异构身份联盟中基于本地差分隐私的信任评估算法

毛一凡[1] 赵 涛[1] 于鹏飞[2,3] 高先周[2,3] 杨如侠[2,3]

[1](国家电网有限公司大数据中心 北京 100031)

[2](全球能源互联网研究院有限公司 江苏 南京 210003)

[3](信息网络安全国网重点实验室 江苏 南京 210003)

摘 要 面对海量异构的身份管理、跨网跨域信任服务和身份隐私保护需求,构建异构身份联盟体系是一种有效的解决方法。针对联盟体系内关于信任评估计算中所存在的隐私泄露问题展开详细的研究,并利用本地差分隐私技术设计具有隐私保护效果的信任评价算法,对其隐私信息进行有效的保护。从理论上证明了该算法满足本地差分隐私,并分析其估计结果的误差大小,进行的相关实验论证说明算法的可行性与有效性。

关键词 异构身份联盟 本地差分隐私 信任评价

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2023.02.053

CREDIBILITY EVALUATION BASED ON LOCAL DIFFERENTIAL PRIVACY IN HETEROGENEOUS IDENTITY ALLIANCE SYSTEM

Mao Yifan[1] Zhao Tao[1] Yu Pengfei[2,3] Gao Xianzhou[2,3] Yang Ruxia[2,3]

[1](*Big Data Center of State Grid Corporation of China*, *Beijing 100031*, *China*)

[2](*Global Energy Interconnection Research Institute Co.*, *Ltd.*, *Nanjing 210003*, *Jiangsu*, *China*)

[3](*State Grid Key Laboratory of Information & Network Security*, *Nanjing 210003*, *Jiangsu*, *China*)

Abstract Facing the needs of massive heterogeneous identity management, cross-domain trust services and identity privacy protection, it is a feasible solution to construct the heterogeneous identity alliance system. This paper conducted the detailed research on the problem of privacy leakage in credibility evaluation calculation in the alliance system, and designed the privacy-preserving credibility evaluation algorithms with local differential privacy to protect the privacy information effectively. It could be theoretically proved that this algorithm satisfied the local differential privacy. The error of its estimation results was analyzed. The feasibility and effectiveness of the algorithm were demonstrated by relevant experiments.

Keywords Heterogeneous identity alliance Local differential privacy Credibility evaluation

0 引 言

随着网络技术的不断发展,网络空间中不同体系结构、不同应用领域的异构网络协同并存,如何统一管理网络实体的多域多形态身份是一个挑战性问题。针对该问题,构建信任联盟实现网络身份管理,已经成为学术界和产业界的共识。微软的 Passport[1]、Google 基于 OpenID 协议[2]建立的 Google Accounts 及 CICP 服务已形成商用化的身份管理联盟,能够为用户提供联盟内一致的身份和账户管理,将用户身份的有效域从单一机构扩展到联盟范围。然而,在跨域信任联盟中依然存在着一些问题,如身份认证[3]、跨域信任评价等。本文将针对联盟体系中信任评价问题进行深入的研究。

异构身份联盟体系中存在多个身份管理域,在单

收稿日期:2020-05-13。**毛一凡**,高工,主研领域:系统架构。**赵涛**,工程师。**于鹏飞**,高工。**高先周**,工程师。**杨如侠**,工程师。

个评价周期内,每个身份管理域根据域内用户的状态、行为以及历史记录,分析获得用户身份可信程度的评价值,并将该评价值共享给其他身份管理域以形成联盟内对用户的综合可信度评价。该综合可信度评价结果将为各个域对用户访问服务/资源的权限管理提供重要依据。其中,身份管理域内获取的用户可信度评价对该身份域而言可能是敏感信息。每个身份域不想将其产生的对用户的真实评价结果直接暴露给其他身份域。从一方面来说,在身份域共享用户可信度评价结果时,可能被某些用户截获,当用户发现自己评价较低时,或许会采取脱离该身份域等行为,这可能对身份管理域产生一些不好的影响;另一方面,身份域在获知其他域共享来的用户真实评价后,有可能会在用户的评价结果中加入主观因素的考量,从而无法得到身份域对用户客观真实的评价结果。因此,本文将借助本地差分隐私[4-6]设计相应的隐私保护机制,使得身份域在共享用户可信度评价时能够隐藏其隐私信息,同时仍然能够计算出对用户的综合可信度评价结果。

1 基础知识

1.1 本地差分隐私定义

定义 1 (本地差分隐私 ε-LDP[4-6])一个随机化的算 $A:D\to O$ 满足 ε-本地差分隐私(LDP),当且仅当对于任意的输入 $d,d'\in D$,以及任意的输出 $o\in O$,其满足:

$$\frac{Pr(A(d)=o)}{Pr(A(d')=o)}\leqslant e^{\varepsilon} \tag{1}$$

式中:ε 被称为隐私保护预算($\varepsilon\geqslant 0$)。ε 在一定程度可以衡量隐私保护程度的大小,由式(1)可知,ε 越小(大),任意两个不同的输入(d,d')经过算法 A 之后得到相同输出(o)的概率也就越大(小),则 d 与 d'的不可区分程度也就越高(低)。

1.2 多元随机响应机制(*K*-RR)

最初为了保护人们在敏感问题调研中的个人隐私(例如:您曾经是否有过作弊?),Warner[7] 提出了二元随机响应机制。在该机制下,被调研的用户在回答问题之前,先抛掷一枚有偏的硬币(即,正面朝上的概率为 $p,p>0.5$)。如果用户掷到正面,则提供他正确的回答,反之,则给出错误的答案。当调研者(收集者)收集到足够用户的数据之后,则可根据式(2)估算出人群中真实数据为"是"的频率 $p('yes')$:

$$P('yes')=\frac{\tilde{P}('yes')+p-1}{2p-1} \tag{2}$$

式中:$\tilde{P}('yes')$是用户在抛掷硬币后提供给调研者数据中"是"的频率。

当输入为多元数据,即类别数量为 $K(K\geqslant 2)$的类别数据时,其处理与二元随机机制类似,每个用户以 p $(p>0.5)$的概率提供自己真实的类别数据,以 $1-p$ 的概率从其余 $K-1$ 个类别中随机抽取一个类别数据进行提交。收集者收到足够数据之后,通过式(3)即可估算出某一类$(k,k\in\{1,2,\cdots,K\})$的频率:

$$P(k)=\frac{\tilde{P}(k)-\frac{1-p}{k-1}}{p-\frac{1-p}{k-1}} \tag{3}$$

式中:$\tilde{p}(k)$指收集到的数据中 k 类别数据出现的频率。根据本地差分隐私的定义,可以计算出多(二)元随机响应机制符合的差分隐私保护程度 ε 为:

$$\varepsilon=\log\left(\frac{p(K-1)}{1-p}\right) \tag{4}$$

1.3 Duchi 均值机制

当对数值型数据求均值时,通常可以在数据中加入均值为 0 的拉普拉斯噪声来实现差分隐私的保证(拉普拉斯机制[8-9])。然后,将加过噪声的数据进行相加即可得到无偏的和值以及均值。然而,当 ε 较小时,须要加入方差较大的噪声来满足其隐私保护程度,这将导致最终得到的估计结果准确度偏低。随后,Duchi 等[10-11]提出了一种新的满足本地差分隐私的均值计算方法。在该机制下,假设用户的数据范围为 $[-1,1]$,每个用户通过以下概率对自己的真实数据 d $(d\in[-1,1])$进行变换:

$$Pr(\tilde{d}=x\mid d)\begin{cases}\dfrac{e^{\varepsilon}-1}{2e^{\varepsilon}+2}\cdot d+\dfrac{1}{2} & x=\dfrac{e^{\varepsilon}+1}{e^{\varepsilon}-1}\\[2ex] -\dfrac{e^{\varepsilon}-1}{2e^{\varepsilon}+2}\cdot d+\dfrac{1}{2} & x=-\dfrac{e^{\varepsilon}+1}{e^{\varepsilon}-1}\end{cases} \tag{5}$$

式中:$\tilde{d}$ 为用户扰乱后的数据。通过计算可知,用户变换之后的数据($\tilde{d}$)的期望正是用户本身的真实数据,所以,当收集者得到用户扰乱后的数据之后,直接对其进行均值计算即可得到无偏的均值。

2 本地差分隐私下的联盟体系内信任评价方案

2.1 问题描述

异构身份联盟体系中包含多个服务提供者,它们形成了多个身份管理域,其中每个域涵盖了一个或多个服务提供者。在一个评价周期内,每个域对其所拥

有的用户等实体的可信度进行评价,并将其所得到的用户可信度传递给联盟内的其他用户管理域,最终形成联盟内对用户的综合可信度评价。

假设联盟中共有 n 个身份管理域,其中,令 C_{ij} 表示域 $R_i(i\in\{1,2,\cdots,n\})$ 对用户 u_j 在某一周期内的可信度评估结果,通常 C_{ij} 的取值是 0 到 1 范围上的实数,即 $C_{ij}\in[0,1]$。通过表 1 可将实数表示的 C_{ij} 对应转换成离散的可信度级别 T_{ij},$T_{ij}\in\{1,2,\cdots,5\}$。

表 1　用户可信度相对关系

可信度级别	可信度取值	可信度描述
5	[0.8,1.0]	可信度很高
4	[0.6,0.8)	可信度较高
3	[0.4,0.6)	可信度一般
2	[0.2,0.4)	可信度较低
1	[0.0,0.2)	可信度很低

然后每个域 R_i 将转为离散数据的可信度评价结果 T_{ij} 共享给其余 $n-1$ 个域。接收到其余域对用户 u_j 的评价之后,R_i 通过均值计算则可获得该周期内联盟中对用户 u_j 的总和评价结果 Z_j,即 $Z_j=mean(T_{1j},T_{2j},\cdots,T_{nj})$。

然而,每个域对用户的评价结果都是敏感的,它们不愿将自己对用户的真实评价公布给其他的身份域。因此,本文将借助本地差分隐私技术设计具有隐私保护效果的信任评价方案,实现对身份域评价结果的隐私保护,同时也能够使每个身份域获得联盟中对用户的综合评价。

2.2　基于 Duchi 机制的信任评价方案(DTM)

本文采取 Duchi 求均值的机制实现对每个身份域敏感信息(用户信任评价结果)的隐私保护,并获取多个身份域评价结果的均值信息。由于 Duchi 机制中的数据范围为[-1,1],因此,每个身份域 R_i 首先须要对所得的用户可信度级别(T_{ij})做一个幅度缩放,将其映射到[-1,1]的范围上:

$$d_{ij}=-1+\frac{1}{2}\cdot(T_{ij}-1) \tag{6}$$

式中:d_{ij} 即是映射后的用户可信度取值。随后,R_i 将缩放后的数值 d_{ij} 代入 Duchi 机制中进行扰乱处理,并将扰乱后的数据 $\tilde{d}_{ij}$ 共享给其余身份域。具体的方案描述如算法 1 所示。

算法 1　DTM

输入:身份域 R_i 对用户 u_j 的可信度级别 T_{ij},隐私预算 ε。

输出:经过隐私保护处理的可信度级别 $\tilde{d}_{ij}$。

1) 根据式(6)对真实的可信度级别 T_{ij} 进行幅度缩放,并将缩放后的数值标记为 d_{ij}。

2) 将 d_{ij} 按照以下概率进行变换:

$$Pr(\tilde{d}_{ij}=x\mid d_{ij})\begin{cases}\dfrac{e^{\varepsilon}-1}{2e^{\varepsilon}+2}\cdot d_{ij}+\dfrac{1}{2} & x=\dfrac{e^{\varepsilon}+1}{e^{\varepsilon}-1}\\[2ex] \dfrac{-e^{\varepsilon}-1}{2e^{\varepsilon}+2}\cdot d_{ij}+\dfrac{1}{2} & x=\dfrac{-e^{\varepsilon}+1}{e^{\varepsilon}-1}\end{cases} \tag{7}$$

3) 返回 2)中所得的 $\tilde{d}_{ij}$,并将其共享给其余身份域。

当身份域 R_i 收到了来自其余所有身份域对用户 u_j 的可信度估值之后,对所有的可信度 $\{\tilde{d}_{1j},\tilde{d}_{2j},\cdots,\tilde{d}_{nj}\}$ 估值,进行均值计算得到该评价周期内对用户 u_j 的总和评价结果 a_j,$a_j=mean(\tilde{d}_{1j},\tilde{d}_{2j},\cdots,\tilde{d}_{nj})$。由于在计算之前,身份域对可信度级别进行了幅度缩放,此时得到的均值是数据缩放后的结果,所以计算出 a_j 后,还须将其等比例变换回去,得到最终的估计结果 $\hat{Z}_j$:

$$\hat{Z}_j=2\cdot(a_j+1)+1$$

定理 1　方案 DTM 满足 ε-本地差分隐私。

证明　在该证明中,令 A 代表方案 DTM。根据本地差分隐私的定义,可以写出:

$$\frac{Pr(A(T_{ij})=d^*)}{Pr(A(T_{i'j})=d^*)}=\frac{\dfrac{e^{\varepsilon}-1}{2e^{\varepsilon}+2}\cdot d_{ij}+\dfrac{1}{2}}{\dfrac{e^{\varepsilon}-1}{2e^{\varepsilon}+2}\cdot d_{i'j}+\dfrac{1}{2}} \tag{8}$$

或者:

$$\frac{Pr(A(T_{ij})=d^*)}{Pr(A(T_{i'j})=d)}=\frac{-\dfrac{e^{\varepsilon}-1}{2e^{\varepsilon}+2}\cdot d_{ij}+\dfrac{1}{2}}{-\dfrac{e^{\varepsilon}-1}{2e^{\varepsilon}+2}\cdot d_{i'j}+\dfrac{1}{2}} \tag{9}$$

式中:T_{ij}、d_{ij}、$T_{i'j}$、$d_{i'j}$ 是任意两个身份域 R_i、$R_{i'}$ 对用户 u_j 的可信度评价以及其缩放后的数值。当 $d_{ij}=1$、$d_{i'j}=-1$ 时,式(8)取得最大值,即为 e^{ε};当 $d_{ij}=-1$、$d_{i'j}=1$ 时,式(9)取得最大值,即为 e^{ε};综上可得:

$$\frac{Pr(A(T_{ij})=d^*)}{Pr(A(T_{i'j})=d^*)}\leqslant e^{\varepsilon}$$

因此,该方案 DTM 满足满足 ε-本地差分隐私。

定理 2　身份域 R_i 从方案 DTM 中所得的总和评价结果 $\hat{Z}_j$ 是关于真实评价 Z_j 的无偏估计,即 $E[\hat{Z}_j]=Z_j$,并且 $\hat{Z}_j$ 的方差上界为:

$$Var[\hat{Z}_j]\leqslant\frac{4}{n}\left(\frac{e^{\varepsilon}+1}{e^{\varepsilon}-1}\right)^2 \tag{10}$$

证明　根据式(7)的概率变换,可得出关于 $\tilde{d}_{ij}$ 的期望如下:

$$E[\tilde{d}_{ij}]=\frac{e^{\varepsilon}+1}{e^{\varepsilon}-1}\cdot\left(\frac{e^{\varepsilon}-1}{2e^{\varepsilon}+2}\cdot d_{ij}+\frac{1}{2}\right)-\frac{e^{\varepsilon}+1}{e^{\varepsilon}-1}\cdot\left(-\frac{e^{\varepsilon}-1}{2e^{\varepsilon}+2}\cdot d_{ij}+\frac{1}{2}\right)=d_{ij}$$

所以：

$$E[\hat{Z}_j]=E[2\cdot(a_j+1)+1]=E\left[2\cdot\left(\frac{1}{n}\sum_i\tilde{d}_{ij}+1\right)+1\right]=\frac{1}{n}\sum_i(2\cdot E[\tilde{d}_{ij}]+1)+1=\frac{1}{n}\sum_i T_{ij}=Z_j$$

关于 $\hat{Z}_j$ 的方差：

$$Var[\hat{Z}_j]=Var\left[2\cdot\left(\frac{1}{n}\sum_i\tilde{d}_{ij}+1\right)+1\right]=\frac{4}{n^2}\sum_i Var[\tilde{d}_{ij}] \tag{11}$$

其中：

$$Var[\tilde{d}_{ij}]=E[\tilde{d}_{ij}^2]-(E[\tilde{d}_{ij}])^2=\left(\frac{e^\varepsilon+1}{e^\varepsilon-1}\right)^2\cdot\left(\frac{e^\varepsilon-1}{2e^\varepsilon+2}\cdot d_{ij}+\frac{1}{2}\right)+\left(-\frac{e^\varepsilon+1}{e^\varepsilon-1}\right)^2\cdot\left(-\frac{e^\varepsilon-1}{2e^\varepsilon+2}\cdot d_{ij}+\frac{1}{2}\right)-d_{ij}^2=\left(\frac{e^\varepsilon+1}{e^\varepsilon-1}\right)^2-d_{ij}^2 \tag{12}$$

由式(12)可知，当 $d_{ij}=0$ 时，其方差取到最大值，因此：

$$Var[\tilde{d}_{ij}]\leqslant\left(\frac{e^\varepsilon+1}{e^\varepsilon-1}\right)^2 \tag{13}$$

由式(11)与式(13)可得：

$$Var[\hat{Z}_j]\leqslant\frac{4}{n}\left(\frac{e^\varepsilon+1}{e^\varepsilon-1}\right)^2$$

2.3 基于多元随机响应机制的信任评价方案(RTM)

2.1 节介绍了表 1 可将每个身份域 R_i 对用户 u_j 的可信度评估值 C_{ij} 转换成离散数据型的可信度级别 T_{ij}。在计算 Z_j 时，除了把 $\{T_{1j},T_{2j},\cdots,T_{nj}\}$ 按照数值相加求平均来做之外，还可将其转化为加权平均值的问题来进行处理，正如式(14)所示。

$$Z_j=\sum_{t=1}^{5}tf(t) \tag{14}$$

式中：$t\in T$，$T=\{1,2,\cdots,5\}$，表示五个不同可信度级别取值的集合；$f(t)$ 代表 t 在 $\{T_{1j},T_{2j},\cdots,T_{nj}\}$ 中出现的频率。此时，求解平均值的问题就转变成求解每个可信度级别频率 $f(t)$ 的问题。考虑到每个身份域敏感信息的隐私保护问题，本文将借助多元随机响应机制实现差分隐私下的可信度级别的频率估算。

首先，每个身份域 R_i 抛掷一枚有偏的硬币，该硬币正面朝上的概率为 $\frac{e^\varepsilon}{e^\varepsilon+4}$。当 R_i 掷出正面时，它将把自己对用户 u_j 做出的真实可信度评价 T_{ij} 共享给其他身份域；如果 R_i 掷出了反面，它将在剩余的四个可信度级别中，即 $T\backslash\{T_{ij}\}$，随机选出一个虚假的可信度级别共享给其他身份域。具体的算法表达如算法 2 所示。

算法 2 RTM-1

输入：身份域 R_i 对用户 u_j 的可信度级别 T_{ij}，隐私预算 ε。

输出：经过隐私保护处理的可信度级别 $\tilde{T}_{ij}$。

1）将 T_{ij} 按照以下概率进行扰乱：

$$Pr(\tilde{T}_{ij}=t\mid T_{ij})\begin{cases}\frac{e^\varepsilon}{e^\varepsilon+4} & t=T_{ij}\\ \frac{1}{e^\varepsilon+4} & t\in T\backslash\{T_{ij}\}\end{cases} \tag{15}$$

2）返回 1）中所得的 $\tilde{T}_{ij}$，并将其共享给其余身份域。

当身份域 R_i 接收到全部身份域发送来的可信度级别之后，便可以按照如下公式可以对所有的可信度级别进行频率估计：

$$\hat{f}(t)=\frac{4\tilde{f}(t)+p-1}{5p-1} \tag{16}$$

式中：$t\in T$，$p=\frac{e^\varepsilon}{e^\varepsilon+4}$。$\tilde{f}(t)$ 代表 t 在所有身份域共享的可信度级别 $\{\tilde{T}_{1j},\tilde{T}_{2j},\cdots,\tilde{T}_{nj}\}$ 中出现的频率。计算出所有的 $\hat{f}(t)$ 之后，R_i 将其代入式(14)中即可获得所有可信度级别的均值，即对用户 u_j 的总和评价结果 $\hat{Z}_j$。关于频率以及总和评价计算的算法如算法 3 所示。

算法 3 RTM-2

输入：所有身份域共享的对用户 u_j 的可信度级别评价 $\{\tilde{T}_{1j},\tilde{T}_{2j},\cdots,\tilde{T}_{nj}\}$，差分隐私预算 ε。

输出：针对用户 u_j 的总和评价结果 $\hat{Z}_j$。

1）对每一个 $t\in\{1,2,\cdots,5\}$，统计其出现在 $\{\tilde{T}_{1j},\tilde{T}_{2j},\cdots,\tilde{T}_{nj}\}$ 中的频率 $\tilde{f}(t)$；

2）通过式(16)，估算出每一个 t 在 $\{T_{1j},T_{2j},\cdots,T_{nj}\}$ 中出现的频率 $\hat{f}(t)$；

3）将 2）所得的所有 $\hat{f}(t)$，$t\in\{1,2,\cdots,5\}$ 代入式(14)，计算出最终对用户 u_j 的综合评价结果 $\hat{Z}_j$。

定理 3 方案 RTM-1 满足 ε-本地差分隐私。

证明 在该证明中，令 A 代表方案 RTM-1。根据本地差分隐私的定义，可以写出：

$$\frac{Pr(A(T_{ij})=T^*)}{Pr(A(T_{i'j})=T^*)}=\frac{Pr(\tilde{T}_{ij}=T^*\mid T_{ij})}{Pr(\tilde{T}_{i'j}=T^*\mid T_{i'j})} \tag{17}$$

式中：T_{ij}、$T_{i'j}$ 是任意两个身份域 R_i、$R_{i'}$ 对用户 u_j 的可信度评价。根据式(15)可知，当 $T_{ij}=T^*$ 且 $T_{i'j}\neq T^*$ 时，式(17)取得最大值，即 e^ε，所以：

$$\frac{Pr(A(T_{ij})=T^*)}{Pr(A(T_{i'j})=T^*)}\leqslant e^\varepsilon \tag{18}$$

方案 RTM-1 满足 ε-本地差分隐私。

定理 4　身份域 R_i从方案 RTM 中所计算出用户 u_j的总和评价结果 $\hat{Z}_j$是关于真实评价 Z_j的无偏估计,即 $E[\hat{Z}_j]=Z_j$,并且 $\hat{Z}_j$的方差为:

$$Var[\hat{Z}_j]\approx\frac{55\cdot(3+e^{\varepsilon})}{n(e^{\varepsilon}-1)^2} \tag{19}$$

证明　根据式(14)和式(16),可得:

$$E[\hat{Z}_j]=E\Big[\sum_{t=1}^{5}t\hat{f}(t)\Big]=\sum_{t=1}^{5}t\cdot E[\hat{f}(t)]=\sum_{t=1}^{5}t\cdot\Big[\frac{4E[\tilde{f}(t)]+p-1}{5p-1}\Big] \tag{20}$$

式中:$E[\tilde{f}(t)]=f(t)\cdot p+\frac{1-p}{4}\cdot(1-f(t))$。将其代入式(20),可得关于 $\hat{Z}_j$的方差:

$$Var[\hat{Z}_j]=Var\Big[\sum_{t=1}^{5}t\hat{f}(t)\Big]=\sum_{t=1}^{5}t^2\cdot Var[\hat{f}(t)] \tag{21}$$

根据文献[12]中的式(4),可计算出:

$$Var[\hat{f}(t)]\approx\frac{e^{\varepsilon}+3}{n(e^{\varepsilon}-1)^2}$$

将 $Var[\hat{f}(t)]$代入式(21)得:

$$Var[\hat{f}(t)]\approx\frac{55\cdot(e^{\varepsilon}+3)}{n(e^{\varepsilon}-1)^2}$$

2.4　方案对比

本节将对 2.2 节和 2.3 节中的方案进行理论上的对比,分析差分隐私预算的大小对两种方案误差的影响。

定理 5　当隐私预算 ε 约大于 2.6 时,RTM 方案下关于综合评价结果估算的方差可小于 DTM 方案下的方差。

证明　由式(10)和式(19)写出:

$$\frac{55\cdot(e^{\varepsilon}+3)}{n(e^{\varepsilon}-1)^2}\leqslant\frac{4}{n}\left(\frac{e^{\varepsilon}+1}{e^{\varepsilon}-1}\right)^2$$

化简可得:

$$55\cdot(e^{\varepsilon}+3)\leqslant4(e^{\varepsilon}+1)^2$$

$$165\leqslant4(e^{\varepsilon}+1)^2-55e^{\varepsilon}$$

$$\varepsilon\geqslant2.6$$

3　实验结果与分析

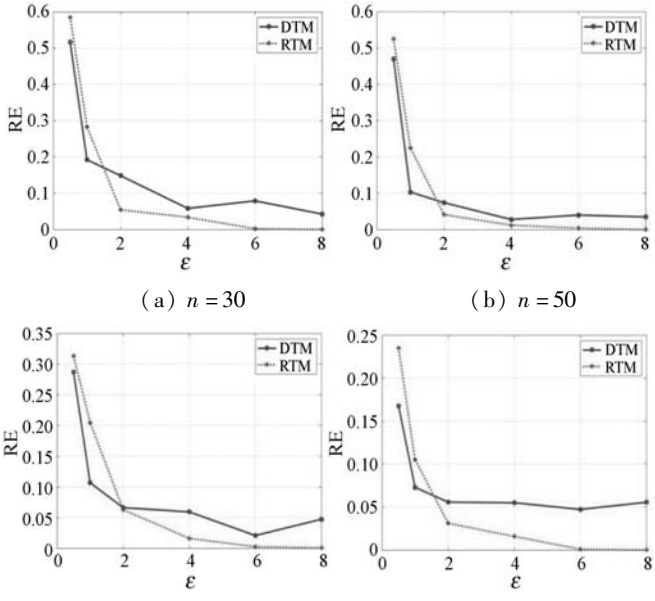
实验部分主要针对本文方案的估算精度进行了深入的分析。具体地,本文想要从隐私保护预算以及参与对某一用户信任度评价的身份域数目两方面,来分析其对综合信任度估算的准确度影响。为了到达上述目的,本文随机生成四个分别包含 30 条、50 条、80 条和 100 条数据的均匀分布数据集,用以模拟 30 个、50 个、80 个和 100 个身份域对某一用户做出的信任度评价。四个数据集中每条数据取值范围均为[0,1]。数据在进行隐私保护之前,需将其根据表 1 进行离散化,然后再利用本文提出方案中的数据处理算法(DTM-1,RTM-1)对其进行随机扰乱来达到隐私保护目的。实验中用相对误差(RE)来衡量估算出的综合信任度评价与真实值之间的差异:

$$R=\frac{|\hat{Z}-Z|}{Z} \tag{22}$$

式中:$\hat{Z}$ 是估算出的对某用户的综合信任度评价,Z 是对某用户综合信任度评价的真实值。

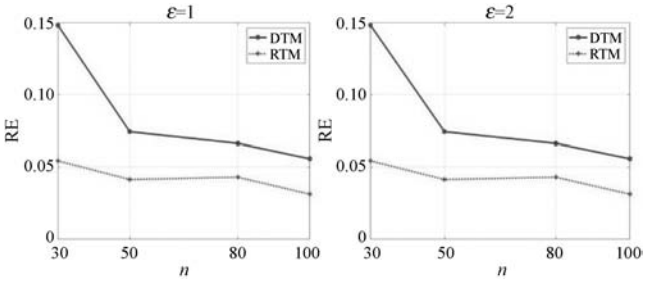
实验环境为 Intel Core i5 CPU 3.1 GHz,8 GB 内存。本文算法均在 MATLAB 中进行实现,并做出实验图表,实验结果取 10 次实验的平均值。

为了有效地说明本文算法的可用性,本节将设计的两种算法(DTM,RTM)在不同的隐私预算下进行了对比,并将其趋势呈现在图 1 中。实验中,差分隐私预算的取值大小分别为{0.5,1,2,4,6,8}。从图 1 可以看出,在所有数据集上,随着隐私预算 ε 的增大,两种算法估计结果的误差呈现出下降的趋势,即估算精度逐步提高。此外,在所有数据集上,当隐私预算 ε 大于 2 时,RTM 算法的估计结果的准确度总是比 DTM 算法的更加精确,这与 2.4 节中的理论分析结果相一致。图 2 中对比了两种算法在相同隐私预算下不同数据集上的表现,即参与评价的身份域数目对估算结果的影响。可以观察到,这与第 2 节中的误差理论分析相吻合。



(a) $n=30$　(b) $n=50$　(c) $n=80$　(d) $n=100$

图 1　不同 ε 取值下 DTM 与 RTM 算法的误差对比



(a) (b)

图 2 不同数据集下 DTM 与 RTM 算法的误差对比

总的来说,当隐私预算 ε 较小时,DTM 方案呈现出较好的优势;当 ε 逐渐变大后,RTM 方案将得到精度更高的估算结果。整体来看,当隐私预算 ε 取到 4 时,本文两种方案的估计误差基本不会超过 0.05。另外,参与计算的身份域个数也对计算结果的精度有所影响,身份域个数越多,估算出结果更加准确。通过本节的实验,可以证明本文提出的两种算法能够有效达到隐私保护的效果,同时也能估算出较为精确的综合信任度评价。

在目前已有的异构环境下的信任评估工作[13-14]中,多是考虑用户在跨域访问中由于不同系统信任度评价机制不统一造成的对数据访问的安全威胁,还未出现与本文类似的针对用户可信度评价数据的隐私保护工作。此外,与本文均值计算相关的隐私保护方案,除了基于本地差分隐私的均值机制,还存在一些利用安全多方计算技术进行设计的均值计算算法。然而,安全多方计算中多用到密码学工具,虽然可以获得准确的计算结果,但其通信和计算开销往往较大,难以有效地在异构身份联盟环境下应用。

4 结 语

本文主要研究了联盟体系内关于用户综合信任度评估计算中存在的隐私泄漏问题,并基于已有的差分隐私保护机制,设计了两种满足 ε-本地差分隐私的综合可信度计算算法。在该算法下,每个身份域在共享对用户的真实评价结果时可以有效地隐藏其真实信息,同时,仍然能够从所有身份域扰乱的评价结果中恢复出对用户的综合可信度评价结果。通过理论分析和实验验证,该算法能够达到相应的隐私保护效果,并能获得高准确率的计算结果。

参 考 文 献

[1] Oppliger R. Microsoft. Net passport: A security analysis[J]. Computer, 2003, 36(7): 29-35.

[2] Ellin B. About openID[EB/OL]. [2023-01-05]. http://www. openidenabled. com/openid/about-openid.

[3] Ping identity. ShoCard blockchain identity management white paper. [EB/OL]. [2023-01-05]. https://shocard. com/blockchain-identity-whitepapers/.

[4] Kasiviswanathan S P, Lee H K, Nissim K, et al. What can we learn privately? [J]. SIAM Journal on Computing, 2008, 40(3): 793-826.

[5] Gupta A, Hardt M, Roth A, et al. Privately releasing conjunctions and the statistical query barrier[J]. SIAM Journal on Computing, 2013, 42(4): 1494-1520.

[6] Erlingsson U, Ifar V. Pihur A. Korolova, RAPPOR: Randomized aggregatable privacy-preserving ordinal response [C]//Proceedings of ACM Sigsac Conference on Computer and Communications Security, 2014.

[7] Warner S L. Randomized response: A survey technique for eliminating evasive answer bias[J]. Journal of the American Statistical Association, 1965, 60(309): 63-66.

[8] Dwork C. Differential privacy[C]//Proceedings of International Conference on Automata, Languages and Programming, 2006.

[9] Dwork C, McSherry F, Nissim K, et al. Calibrating noise to sensitivity in private data analysis[C]//Proceedings of Theory of Cryptography Conference, 2006.

[10] Duchi J C, Jordan M I, Wainwright M J. Local privacy and statistical minimax rates[C]//Proceedings of IEEE Symposium on Foundations of Computer Science, 2013.

[11] Duchi J C, Jordan M I, Wainwright M J. Minimax optimal procedures for locally private estimation[J]. Journal of the American Statistical Association, 2018, 113(521): 182-201.

[12] Wang T, Blocki J, Li N, et al. Locally differentially private protocols for frequency estimation[C]//Proceedings of the 26th USENIX Security Symposium, 2017.

[13] 汪伦伟,廖湘科,王怀民. 可信度共享认证模型研究[J]. 计算机工程与科学,2005,27(9):29-31.

[14] 董贵山,陈宇翔,李洪伟,等. 异构环境中基于区块链的跨域认证可信度研究[J]. 通信技术,2019,52(6):1450-1460.

(上接第 338 页)

[13] 韦炜,全渝娟,卓奕涛,等. 基于多阶马尔可夫预测的个性化推荐算法[J]. 计算机工程,2015,41(11):59-66.

[14] Bulba Y, Ponochovny Y, Sklyar V, et al. Classification and research of the reactor protection instrumentation and control system functional safety Markov models in a normal operation mode[C]//2nd International Workshop on Theory of Reliability and Markov Modeling for Information Technologies, 2016.