	*Sd*4
3*	171	71	*Sd*5
3*	171	71	*Sd*6
2*	187	86	*Sd*7
2*	187	86	*Sd*8

3　面向可穿戴设备数据的聚类匿名化重发布方法

3.1　算法原理

基于聚类的匿名化重发布算法是针对匿名化发布可穿戴设备数据所提出的匿名化重发布算法,根据可穿戴设备用户增长较快的特点,该算法必须能够支持可穿戴设备数据被安全、可用、高效地匿名化重发布。

根据前文所述,匿名化重发布导致隐私泄漏的原因是前后版本数据匿名化操作的力度不同,所得结果的详细程度不同。例如,表 4 中第一条记录的年龄属性相对于表 2 中的第一条记录的年龄属性而言更为具体,这增加了隐私泄漏的风险,原因在于对原有已发布数据进行了修改,并且对后一版本数据的匿名化操作力度较轻。例如,表 4 中的数据相对于表 2 更具体,这直接增加了用户隐私被泄漏的可能性。所以,数据匿名化重发布导致隐私泄漏的原因在于,后一版本发布的数据匿名化的程度不及前一版本的数据。

为了保护隐私安全,基于聚类的匿名化重发布算法对于已匿名化发布的数据不再做任何改变,这

从根本上可以杜绝前后版本数据匿名化操作的不统一问题,并且可以避免大量冗余计算。本文使用聚类的方法降低因保护用户隐私安全所带来的高信息损失。根据目前已有的相关研究可以证明,使用聚类的方式实现 K-匿名可以有效地减少因匿名化操作所造成的信息损失[18]。

3.2 基于聚类的匿名化重发布算法

设增量数据的数据表为 ΔT,原数据表的匿名化结果为 T,其 K-匿名的参数为 $K(K\geqslant 2)$,基于聚类的数据重发布算法描述如下:

算法 1 Republication_based_on_Clustering

输入:原数据表匿名化结果 T、增量数据表 ΔT 以及 K 匿名的匿名化参数 K;

输出:满足 K-匿名的增量更新数据表结果 T'。

1. 生成增量数据表 ΔT 的准标识符链表 LF;
2. 生成一个经过准标识符属性聚类后的链表 L;
3. 选择 C 为第一个等价类的质心,
4. While LF 中的元素大于或等于 K
5. 以 C 为质心,选择其最接近的 $K-1$ 条记录进行聚类,将这些记录从 LF 删除之后添加到 L 中;
6. 选择距离 C 最远的记录 C' 作为新的质心,$C=C'$;
7. End While
8. 将 LF 中剩余的元素添加到 L 中与其质心最近的簇中;
9. 使用 Generalization 操作统一 L;
10. 将 L 中的结果与 T 连接形成 T';

在上述算法中,记录的准标识符字段之间的距离定义,成为影响结果的一个关键性因素。假定数据表中每条记录有 n 个准标识符属性,设第 i 个准标识符属性为 $a_i(i\leqslant n)$,第 i 个标识符属性的影响因子为 k_n,记录间的距离可以定义为如下形式:

$$d=\sum_{i=1}^{n}((a_i-b_i)\cdot k_i)^2 \tag{1}$$

以上公式所考虑的所有属性为数值型属性,当属性不为数值型时需要将其转化为数值型属性进行计算[15-17]。

在数据表做泛化操作之前,需要对其进行聚类操作,在聚类阶段,选择距离质心最近的 $K-1$ 个元组的操作时间复杂度为 $O(n)$,选择最远的记录作为下一个质心的操作时间复杂度为 $O(n)$,故完整聚类操作的时间复杂度为 $O(n^2)$。在泛化操作的过程中,会按照聚类的结果遍历完整数据表,因此其时间复杂度也为 $O(n^2)$。所以,其整体的时间复杂度为 $O(n^2)$。这证明基于聚类的数据匿名化重发布方法可以在有限时间内完成。

采用基于聚类的数据匿名化重发布算法直接对增量数据进行聚类操作和匿名化操作,省略了增量数据重发布过程中对已发布数据重复匿名化的操作,避免隐私泄漏的同时,也提高了算法的执行效率。基于聚类的可穿戴设备匿名化重发布算法,在增量数据规模较小或者准标识符属性取值范围较大的情况下,可能会造成较大的信息损失。但是,考虑到可穿戴设备用户量大,增长速度快,并且所采集的准标识符属性一般取值空间范围有限,所以在这种情况下,采用基于聚类的可穿戴设备数据重发布算法可以有效地减少信息损失,同时避免因算法复杂程度所带来的高昂成本。

4 性能评估

在本节中,我们用实验验证基于聚类的匿名化重发布算法是否能取得预期的效果。本实验会对比几种不同匿名化重发布算法的执行效率,以及这些算法所带来的信息损失,从而展示该算法的有效性。

4.1 实验设置

本文对所提出的增量数据重发布算法的有效性、匿名数据的质量和算法的效率进行了实验分析。实验比较了四种不同的增量数据重发布方式:Static I、Static II、K-PPRP 以及基于聚类的数据重发布算法 CRP。其中 Static I 采取了对增量更新的数据集进行独立匿名的方法,Static II 采取对增量更新后的整个数据集进行重新匿名化操作的方法。本文采用来自 UC Irvine Machine Learning Repository 的数据集,以 $\{Age,Height,Weight\}$ 作为准标识符,三轴加速器所采集的数据为敏感属性。

4.2 实验结果对比分析

安全性比较:本文选取了 1 500 条记录作为初始数据 T,另外每次选择 1 500 条作为增量数据更新数据集,分别采用 Static I、Static II、K-PPRP 以及基于聚类的数据重发布算法(CRP)对数据集进行匿名化处理,一般认为数据重发布后,如果后一版本的数据相比较前一版本的对应数据更为具体,则认为是数据的重发布造成了隐私的泄漏。图 1 给出了以上四种算法所造成的隐私泄漏情况。

下文通过隐私泄漏情况、执行时间以及数据的质量三个方面对算法的优劣进行比较。

如图 1 所示,本文所定义的隐私泄漏为数据重发布时,后发布的版本含有比前一个数据版本更为具体的数据,由于其他的三种数据重发布算法为直接操作增量数据或者对增量数据逐一插入原数据表,所以避免了以上所提到的隐私泄漏问题。

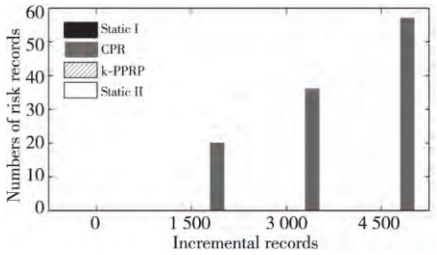

Figure 1　Privacy leakage of the re-dissemination algorithms

图 1　各种重发布算法的隐私泄漏情况

数据质量的比较:本文中所用的匿名化方法为数据的泛化方法,用泛化进行匿名化操作的本质在于降低数据的精确度,使精确的数据变得模糊。这种方法虽然可以保护数据的隐私安全,但同时也降低了数据的可用性,若数据的可用性降低至一定程度,数据的发布也会失去意义。因此,在保证用户的隐私安全前提下,数据的可用性则是数据匿名化发布算法优劣的另外一个重要指标。本文采用数据匿名化过程中执行泛化操作的次数来展示数据的损失程度,执行泛化次数越多,则信息的损失程度越大。如图 2 所示,其中 Static I 的泛化次数最多,Static II 的泛化次数最少,K-PPRP 相比较于 CRP 来说泛化次数略少,其中后三种匿名化发布算法所造成的信息损失程度差距不大,Static I 与后三种相比差别较为明显。

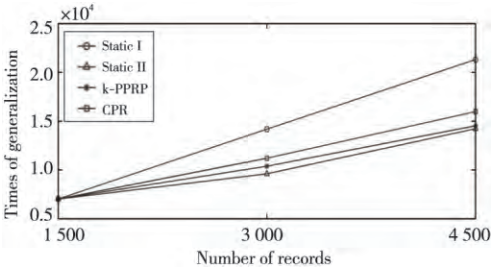

Figure 2　Times of re-dissemination

图 2　不同重发布算法的泛化操作次数

执行时间比较:数据量较小时,发布算法的执行时间问题并不引人注意,但是若数据规模庞大时(例如本文中所需面对的可穿戴设备客户数据),算法的执行效率就会成为一个不可忽视的问题。基于聚类的重发布算法很好地利用了 Static I 方法简洁的优点,直接对增量数据进行匿名化操作,使得其执行时间被有效地缩短。

如图 3 所示,K-PPRP 与 Static II 算法较为复杂,执行时间较长;Static I 算法最简单,其执行时间也最短,因为只需考虑增量数据部分的匿名化操作,而本实验中增量数据为固定大小。因此,CRP 与 Static I 的执行时间都较为固定。

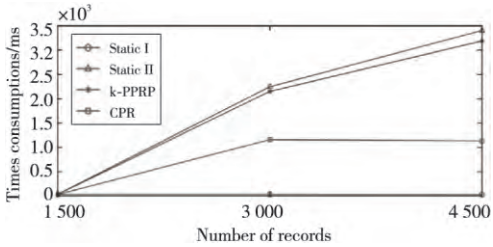

Figure 3　Comparison of executing time

图 3　各种算法执行时间对比

综上所述,基于聚类的匿名化重发布算法首先能够满足用户隐私安全的基本需求,其次,在隐私安全的前提下,基于聚类的匿名化重发布算的数据可用性较好,并且算法的效率较高,适合于可穿戴设备用户数据的发布。

4.3　讨论

本文在可穿戴设备数据发布的背景下提出了基于聚类的数据匿名化重发布算法。该算法直接对增量数据进行匿名化操作,减少了对已发布数据的再次操作过程,从而提高了该算法的执行效率,聚类算法可以在增量数据规模较大的条件下有效减少数据的损失。但是,也有如下几点不足:

(1)聚类对于隐私的威胁:采用聚类的方法实现数据的重发布,在数据量较大时,可能会造成等价类内部元组太过相似,匿名化操作进行得不彻底,最终导致隐私泄漏。

(2)距离的度量:聚类操作的优劣很重要的一个因素在于,元组间距离的定义以及计算方法。但是,不同元组间由于属性的多样性,很难准确定义并且计算元组间的距离。

(3)聚类方法的局限性:针对大规模的增量数据,采用聚类的方法相较于其他方法可以有效地减少数据的损失量,但是如果增量数据的规模较小,则对数据损失减小的效果不会很明显。

5　结束语

目前已存在不少的数据匿名化发布算法,但是这些算法更多面向的是一次性发布的应用场景,虽然一些方法可以被使用于数据重发布的应用场景中,但是很难保证数据的有效性和隐私安全性,虽然有些方法可以兼顾这两点,但是,其算法相较于

其他算法较为复杂。

本文提出的基于聚类的数据重发布算法,以可穿戴设备数据的重发布为背景,较大的用户增量为前提,在保护用户隐私以及保证数据可用性的前提下,降低了重发布算法的复杂程度。实验结果也表明该算法取得了预期效果。但是,其中也存在个别不足,例如算法应用于数据增量较小场景效果不佳,有待后续工作的完善。

参考文献:

[1] Yan T,Lu Y,Zhang N. Privacy disclosure from wearable devices[C]// Proc of the ACM Workshop on Privacy-Aware Mobile Computing,2015:13-18.

[2] Statista. Wearable device market value from 2010 to2018 (in million u. s. dollars)[EB/OL]. [2016-04-11]. http://www.statista. com/statistics/259372/wearable-device-market-value/.

[3] Cornelius C,Peterson R,Skinner J,et al. A wearable system that knows who wears it[C]// Proc of the 12th ACM Annual International Conference on Mobile Systems, Applications, and Services,2014:55-67.

[4] Lara O D,Labrador M A. A survey on human activity recognition using wearable sensors[J]. IEEE Communications Surveys & Tutorials,2013,15(3):1192-1209.

[5] Casale P,Pujol O,Radeva P. Personalization and user verification in wearable systems using biometric walking patterns [J]. Personal and Ubiquitous Computing,2012,16(5):563-580.

[6] Mannini A, Sabatini A M. Machine learning methods for classifying human physical activity from on-body accelerometers[J]. Sensors,2010,10(2):1154-75.

[7] Casale P,Pujol O,Radeva P. Human activity recognition from accelerometer data using a wearable device[M]// Pattern Recognition and Image Analysis. Berlin:Springer Berlin Heidelberg,2011:289-296.

[8] Ali H K,Amalarethinam D I G. Activity recognition with multi-tape fuzzy finite automata[J]. International Journal of Modern Education & Computer Science,2013,5(5):60-65.

[9] Zhang M,Sawchuk A. USC-HAD:A daily activity dataset for ubiquitous activity recognition using wearable sensors[C]// Proc of ACM Conference on Ubiquitous Computing. 2012:1036-1043.

[10] Sweeney L. *k*-anonymity: A model for protecting privacy [J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,2012,10(5):557-570.

[11] Machanavajjhala A,Gehrke J,Kifer D,et al. *L*-diversity:Privacy beyond k-anonymity[C]// Proc of IEEE International Conference on Data Engineering,2006:24.

[12] Li Ning-hui, Li Tian-cheng, Venkatasubramanian S. *t*-closeness:Privacy beyond *k*-anonymity and *l*-diversity[C]// Proc of IEEE 23rd International Conference on Data Engineering,2007:106-115.

[13] Wu Ying-jie,Ni Wei-wei,Zhang Bai-li,et al. *k*-APPRP: A partitioning based privacy preserving *k*-anonymous algorithm for re-publication of incremental datasets[J]. Journal of Chinese Computer Systems,2009,30(8):1581-1587. (in Chinese)

[14] Zhu H, Ye X. Achieving *k*-anonymity via a density-based clustering method[C]// Proc of Joint,Asia-Pacific Web and, International Conference on Web-Age Information Management Conference on Advances in Data and Web Management,2007:745-752.

[15] Peng Jiing,Tang Chang-jie,Cheng Wen-quan,et al. A hierarchy distance computing based clustering algorithm [J]. Chinese Journal of Computers,2007,30 (5):786-795. (in Chinese)

[16] Li Jie,Gao Xin-bo,Jiao Li-cheng. A GA-based clustering algorithm for large datasets with mixed numeric and categorical values [J]. Journal of Electronics & Information Technology,2004,26(8):1204-1209. (in Chinese)

[17] Domingo-Ferrer J, Mateo-Sanz J M, Torra V. Comparing SDC methods for microdata on the basis of information lossanddis closure risk[C]// Proc of ETK-NTTS, 2002. 807-826.

[18] Sweeney L. Achieving *k*-anonymity privacy protection using generalization and suppression[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2012,10(5):571-588.

附中文参考文献:

[13] 吴英杰,倪巍伟,张柏礼,等. *k*-APPRP:一种基于划分的增量数据重发布隐私保护 *k*-匿名算法[J]. 小型微型计算机系统,2009,30(8):1581-1587.

[15] 彭京,唐常杰,程温泉,等. 一种基于层次距离计算的聚类算法[J]. 计算机学报,2007,30(5):786-795.

[16] 李洁,高新波,焦李成. 一种基于 GA 的混合属性特征大数据集聚类算法[J]. 电子与信息学报,2004,26(8):1204-1209.

作者简介:

李桐(1992-),男,陕西乾县人,硕士,研究方向为网络安全。E-mail:18739965789@163.com

LI Tong, born in 1992, MS, his research interest includes network security.

刘强(1986-),男,江西临川人,博士,讲师,CCF 会员(49698M),研究方向为无线网络安全、物联网和机器学习。E-mail:lisi@263.net.cn

LIU Qiang, born in 1986, PhD, lecturer, CCF member (49698M), his research interests include wireless network security, Internet of Things, and machine learning.