doi:10.11835/j.issn.1000-582X.2018.09.010

多维分解加噪算法在智能电网隐私保护中的优化

陈　倩,刘　云
(昆明理工大学 信息工程与自动化学院,昆明 650500)

摘要:在智能电网的数据采集监测中,针对用户隐私泄露安全隐患问题,采取加噪为主的方式来实现隐私保护。提出一种基于多维分解的拉普拉斯噪声算法(MDLN, multidimensional laplacian noise algorithm),该算法将原始测量值分解成多维数据,并根据各维度的隐私敏感度,自适应决定需添加的拉普拉斯噪声幅度,通过有效的噪声扰动方式实现差分隐私。通过与 SLN (simple laplacion noise algorithm)算法 ULN(uniform laplacian noise algorithm)算法相比较,仿真表明,MDLN 算法的隐私保护强度较高,且效能更高。

关键词:实时监测系统;拉普拉斯噪声;多维分解;差分隐私;MDLN 算法
中图分类号:TN918　　**文献标志码**:A　　**文章编号**:1000-582X(2018)09-086-08

Optimization of multi-dimensional decomposition and plus noise algorithm in intelligent grid privacy protection

CHEN Qian, *LIU Yun*
(Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650500, P.R.China)

Abstract: To address the security problem of user privacy leak in the data acquisition and monitoring of smart grid, noise is usually added to achieve privacy protection. In this paper, a Laplacian noise algorithm based on multidimensional decomposition (MDLN) is proposed. The algorithm decomposes the original measured value into multidimensional data, and adaptively determines the Laplacian noise amplitude to be added according to the sensitivity of each dimension, achieving differential privacy by effective noise perturbation. The simulation results show that the MDLN algorithm has higher privacy protection and higher performance compared with the SLN (simple Laplacian noise algorithm) algorithm and ULN (uniform Laplacian noise algorithm) algorithm.

Keywords: real-time monitoring system; Laplacian noise; multidimensional decomposition; difference privacy; MDLN algorithm

在智能电网的实时监测系统中,随着智能设备、智能表计和智能终端等广泛使用,细粒度测量使用户隐私泄露问题越加的严重[1-2]。从传感器收集实时测量可以推断出用户的行为隐私,虽然细粒度的测量不能直接访问,但仍可以通过现有的差分攻击从实时聚合的动态序列中推断出详细测量。为了使用户隐私得到有

收稿日期:2017-12-11
基金项目:国家自然基金资助项目(61262040)。
Supported by the National Natural Science Foundation of China(61262040).
作者简介:陈倩(1994—),女,云南人,硕士研究生,主要从事无线传感网方向研究,(E-mail)1575093316@qq.com。
通讯作者:刘云(1973—)男,云南人,副教授,主要从事无线通信研究,(E-mail)liuyun@kmust.edu.cn。

效保护，一般采用加密和加噪 2 种方式实现[3]，虽然加密方式可以有效实现数据的完整性和机密性，但机密性不等于隐私性且开销较高。因此，将采用更为高效，成本较低的加噪方式实现隐私保护。

Anandan B 等人提出了一种简单的拉普拉斯噪声算法(SLN, simple laplacian noise algorithm)[4]，该算法根据给定的全局敏感度来直接添加拉普拉斯噪声，通过噪声扰动的方式，使用户数据与噪声之间不易区分，有效避免了隐私泄露。但由于全局敏感度较高，使所添加的噪声幅度增大，导致隐私保护效用降低以及噪声方差增加。Geng Q 等人提出一种均匀拉普拉斯噪声算法(ULN, uniform laplacian noise algorithm)[5]，该算法具有等概率的噪声分布，即每个维度所添加噪声一致，有效实现了数据隐私保护，但其效能性依然无法达到最优。

在 SLN 算法和 ULN 算法研究基础上，提出一种基于多维分解的拉普拉斯噪声算法(MDLN, multi-dimensional laplacian noise algorithm)，该算法将原始测量值分解成多维数据，计算各维度的隐私敏感度，并根据相应的敏感度自适应决定需添加的拉普拉斯噪声幅度，针对高相关性和高度波动的时间序列数据，通过噪声扰动方式可以有效实现差分隐私。通过与 SLN 算法和 ULN 算法仿真相比较，MDLN 算法的隐私保护强度较高，且效能更高。

1　模型建立

1.1　模型构建

在简单的拉普拉斯噪声算法中，由于给定的全局敏感度较高，使整体需添加的拉普拉斯噪声较大，从而导致噪声方差增加以及数据效能下降。因此，在满足差分隐私前提下，根据输出函数的各维度敏感度来自适应计算需添加的拉普拉斯噪声，以提高数据效能是至关重要的，即采用降低敏感度的方式来提高数据效能。

模型建立如下：在实时的监测系统中，传感器部署在用户端以完成数据采集监测，并将实时测量的数据传送到集中式服务器，服务器对接收到的数据进行统计分析，即针对个体用户的时间序列进行聚合[6-7]。假设传感器仪表是值得信赖的设备，且传感器仪表与集中式服务器之间的通信通道安全可靠。现假定一个单变量的离散时间序列 $X=\{x_k\}$ 表示为时隙 k 的实时测量数据，且第 t 个时隙实时聚合表示为 $r_t=\sum_{k=1}^{t}x_k$，即从第 1 时隙到 t 时隙的用户时间序列测量累积和。研究所使用的符号列于表 1 如下所示。

表 1　符号列表

Table 1　List of symbols

符号	含义
g/GS_f	全局敏感度
b	界值
ε	隐私保护预算
d	维度
s_i	第 i 维度的敏感度
m_i	第 i 维度需添加的噪声
$Pr[.]$	分布函数的概率
$\mathrm{Lap}(\lambda)$	零均值和参数 λ 的拉普拉斯分布
r	产生的随机噪声
x_k	第 k 时隙的测量值
r_k	第 k 时隙的聚合结果
E	变量的期望值
var/V	噪声方差
c_k^i	第 k 时隙在第 i 维度的聚合结果

1.2　差分隐私定义

差分隐私(DP，differential privacy)是一种基于数据失真的隐私保护技术，即通过随机噪声的添加使敏

感数据失真,同时保持某些数据或数据属性不变,处理后的数据仍然具有一定的统计特性[8]。

假设 ε 为指定的隐私保护预算,该参数通常用来控制算法在2个邻近数据集上获得相同输出的概率比值。通常情况下,ε 取值较小[9],因为当 ε 减小时,隐私保护强度增加,当 $\varepsilon=0$ 时,隐私保护强度达到最高,此时可以保证算法输出的任意相邻数据集都具有相同的概率分布。因此,ε -差分隐私可以保证具有相同输出的2个相邻数据集的概率非常接近,使概率扩展受到 $\exp(\varepsilon)$ 界限,以致于攻击者几乎不能通过操纵输出来推断单个数据记录[10-11]。

为了实现 ε -差分隐私,提出将正确校准的拉普拉斯噪声添加到输出值,使攻击者无法判断噪声与数据之间的差别。已知拉普拉斯噪声由具有概率密度函数 $\mathrm{Lap}(\lambda)=\frac{1}{2\lambda}e^{-|x|/\lambda}$ 的拉普拉斯分布所绘制,其中参数 λ 由全局敏感度 GS_f 和隐私预算 ε 决定,即 $\lambda=GS_f/\varepsilon$[12-13]。全局敏感度 GS_f 定义为2个相邻数据集输出的最大差值,是决定噪声量添加大小的参数,通常表示为实数值,若为浮点数,则可以转换为实数。

2 MDLN 算法

2.1 算法分析

为了实现高隐私保护强度和高数据效能,提出一种多维分解的拉普拉斯噪声算法(MDLN),算法将输出实数分解成有界数的几个加权维度,并根据给定的全局敏感度 g,隐私保护预算 ε 和界值 b,计算获得随机屏蔽噪声 r,其算法流程如下所示

算法:多维分解拉普拉斯噪声算法 MDLN

输入:全局敏感度 g,界值 b 和隐私保护预算 ε

输出:随机噪声 r

1:计算维数 $d=\lfloor \log_b g \rfloor+1$

2:if 维数 $d=1$ then

3:维度敏感度是 $s_1=g$

4:else

5:指定低于 $d-1$ 维度的敏感度为 $s_i=b-1(i=1,2,\cdots,d-1)$,计算最高维度的敏感度为 $s_d=\left\lfloor \frac{g}{b^d-1} \right\rfloor$

6:end if

7:根据具有参数 s_i 和 ε 的拉普拉斯噪声分布 $\mathrm{Lap}\left(\frac{s_i}{\varepsilon}\right)$ 产生 d 个独立噪声 $m_i(i=1,2,\cdots,d)$

8:产生随机噪声 r,即 $r \leftarrow \sum_{i=1}^{d} m_i b^{i-1}$

根据以上算法流程,进一步说明如下

1)根据给定的全局敏感度 g、界值 $b(2\leqslant b\leqslant g)$ 和隐私保护预算 ε,自适应计算出维度 d,计算公式为:$d=\lfloor \log_b g \rfloor+1$。

2)通过界值 b 可以指定多维度的权重:假设 $b=10$,则可以看作是十进制分解;$b=8$,则为八进制分解;$b=2$,则是二进制分解,则第 i 维度的权重 $w_i=2^{i-1}$。

3)通过界值 b 引入 d 个维度中各维度的敏感度 $s_i(i=1,2,\cdots,d)$,低于 $d-1$ 维度的敏感度 $s_i=b-1(i=1,2,\cdots,d-1)$,第 d 维度的敏感度 $s_d=\left\lfloor \frac{g}{b^d-1} \right\rfloor$,且 $\left\lfloor \frac{g}{b^d-1} \right\rfloor<b-1$。然后根据各维度的敏感度自适应调整需添加的拉普拉斯噪声幅度,并生成所有维度的屏蔽噪声 r。

4)根据所绘制的拉普拉斯分布 $\mathrm{Lap}\left(\frac{s_i}{\varepsilon}\right)$,决定各维度需添加的独立噪声 $m_i(i=1,2,\cdots,d)$,在所有 d 维度上实现差分隐私。

5)最后,将各维度的相应权重 $w_i=b^{i-1}$ 与独立噪声 m_i 线性结合,得到整体掩蔽噪声 $r=\sum_{i=1}^{d} m_i b^{i-1}$,掩蔽噪声 r 可用于实现总体差分隐私。

6)当 $b\geqslant g+1$ 时,维度数 $d=1$,则维度敏感度应为 $s_1=g$。此时,MDLN 算法降解为简单的拉普拉斯噪

声算法 SLN。

对于每个维度,基于拉普拉斯噪声机制计算添加的噪声 m_i 以实现差分隐私,根据平行组合定理,在不同维度的不相交子集上计算所有噪声,平行组合可以满足差分隐私[14]。根据并行组合定理,所有独立维度的组合输出仍然可以保证相同水平的差分隐私。

2.2　MDLN 隐私分析

针对 MDLN 算法的差分隐私进行分析,即定理如下

定理 1:MDLN 算法满足 ε −差分隐私。

证明:将 C 表示为 MDLN 算法的多维分解,C_i 表示第 i 维的分解输出,v 表示为观察值,v_i 表示每个维度的分解结果。根据 MDLN 算法,各维度输出 C_i 和 $v_i(i=1,2,\cdots,d-1)$应在范围$[0,b-1]$内,C_d 和 v_d 应在$[0,s_d]$内。每个维度通过添加校准拉普拉斯噪声 $\mathrm{Lap}(\lambda)=\frac{1}{2\lambda}e^{-|x|/\lambda}$来满足ε−差分隐私,其中 $\lambda=\Delta f/\varepsilon$ 且 Δf 表示全局敏感度,噪声 $\delta(x)$与 $\exp(-\varepsilon|x|/\Delta f)$成比例。

在组合中,分解的维度具有不同的权重 $w_i=b^{i-1}$,因此每个维度值应该被缩放为新的变量 $Y_i=b^{i-1}C_i(S)$。则组合后的测量值 $S=Y_1+Y_2+\cdots+Y_d$ 的敏感度为 $\Delta f=\sum_{i=1}^{d-1}(b-1)b^{i-1}+s_db^{d-1}=b^{d-1}+s_db^{d-1}-1$。假设在 d 个维度上相邻测量值 S'由 d 个独立测量 $Y'_1,Y'_2,\cdots,Y'_d$ 组成,可以得到 $Y'_i=w_iC_i(S')$。在每个维度上,第 i 维上的变量 Y_i 和 Y'_i 应该遵循关系 $Pr\,[Y_i]=Pr\,[Y'_i]\times\exp\left(\frac{\varepsilon}{\Delta f}|Y_i-Y'_i|\right)=Pr\,[Y'_i]\times\exp\left(\frac{b^{i-1}\varepsilon}{\Delta f}|C_i-C'_i|\right)$,应该注意的是$|C_i-C'_i|\leqslant b-1$ 以及 $|C_d-C'_d|\leqslant s_d$。使用上述差分隐私的关系和定义,假设有 2 个测量值 S 和 S',通过 MDLN 算法分别分解为 d 个维度测量值 $Y_i=w_i\cdot C(S)$和 $Y'_i=w_i\cdot C(S')$,并且在每个维度添加噪声之后,S 和 S'将映射到具有 d 维度相同的测量值 v 和 v_i,则

$$
\begin{aligned}
Pr\,[C(S)=v]&=\prod_{i=1}^{d}Pr\,[Y_i=v_i]=\prod_{i=1}^{d}Pr\,[w_iC_i(S)=v_i]=\\
&\prod_{i=1}^{d}Pr\,[w_iC_i(S')=v_i]\times\prod_{i=1}^{d}\exp\left(\frac{\varepsilon}{\Delta f}\times w_i|C_i(S)-C_i(S')|\right)=\\
&\prod_{i=1}^{d}Pr\,[w_iC_i(S')=v_i]\times\prod_{i=1}^{d-1}\exp\left(\frac{\varepsilon}{\Delta f}\times b^{i-1}|C_i(S)-C_i(S')|\right)\times\\
&\exp\left(\frac{\varepsilon}{\Delta f}\times b^{d-1}|C_d(S)-C_d(S')|\right)=\\
&\prod_{i=1}^{d}Pr\,[w_iC_i(S')=v_i]\times\exp\left(\frac{\varepsilon}{b^{d-1}+s_db^{d-1}-1}\times\right.\\
&\left.\sum_{i=1}^{d-1}(b^{i-1}|C_i(S)-C_i(S')|)\right)\times\\
&\exp\left(\frac{\varepsilon}{b^{d-1}+s_db^{d-1}-1}\times b^{d-1}|C_d(S)-C_d(S')|\right)\leqslant\prod_{i=1}^{d}Pr\,[w_iC_i(S')=v_i]\times\\
&\exp\left(\frac{\varepsilon}{b^{d-1}+s_db^{d-1}-1}\times(b^{d-1}+s_db^{d-1}-1)\right)=\\
&\prod_{i=1}^{d}Pr\,[w_iC_i(S')=v_i]\times\exp(\varepsilon)=\\
&Pr\,[C_i(S')=v]\times\exp(\varepsilon)
\end{aligned}
\tag{1}
$$

由以上可知,在 MDLN 算法中映射到相同测量 v 的 2 个测量 S 和 S'是不可区分的。因此,MDLN 算法满足 ε −差分隐私。

2.3　MDLN 效能分析

针对 MDLN 算法的效能进行分析,已知通过 MDLN 算法可以获得掩蔽噪声的分布特征。首先,对满足 ε −差分隐私的 SLN 算法掩蔽噪声的方差表示为

$$V_{\mathrm{SLN}}=2\left(\frac{g}{\varepsilon}\right)^2, \tag{2}$$

其中全局敏感度 g 满足以下不等式

$$b^{2(d-1)}\leqslant g^2\leqslant(b^d-1)^2。 \tag{3}$$

然后，对 MDLN 算法中噪声的预期值和方差详细分析如下：首先，每个维度上所加噪声都遵循拉普拉斯分布，即 $m_i\sim\mathrm{Lap}(s_i/\varepsilon)$，且每个噪声的预期值为 0，这些噪声彼此独立。因此，预期值为 0 的 d 个独立噪声线性组合后掩蔽噪声 r 的预期值仍为 0。已知 $m_i\sim\mathrm{Lap}(s_i/\varepsilon)$，根据拉普拉斯分布特征，噪声方差为$2\left(\frac{s_i}{\varepsilon}\right)^2$。因为维度权重表示为 b^{i-1}，则维度方差为 $v_i=b^{2(i-1)}\times2\left(\frac{s_i}{\varepsilon}\right)^2$。根据噪声的独立性，组合输出 r 的方差 V 应该是 d 个噪声值 m_i 的方差总和。可以得到

$$V=\sum_{i=1}^{d}v_i=\sum_{i=1}^{d}b^{2(i-1)}\times2\left(\frac{s_i}{\varepsilon}\right)^2=\sum_{i=1}^{d}(b^{(i-1)}s_i)^2\times2\left(\frac{1}{\varepsilon}\right)^2, \tag{4}$$

其中 $s_i\leqslant b-1$。

现定义有利比率(FR，favorable ratio)来显示 MDLN 算法与 SLN 算法相比的有效性，以及 ULN 算法与 SLN 算法相比的有效性，定义如下

定义 1(有利比率)：当给定相同的全局敏感度 g 和隐私保护预算 ε，计算 MDLN 算法比 SLN 算法输出较少的噪声方差的概率，以及 ULN 算法比 SLN 算法输出较少噪声方差的概率。现在对 MDLN 算法的效能分析描述如下

首先全局敏感度 g 满足以下不等式

$$nb^{d-1}\leqslant g\leqslant(n+1)b^d-1, \tag{5}$$

$$n^2b^{2(d-1)}\leqslant g^2<(n+1)^2b^{2d},(n=1,2,\cdots,b), \tag{6}$$

且相应的方差表示为

$$\begin{aligned}V_{\mathrm{MDLN}}=&\sum_{i=1}^{d}b^{2(i-1)}\cdot2\left(\frac{s_i}{\varepsilon}\right)^2=\\&\sum_{i=1}^{d-1}b^{2(i-1)}\cdot2\left(\frac{b-1}{\varepsilon}\right)^2+b^{2(d-1)}\cdot2\left(\frac{s_d}{\varepsilon}\right)^2=\\&\sum_{i=1}^{d-1}b^{2(i-1)}\cdot2\left(\frac{b-1}{\varepsilon}\right)^2+b^{2(d-1)}\cdot2\left(\frac{n}{\varepsilon}\right)^2\leqslant\\&\left(\sum_{i=1}^{d}b^{2(i-1)}\right)2\left(\frac{b-1}{\varepsilon}\right)^2\leqslant2\left(\frac{g}{\varepsilon}\right)^2,\end{aligned} \tag{7}$$

其中 MDLN 算法的噪声方差远小于 SLN 算法，显示出更好的效能。

此外，将 L 和 l 分别定义为间隔 $[n^2b^{2(d-1)},(n+1)^2b^{2d}]$ 和$\left[\frac{(b-1)(b^{2(d-1)}-1)}{b+1}+n^2b^{2(d-1)},(n+1)^2b2d\right]$的长度，且定义比率 l/L 表示 MDLN 算法的有利比率。可以得到

$$\lim_{d->\infty}fr(b,d)=\lim_{d->\infty}\frac{l}{L}=\frac{b^3-3}{(b+1)(b^2-1)}, \tag{8}$$

$$\lim_{b->\infty}fr(b,d)=\lim_{b->\infty}\frac{l}{L}=1(b,d\in N^+)。 \tag{9}$$

从上式可以看出，MDLN 算法的有利比率将随界值 b 和维度 d 的增长而增长，最终趋向于 1，且界值 b 将增加时，维度 d 将减小。

3 仿真分析

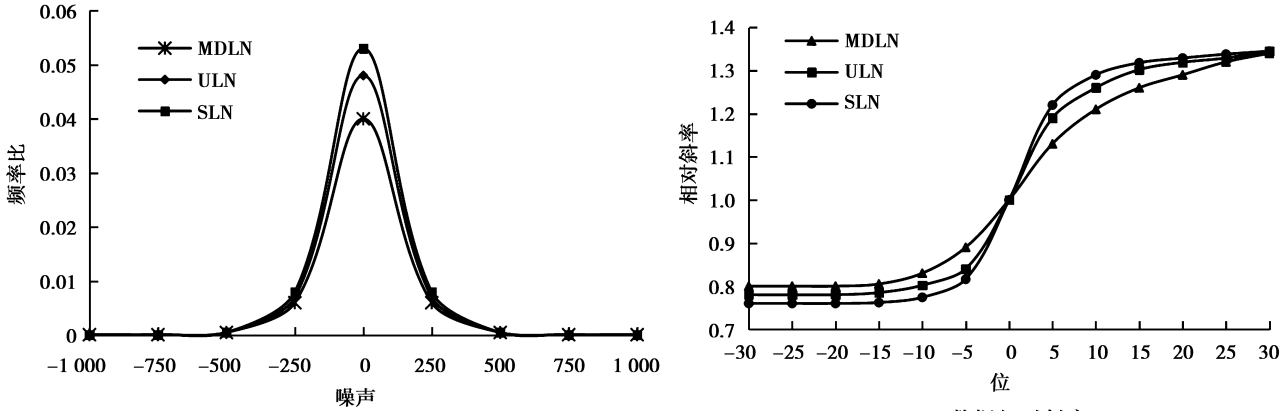
为了验证相比 ULN 算法和 SLN 算法，MDLN 算法在隐私保护强度和效能上达到最优，需对仿真参数进行设定。首先，假定一个智能计费系统场景，住宅智能电表将定期收集用户用电量的实时测量值，累计用

户的用电量,并将实时汇总返回系统服务器进行结算[15]。根据 Richardson 等人开发的模拟器生成的电量使用数据[16],随机选择了不同家庭大小,不同家用电器和不同占用模式的用户一天用电量数据进行仿真,所有测量值将被预处理为整数,浮点数也可以转换为整数。现设全局敏感度 g 的范围为 1 到 2 000,差异隐私保护预算 $\varepsilon=2$,参数 b 可取不同的值,

在仿真比较中,将采用噪声分布和数据相邻位的相对斜率来间接表示 3 种算法的隐私保护强度。相对斜率由相邻位之间频率比计算可得,即通过 $\exp(\varepsilon)=1+\varepsilon$ 反映隐私保护强度,相对斜率与 1 之间的最大绝对差即显示了隐私保护预算 ε。当相对斜率为 1 时,表示 $\varepsilon=0$ 且相邻位之间具有完全相同的隐私概率。当相对斜率比 1 大出$(1+\varepsilon)$或比 1 小出$(1-\varepsilon)$时,表示隐私保护强度较低。采用噪声方差和有利比率来间接表示 3 种算法的效能性,见公式(7)-(9)。

1)隐私保护强度分析

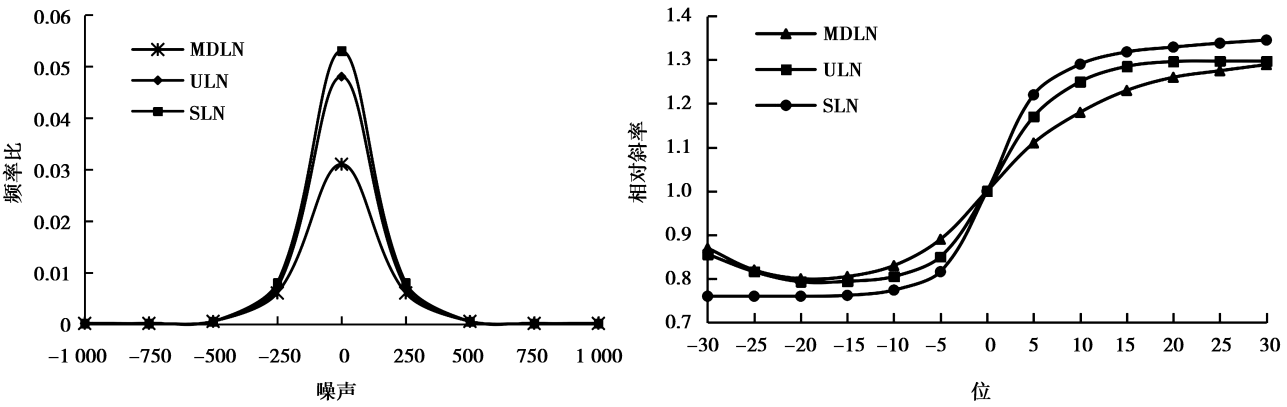
为了表征 MDLN 算法,ULN 算法和 SLN 算法的隐私保护强度,采用噪声分布和数据相邻位的相对斜率间接表示。如图 1(a)和图 2(a)所示,显示了 MDLN 算法,ULN 算法和 SLN 算法的噪声分布结果。从图中看出,相比 SLN 算法和 ULN 算法,MDLN 算法的噪声分布更加紧凑,且频率比较低,表示该噪声具有更高的集中性和效能性。如图 1(b)和图 2(b)所示,显示了 MDLN 算法,ULN 算法和 SLN 算法在数据相邻位的相对斜率。从图中看出,相比 SLN 算法和 ULN 算法,MDLN 算法的相对斜率在负半轴中较大,在正半轴中较小,表示 MDLN 算法的相邻测量值之间的噪声差异较小。对比 SLN 算法和 ULN 算法,MDLN 算法的隐私保护强度更好。



(a)噪声分布直方图　　(b)数据相对斜率

图 1　$b=2,\varepsilon=2$ 时隐私保护强度变化示意图

Fig.1　the privacy protection strength changes map $b=2,\varepsilon=2$



(a)噪声分布直方图　　(b)数据相对斜率

图 2　$b=5,\varepsilon=2$ 时隐私保护强度变化示意图

Fig.2　The privacy protection strength changes map $b=5,\varepsilon=2$

2)效能分析

为了表征 MDLN 算法,ULN 算法和 SLN 算法的效能性,采用噪声方差和有利比率来间接表示。如图 3 所示,显示了 MDLN 算法,ULN 算法和 SLN 算法噪声方差随全局敏感度的变化示意图。从图中可以看出,随着全局敏感度的增加,MDLN 算法,ULN 算法和 SLN 算法的噪声方差逐渐增加,且 ULN 算法的噪声方差小于 SLN 算法的噪声方差。对比 SLN 算法和 ULN 算法,MDLN 算法的噪声方差达到最小。

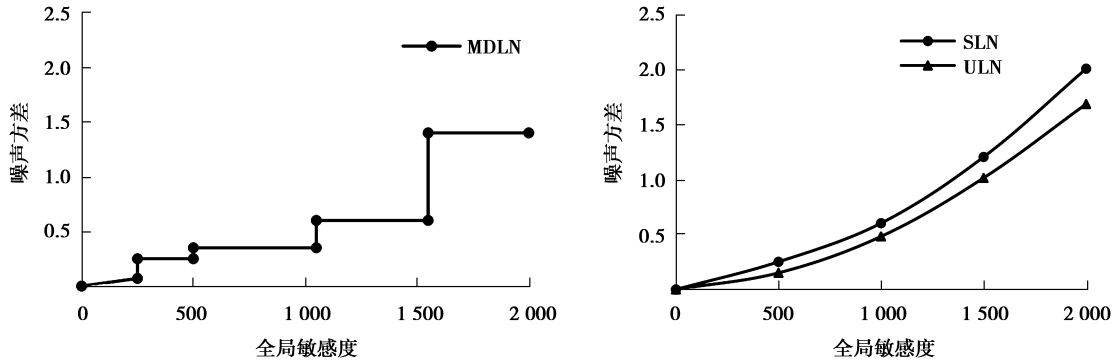


图 3 噪声方差随全局敏感度的变化示意图

Fig.3 Variation of noise variance with global sensitivity

如图 4 所示,显示了 MDLN 算法和 ULN 算法有利比率随界值 b 的变化示意图($g=2\ 000$)。从图中可以看出,随着 b 值的增加,ULN 算法的有利比率逐渐下降(波动是由界值 b 相对较小时,分解后维度 d 增大所引起),而 MDLN 算法的有利比率均大于 0.5。可以得出,当给定的界值 b 较大时,分解后的维度 d 下降,此时所有维度都具有更高效的噪声覆盖。在 MDLN 算法中,由于最高维度敏感度小于界值 b,因此屏蔽噪声的效率更高。相比 ULN 算法,MDLN 算法的数据效能性更高。

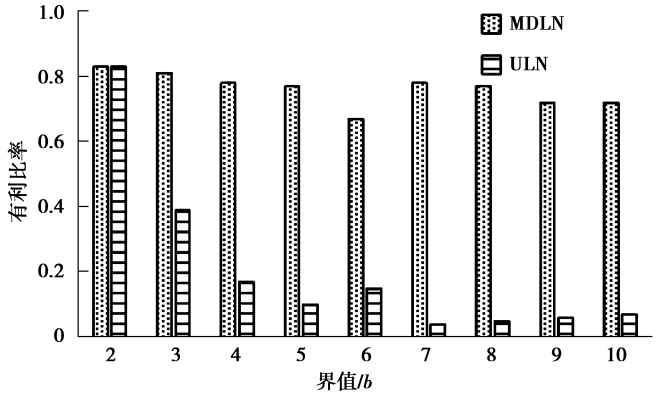


图 4 有利比率随 b 值的变化示意图

Fig.4 diagram of the change in favorability ratio with b value

4 结 论

为解决智能电网中用户隐私泄露问题,实现用户数据的完整性和强安全性,笔者提出一种基于多维分解的拉普拉斯噪声算法(MDLN),该算法对用户的电能数据进行聚合,并根据给定的界值对聚合后的原始数据进行分解,计算分解后各维度的隐私敏感度,根据敏感度自适应添加拉普拉斯噪声,通过验证,该算法可以有效的实现差分隐私。仿真表明,与 SLN 算法和 ULN 算法相比较,MDLN 算法的隐私保护强度较高,且效能更高。鉴于隐私特性,该算法同样适用于其它弱终端无线传感网的监测系统。

参考文献:

[1] 黄秀丽,张涛,马媛媛,等.智能电网隐私保护技术的分析研究[J].计算机技术与发展,2014(2):189-193.
HUANG Xiuli, MA Tao, MA Yuanyuan, et al. Analysis and research on intelligent power grid privacy protection technology[J].Computer Technology and Development,2014(2):189-193.(in Chinese)

[2] Birman K, Kleinberg R, Tremel E. Building a secure and privacy-preserving smart grid[J]. Acm Sigops Operating Systems Review, 2015, 49(1):131-136.

[3] Li Y, Dai W, Ming Z, et al. Privacy protection for preventing data over-collection in smart city[J]. IEEE Transactions on Computers, 2016, 65(5):1339-1350.

[4] Anandan B, Clifton C. Laplace noise generation for two-party computational differential privacy[C]// Conference on Privacy, Security and Trust. Turkey: IEEE Computer Society, 2015:54-61.

[5] Geng Q, Viswanath P. Optimal noise adding mechanisms for approximate differential privacy[J]. IEEE Transactions on Information Theory, 2013, 62(2):952-969.

[6] Gudžius S, Gvozdas V, Markevi L A, et al. Real time monitoring of the state of smart grid[J]. Elektronika Ir Elektrotechnika, 2015, 2(10):405-416.

[7] Nithin S, Sivraj P, Sasi K K, et al. Development of a real time data collection unit for distribution network in a smart grid environment[C]// Power and Energy Systems Conference: Towards Sustainable Energy. India: IEEE, 2014:1-5.

[8] 宋健,许国艳,夭荣朋.基于差分隐私的数据匿名化隐私保护方法[J].计算机应用,2016,36(10):2753-2757.
SONG Jian,XU Guoyan,YAO Rongpeng. Data anonymity privacy protection method based on differential privacy[J]. Journal of Computer Applications,2016,36(10):2753-2757.(in Chinese)

[9] 兰丽辉,鞠时光.基于差分隐私的权重社会网络隐私保护[J].通信学报,2015,36(9):145-159.
LAN Lihui, JU Shiguang. Weighted social network privacy protection based on differential privacy[J]. Journal on Communications,2015,36(9):145-159.(in Chinese)

[10] Redmond M. Mechanism design via differential privacy[J]. Foundations of Computer Science Annual Symposium on, 2016:94-103.

[11] 郭旭东,吴英杰,杨文进,等.隐私保护轨迹数据发布的 l-差异性算法[J].计算机工程与应用,2015,51(2):125-130.
GUO Xudong, WU Yingjie, YANG Wenjin, et al. Privacy protection trajectory data release l-difference algorithm[J]. Computer Engineering and Applications,2015,51(2):125-130.(in Chinese)

[12] 王宝楠. 基于差分隐私拉普拉斯机制的线性回归分析研究[D]. 合肥:安徽理工大学, 2016.
WANG Baonan. Linear regression analysis based on differential privacy laplace mechanism[D]. Hefei: Anhui University of Science and Technology,2016.(in Chinese)

[13] He S W, Wang J G, Yao R Q. The characterizations of laplacians in white noise analysis[J]. Nagoya Mathematical Journal, 2016, 143(588):93-109.

[14] Kairouz P, Viswanath P. The composition theorem for differential privacy[J]. IEEE Transactions on Information Theory, 2015,63(6):4037-4049.

[15] Ren X, Yang X, Lin J, et al. On binary decomposition based privacy-preserving aggregation schemes in real-time monitoring systems[J]. IEEE International Conference on Communications. IEEE, 2015:7083-7088.

[16] Bera S, Misra S, Rodrigues J P C. Cloud computing applications for smart grid: a survey[J]. Parallel & Distributed Systems IEEE Transactions on, 2015, 26(5):1477-1494.

(编辑　侯　湘)