Non-Invasive Identification of Electrical Equipment in a Limited Security Environment*

WANG Senlin, CHEN Si, LEI Jiahao, BAO Yongqiang*
(School of Electric Power Engineering, Nanjing Institute of Technology, Nanjing Jiangsu 211167, China)

Abstract: Targeting at the problems of high computing cost of encryption and decryption in the existing non-invasive load identification data security environment and poor data availability in the disturbed environment, a non-invasive identification method for electrical equipment in the limited security environment is proposed based on the concept of data disturbance. Mel-scale frequency cepstral coefficients (MFCC) are taken as load characteristics, pseudo-random signals whose bandwidth corresponds to the subbands of the electrical data to be protected are constructed and added with the current data to mask the subbands of the current data to be protected. MFCC feature is extracted from unmasked subbands, corresponding learning and recognition process is carried out by using SVM. At the same time, Pearson correlation coefficient and Euclidean distance are used to optimize the subbands that need to be masked by particle swarm optimization. The experimental results show that the proposed scheme has advantages over the traditional scheme of adding random disturbance in device recognition rate and avoids the computational loss caused by traditional encryption and decryption data, and can protect the specific spectrum information of data while taking into account data availability.

Key words: load identification; data perturbation; non-intrusive load monitoring; privacy protection; MFCC
EEACC: 7220; 8110B **doi**: 10.3969/j.issn.1005-9490.2026.03.027

有限安全环境下的用电设备非侵入式识别*

王森林, 陈 思, 雷家浩, 包永强*
(南京工程学院电力工程学院, 江苏 南京 211167)

摘 要: 针对现有非侵入式负荷识别数据安全环境下加解密计算开销大和添加扰动环境下数据可用性较差问题, 基于数据扰动理念, 提出一种在有限安全环境下的用电设备非侵入式识别方法。以梅尔倒谱系数(Mel-scale Frequency Cepstral Coefficients, MFCC)作为负荷特征, 构建其带宽对应于需要保护的用电数据的子频带的伪随机信号与电流数据进行相加, 以遮掩需要保护的电流数据子频带, 通过对数据未遮掩子频带进行 MFCC 特征提取进行 SVM 的学习与识别。同时利用粒子群算法以皮尔逊相关系数和欧几里得距离作为指标优化需要遮掩的子频带。实验结果表明, 所提方案比传统添加随机扰动方案在设备识别率上具有优势, 可绕开传统加解密数据带来的计算损耗, 在兼顾数据可用性下可以对数据特定频谱信息进行保护。

关键词: 负荷识别; 数据扰动; 非侵入式负荷监测; 隐私保护; MFCC
中图分类号: TM714 **文献标识码**: A **文章编号**: 1005-9490(2026)03-0665-07

新型电力系统中作为热点之一的非侵入式负荷监测(Non-Intrusive Load Monitoring, NILM)技术可以利用用户侧采集的负荷数据, 通过负荷识别算法处理得到用户负荷情况。非电气类和电气类特征是 NILM 特征提取中主要使用的特征类别。电气类特征主要包括: 功率类、电流类和电压-电流(V-I)轨迹类。非电气类指标即使用非电气量作为特征指标计算得到的设备特征, 又称非传统特征, 在近年的 NILM 算法研究中已较少使用[1]。

非侵入式监测技术通过互联网进行数据传输完成交互, 若数据安全性无法保证, 会直接影响数据的完整性和有效性, 会造成隐私安全问题[2]。现有的对非侵入式负荷监测数据隐私保护技术主要包括加密和数据扰动两种方法。加密技术是一种以增加计算复杂度为代价的信息安全策略, 在智能电表隐私保护上, 同态加密技术是目前得到广泛应用的数据隐私保护方法[3]。同态加密技术具有在密文域上可以实现数据加密计算的性质, 利用此性质文

项目来源: 江苏省教育科学规划重点资助课题项目(B/2022/01/80)
收稿日期: 2024-03-29 **修改日期**: 2024-04-24

献[4-9]在对用电数据进行加密的同时实现了多维用电数据的聚合,而文献[10]将秘密共享和 Paillier 半同态加密算法结合构建安全多方协议进行模型加密运算,实现 NILM 负荷识别模型的全同态加密运算。也有研究从常规加密手段出发加密用电数据,文献[2]将对称加密算法和非对称加密算法结合,利用 AES+RSA 混合加密用户数据。虽然加密技术可以提供用电数据良好的隐私安全性,但其计算复杂度高,计算开销大。

数据扰动技术通过对原始数据添加扰动从而改变原始数波形来提高数据的机密性,但是数据扰动技术需要平衡添加扰动后的数据可用性和隐私安全问题。目前最常用在智能电表领域的数据扰动方法主要包括随机扰动、充电电池和差分隐私。充电电池技术基本思想是将一个额外设备的充放电操作添加到用户数据中来隐藏电力事件或者电器的负载特征[11]。文献[12-14]利用充电电池产生额外的充放电扰动来隐藏消费事件或单个电器的负载特征,提高了模式隐私的安全性。差分隐私技术本质是通过向数据中加入特定分布的噪声,使得任意单个数据或单条记录在统计结果上不可被区分[15],但是差分隐私技术主要保护单一数据,对于用户数据中隐含的变化规律保护不足,通常结合加密方案实现数据保护。文献[16]就提出了基于差分隐私与同态加密技术的电力数据聚合算法,在保证电力计费的安全性前提下实现在密文域的数据聚合,但其计算复杂度较高。随机扰动本质是通过给用户数据添加随机噪声,使得用户的原始数据发生变化。向原始数据中添加加性或乘性随机噪声来实现安全性和可用性的权衡是一种典型的方法[17-19],随机扰动方法能够有效地模糊单点数值,但其抗滤波的能力较差。

对上述已有非侵入式负荷识别数据保护方案流程的总结及本文方案流程如图 1 所示。在智能电表端如果承担不了加密所需的计算资源还需要上传至云端进行加密,所以本文方案针对加密情况下计算开销大和随机扰动下数据可用性较差问题,提出一种有限安全环境下的用电设备非侵入式识别方法,其中有限安全意味着对特定部分信息进行保护和允许保护外信息都可以泄露。本文以梅尔倒谱系数(Mel-scale Frequency Cepstral Coefficients,MFCC)作为负荷特征,构建其带宽对应于需要保护的用电数据的子频带的伪随机信号与电流数据进行相加,以遮掩需要保护的电流数据子频带,通过对数据未遮掩子频带进行 MFCC 特征提取进行 SVM 的学习与识别。同时利用粒子群算法以皮尔逊相关系数和欧几里得距离作为指标优化需要遮掩的子频带。

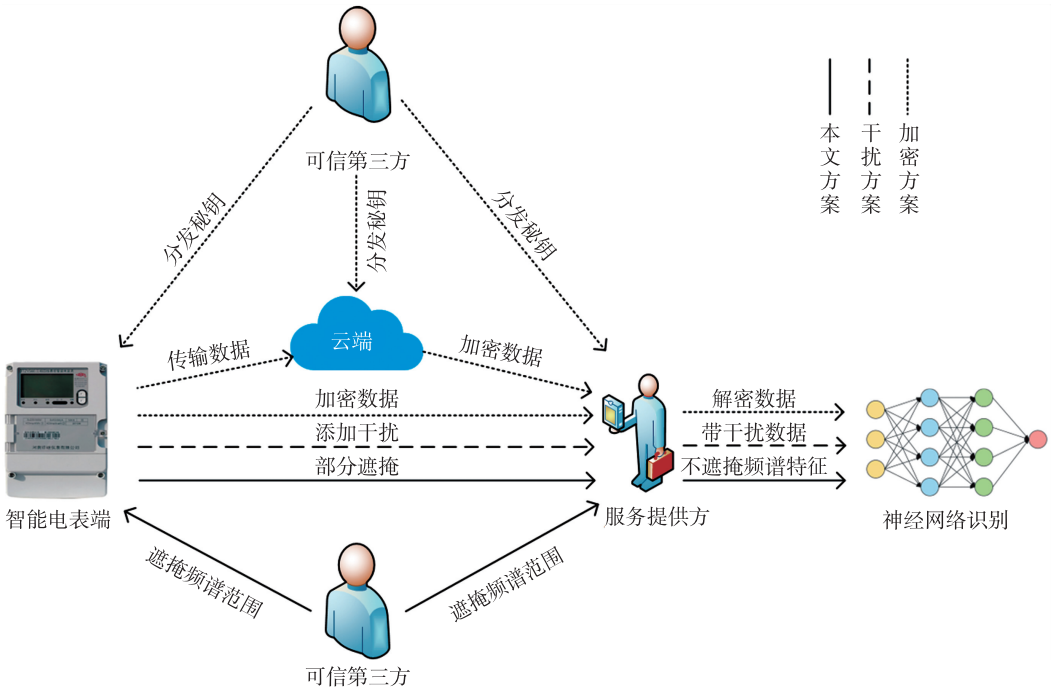

图 1 各方案流程图

1 MFCC 特征提取

1.1 MFCC 概述

Mel 频率倒谱系数(MFCC)由 Stevens、Volkman 和 Newman[20]在 1937 年提出,它是一种在语音信号处理中广泛使用的特征提取方法。它可以将语音信号转换为一组用于语音识别或语音处理的特征向量。它的基本思想是模拟人类听觉系统的特征提取

过程。但它也可以应用于其他信号类型的处理,在电信号处理中,电信号也可以分成若干个短时帧,并通过加窗和傅里叶变换将其转换为频域信号。然后,可以使用一组梅尔滤波器来计算每个频带的能量,并对每个频带的能量取对数。最后,可以使用离散余弦变换(DCT)将对数能量转换为 MFCC 系数作为电力负荷特征。

1.2　提取 Mel 频率倒谱系数流程

提取 MFCC 的过程大致可以分为以下几个步骤:首先,将信号分成短时间段,称为帧。然后,对每个帧应用傅里叶变换,将其转换为频谱。接下来,使用 Mel 滤波器组将频谱转换为 Mel 频率谱。然后,对 Mel 频率谱进行离散余弦变换(DCT),以获得 MFCC 系数。具体步骤如下:

①预加重:对于声音信号来讲,人耳对低频的信号更加敏感,所以在处理声音信号时应该先将信号通过预加重滤波器进而放大高频部分。

$$H_m(k)=\begin{cases}0 & k<f(m-1)\\ \dfrac{2[k-f(m-1)]}{[f(m+1)-f(m-1)][f(m)-f(m-1)]} & f(m-1)\leqslant k\leqslant f(m)\\ \dfrac{2[f(m+1)-k]}{[f(m+1)-f(m-1)][f(m)-f(m-1)]} & f(m)\leqslant k\leqslant f(m+1)\\ 0 & k\geqslant f(m+1)\end{cases} \tag{2}$$

式中:$f(m)$为三角滤波器中心频率。

Mel 刻度的目的是模拟人耳对声音的非线性感知,在较低的频率具有更强的辨别力,Mel 刻度定义如下:

$$F_{\text{mel}}(f)=2595\times\log_{10}\left(1+\frac{f}{700}\right) \tag{3}$$

⑥对数计算:计算每个滤波器组输出的对数能量。

⑦DCT:使用离散余弦变换(DCT)将对数能量转换为 MFCC 系数。

$$C(n)=\sum_{m=0}^{N-1}s(m)\cos\left(\frac{\pi n(m-0.5)}{M}\right),n=1,2,\cdots,L \tag{4}$$

式中:L 指 MFCC 系数阶数。这里 M 是三角滤波器个数。

提取 MFCC 流程如图 2 所示。

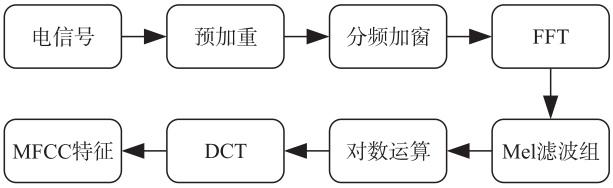

图 2　MFCC 流程图

②分帧:在预加重之后,我们需要将信号分成短时帧。

③加窗:将信号分割成帧后,我们再对每个帧乘以一个窗函数,如 Hamming 窗口,以增加每帧的连续性[21]。从而抵消 FFT 假设,并可以减少频谱泄漏。

④快速傅里叶变换(FFT)及能量求取:由于在时域上的变换通常很难看出信号的特性,通常做 FFT 变换,转换为频域上的能量分布来观察,变换后还需将频谱取模平方得到信号的谱线能量。变换公式如下:

$$X_a(k)=\sum_{n=0}^{N-1}x(n)\mathrm{e}^{-\mathrm{j}2\pi k/N},0\leqslant k\leqslant N \tag{1}$$

式中:$x(n)$为输入信号,N 表示傅里叶变换的点数。

⑤滤波器组:先计算 Mel 滤波器组,然后将功率谱通过一组 Mel 刻度的三角滤波器来提取频带。三角滤波器的频率响应定义为:

2　子频谱的遮掩及优化

本方案中子频谱可以根据具体情况下的安全需求进行选择,例如在对设备故障诊断识别时,可以选择设备数据低频段加入伪随机信号进行遮掩,利用高频段信息进行训练和识别。本文考虑到遮掩子频带方案下数据的可用性和安全性,在无具体安全需求下利用粒子群算法优化选择遮掩的子频带。

2.1　伪随机信号构建

伪随机噪声是一种看似随机的信号,但实际上是由确定性算法生成的。这个算法使用一个种子值作为输入,然后以一定的规律生成一系列数字。随机数的随机性只能在随机序列中体现。设随机变量 X(总体)服从某种随机分布,对其进行 n 次独立实验,得到一组简单随机样本序列 $x_1,x_2,\cdots,x_n$ 满足:

①$x_1,x_2,\cdots,x_n$ 相互独立;

②每一个 $x_1,x_2,\cdots,x_n$ 都与总体 X 同分布。

用递推方法产生伪随机序列如下:

$$x_n=f(x_{n-1},x_{n-2},x_{n-k}) \tag{5}$$

当 n 足够大时数列具有均匀分布随机变量独立抽样序列的性质,这一数列就称为伪随机序列。伪随机序列又有狭义伪随机序列和广义伪随机序列之

分。本文采用狭义伪随机序列,其自相关函数满足下式:

$$R_x(j)=\begin{cases}\dfrac{1}{n}\sum_{i=0}^{n-1}x_i^2=1 & j=0 \bmod n\\ \dfrac{1}{n}\sum_{i=0}^{n-1}a_ia_{i+j}=-\dfrac{1}{n} & j\neq 0 \bmod n\end{cases} \tag{6}$$

本文基于线性同余法产生伪随机数,而线性同余发生器(Linear Congruence Generator,LCG)来源于线性同余法,可以利用同余运算产生随机数。一般基本递推公式为:

$$x_{n+1}=(ax_n+c)\bmod m \tag{7}$$

约束条件为:

$$\begin{cases}a,c\geqslant 0\\ m>x_0,a,c\\ a,c,m\text{ 皆为正整数}\end{cases} \tag{8}$$

由基本递推公式得到的解析式为:

$$\begin{cases}x_1=(ax_0+c)\bmod m\\ x_i=(ax_{i-1}+c)\bmod m\\ u_i=x_i/m,i=1,2,\cdots\end{cases} \tag{9}$$

式中:u_i 为所得区间为[0,1]的随机数。

得到区间为[0,1]的随机数后,本方案需要构建固定频带上带有幅值的伪随机信号,首先生成一个与用户数据信号长度相同的强伪随机信号,然后对强伪随机信号进行傅里叶变换后,强制伪随机信号在需要遮掩的子频带外的频带上幅值为0,即:

$$F(\omega)=\begin{cases}0 & \omega<c_1\\ F(\omega) & c_1\leqslant\omega\leqslant c_2\\ 0 & \omega>c_2\end{cases} \tag{10}$$

式中:c_1,c_2 为需要遮掩的子频带范围。随后对伪随机信号进行傅里叶反变换得到固定频带的伪随机信号。

考虑到数据添加伪随机数后对原本的电信号会造成影响,还需要通过信噪比来选择伪随机数范围,信噪比公式如下:

$$\mathrm{SNR}=10\lg\frac{P_s}{P_n} \tag{11}$$

同时考虑遮掩部分添加随机信号后的数据安全性,以信息熵的概率来衡量数据安全性,信息熵是用来描述信息的不确定度或者信息量的概念,其计算公式为:

$$H(x)=-\sum p(x)\times\log_2(p(x)) \tag{12}$$

式中:$H(X)$表示随机变量 X 的信息熵,$p(x)$表示变量 X 取某个值的概率。

2.2 子频带范围选择

不同子频带构建的强伪随机信号与电流数据进行相加,会导致数据的安全性发生不同变化,而且数据选择不同子频带作 MFCC 变换得到的特征数据可实用性也会发生改变,因此需要选择合适的子频带进行遮掩,所以利用粒子群算法优化选择遮掩的子频带。本文通过利用粒子群算法以皮尔逊相关系数和欧几里得距离作为指标优化需要遮掩的子频带。

在自然科学领域中,皮尔逊相关系数广泛用于度量两个变量之间的相关程度,两个变量之间的皮尔逊相关系数定义为两个变量之间的协方差和标准差的商:

$$\rho(X,Y)=\frac{\mathrm{cov}(X,Y)}{\sigma(X)\sigma(Y)}=\frac{E\{[X-\mu(X))(Y-\mu(Y)]\}}{\sigma(X)\sigma(Y)} \tag{13}$$

皮尔逊系数的绝对值小于或等于 1。系数的值越近进 1 意味着两个变量越接近正相关,即一个变量增加时,另一个变量也同步增加。同理,系数的值越近进-1 意味着两个变量越接近负相关。可以使用皮尔逊系数衡量未加入和已加入伪随机信号相关性,系数越接近-1 两个信号变化趋势相反,即越安全。

欧几里得距离是一种常用的距离度量方法,用于衡量两个数据点之间的相似程度或区分度。在机器学习和数据挖掘领域,欧几里得距离常用于计算特征空间中的数据点之间的相似性或差异性。其 n 维空间计算公式如下:

$$d(x,y)=\sqrt{\sum_{i=1}^{n}(x_i-y_i)^2} \tag{14}$$

计算每一个场景下与其他场景下 MFCC 特征之间的欧几里得距离,然后计算平均欧几里得距离作为各个场景下的区分度指标,其公式如下:

$$\bar{d}=\frac{\sqrt{\sum_{i,j=1}^{k}(x_i-y_j)^2}}{n-1} \tag{15}$$

由皮尔逊相关系数和平均欧几里得距离定义适应度函数为:

$$J(\rho,\bar{d})=\max(-\rho\times\bar{d}) \tag{16}$$

对于需要遮掩的子频谱来说,$J(\rho,\bar{d})$ 值越大,则证明遮掩此频谱的伪随机信号加入后与原始数据相异性和区别度平衡性越好。

本文确定最优的遮掩子频谱范围的具体流程如图 3 所示。

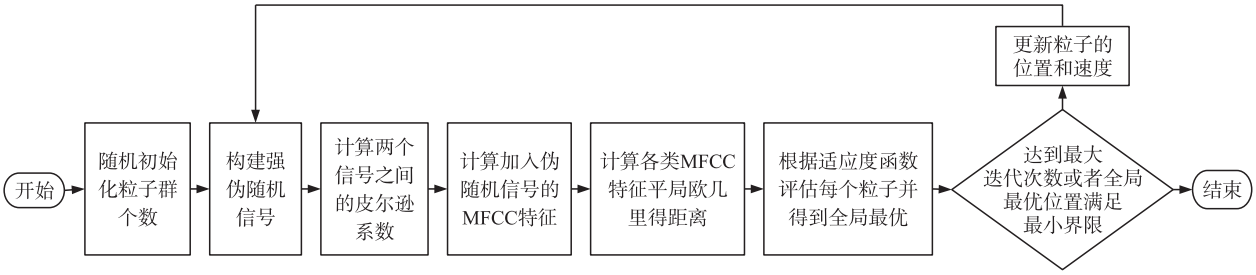

图 3　选择遮掩子频谱范围的流程图

3　实验结果与分析

3.1　数据预处理

本实验使用江苏省电力公司项目数据进行相关实验。实验数据采集的采样频率设置为 800 Hz,本数据库分别对 9 种不同电器使用情况进行电流电压数据的采集,采集的数据可总结为表 1。

表 1　数据库

用电器数	用电设备
单个	飞利浦台灯
	美的电风扇(制冷)
	小米空气净化器
两个	空气净化器+小米台灯
	美的风扇(冷)+小米台灯
	小米热水壶+小米电饭煲
三个	虎牌电热壶+美的电饭煲+美的电风扇(冷)
	虎牌电热壶+小米电饭煲+美的电风扇(冷)
	小米电饭煲+小米净化器+小米台灯

3.2　实验结果

本实验所设定的粒子群参数及寻优所得的需遮掩子频谱范围如表 2 所示。

表 2　粒子群算法实验

粒子种群个数	认知系数	社会学习系数	惯性权重	最大迭代次数	寻优结果
50	0.9	0.9	1	100	8.1 Hz~76.2 Hz

根据所选伪随机数,其各个场景下的数据信噪比如表 3 所示。

为了对比在常规噪声干扰下本方案的优势,所以本文实验了在常用噪声下的设备总识别率,另外以模型训练不加入任何扰动的非侵入式监测作为对抗手段验证各种噪声下的用户数据安全性,结果如表 4 所示。

由表 4 可知,传统添加伪随机噪声的方法与本文方案在模型对抗识别中基本处于同一量级,即安全性相当但是在模型预测识别率上本方案比传统方案的识别率高出 10%。这是由于本方案只采取了部分遮掩,通过可以泄露信息的未遮掩频段进行识别从而提高了设备识别率。

表 3　信噪比实验

用电器数	用电设备	噪声比
单个	飞利浦台灯	-7.23
	美的电风扇(制冷)	18.98
	小米空气净化器	12.60
两个	空气净化器+小米台灯	19.60
	美的风扇(冷)+小米台灯	13.16
	小米热水壶+小米电饭煲	46.25
三个	虎牌电热壶+美的电饭煲+美的电风扇(冷)	44.25
	虎牌电热壶+小米电饭煲+美的电风扇(冷)	43.53
	小米电饭煲+小米净化器+小米台灯	32.58

表 4　噪声对比实验

实验种类	模型预测识别率/%	模型对抗识别率/%
伪随机噪声	85.32	61.95
高斯噪声	88.20	55.15
混沌噪声	83.32	49.96
本文方案	98.61	69.95

对比本方案提出的有限安全环境下数据扰动方案和安全环境下 Paillier 同态加密下计算开销和数据安全性,其中计算开销以加解密时间和添加噪声时间为对比,安全性以皮尔逊系数和信息熵为对比,实验结果如表 5、表 6 和表 7 所示。

由表 5 可知本方案以未遮掩部分进行的特征提取与加密方案下得到的设备识别率基本一致,但是在计算时间上本方案远远优于加密方案。同时由表 6和表 7 可知,本文方案对比传统加解密方案,虽然在数据未加入和加入伪随机数的整体变化趋势上不如加密方案保护性强,但是在对遮掩部分的数据保护程度上与安全环境下的加密方案的安全性基本一致,达到部分信息保密的目的,即有限安全。

表 5　计算时间对比实验

实验类别	平均时间/s	识别率/%
同态加解密	9.08	98.9
本文方案	0.047	98.6

表 6 皮尔逊系数对比实验

用电器数	用电电气	同态加密	本文方案
单个	飞利浦台灯	0.063	0.204 0
	美的电风扇(制冷)	0.060	0.753 1
	小米空气净化器	0.061	0.733 6
两个	空气净化器+小米台灯	0.062	0.754 6
	美的风扇(冷)+小米台灯	0.064	0.736 7
	小米热水壶+小米电饭煲	0.061	0.799 8
三个	虎牌电热壶+美的电饭煲+美的电风扇(冷)	0.059	0.759 9
	虎牌电热壶+小米电饭煲+美的电风扇(冷)	0.069	0.759 9
	小米电饭煲+小米净化器+小米台灯	0.049	0.759 7

表 7 安全性对比实验

用电器数	用电电气	同态加密	本文方案
单个	飞利浦台灯	13.774	11.068
	美的电风扇(制冷)	17.543	15.184
	小米空气净化器	17.551	12.630
两个	空气净化器+小米台灯	17.547	15.300
	美的风扇(冷)+小米台灯	17.546	13.241
	小米热水壶+小米电饭煲	17.546	17.148
三个	虎牌电热壶+美的电饭煲+美的电风扇(冷)	17.543	17.262
	虎牌电热壶+小米电饭煲+美的电风扇(冷)	17.556	17.217
	小米电饭煲+小米净化器+小米台灯	17.547	16.270

4 结束语

本文考虑到有限安全下的非侵入式负荷识别数据保护,即对特定部分信息进行保护和允许保护外信息都可以泄露,以梅尔倒谱系数(Mel-scale Frequency Cepstral Coefficients,MFCC)作为负荷特征,从随机扰动技术出发,针对特定需要保护的电流数据的子频带构建伪随机信号与电流数据进行相加,以遮掩需要保护的电流数据子频带,使得数据敏感信息保护绕开数据加解密所需要的计算开销。另外,针对随机扰动技术会影响数据可用性问题,通过对数据未遮掩子频带进行 MFCC 特征提取,进行 SVM 的学习与识别来提升数据特征之间的区分度。实验结果表明,本方案在数据可用性情况下优于其他添加噪声方案,在对比加密方案实验下兼顾设备识别率和部分信息安全的同时大大节约了智能电表端的计算资源。

参考文献:

[1] 鲍海波,杨舒惠,陈子民,等. 事件检测类非侵入式负荷监测算法综述[J]. 电力系统自动化,2023,47(13):94-109.

[2] 陈子秋,冯瑞珏,郑扬富,等. 非侵入式负荷监测系统数据隐私保护方法研究[J]. 电子技术应用,2021,47(12):116-119,125.

[3] 蔡子伟. 智能电表数据扰动隐私保护方法研究[D]. 武汉:武汉大学,2019.

[4] 郝旭龙,刘明曦,董国芳. 基于同态加密的智能电网多维数据聚合方案[J]. 计算机工程与设计,2023,44(4):984-990.

[5] 王凌宇,傅宏,马创,等. 基于同态加密的电网隐私数据多维聚合优化算法[J]. 重庆邮电大学学报(自然科学版),2023,35(2):352-359.

[6] 徐淑华. 面向智能电网的隐私保护数据聚合方案研究[D]. 杭州:浙江工商大学,2022.

[7] 何胜梅. 面向智能电网 AMI 隐私保护方法的研究[D]. 保定:华北电力大学,2022.

[8] 朱聪聪. 基于抗泄漏同态加密的智能电网数据聚合协议研究[D]. 南京:南京邮电大学,2020.

[9] 周立国. 智能电网中隐私保护数据聚合方案研究[D]. 西安:西安电子科技大学,2020.

[10] 王以良,周鹏,叶卫,等. 基于金字塔网络的非侵入式负荷辨识及其隐私保护方案[J]. 计算机工程,2024,50(5):182-189.

[11] 田秀霞,王晓玲,高明,等. 数据库服务——安全与隐私保护[J]. 软件学报,2010,21(5):991-1006.

[12] Mclaughlin S,McDanial P,Aiello W. Protecting Consumer Privacy from Electric Load Monitoring[C]//18th ACM Conference on Computer & Communications Security,Chicago,IL,USA,ACM,2011:87-98.

[13] Kalogridis G, Efthymiou C, Denic S Z, et al. Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures[C]//2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, IEEE, 2010: 232-237.

[14] Liu Y H, Lee S H, Khisti A. Information-Theoretic Privacy in Smart Metering Systems Using Cascaded Rechargeable Batteries[J]. IEEE Signal Processing Letters, 2017, 24(3): 314-318.

[15] 王璐,孟小峰. 位置大数据隐私保护研究综述[J]. 软件学报,2014,25(4):693-712.

[16] Ács G, Castelluccia C. I Have a DREAM! (DiffeRentially privatE smArt Metering)[C]//3th Information Hiding Conference, Prague, Czech Republic, Springer, 2011: 118-132.

[17] Fang X, Misra S, Xue G, et al. Smart Grid: The New and Improved Power Grid: A Survey[J]. IEEE Communications Surveys&Tutorials, 2012, 14(4): 944-980.

[18] Lin H Y, Tzeng W G, Shen S T, et al. A Practical Smart Metering System Supporting Privacy Preserving Billing and Load Monitoring[C]//10th International Conference on Applied Cryptography and Network Security (ACNS'12), Singapore, 2012: 544-560.

[19] Vuković O, Dán G, Bobba R B. Confidentiality-Preserving Obfuscation for Cloud-Based Power System Contingency Analysis[C]//2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), Vancouver, BC, Canada, 2013: 432-437.

[20] 张毅,谢延义,罗元,等. 一种语音特征提取中 Mel 倒谱系数的后处理算法[J]. 智能系统学报,2016,11(2):208-215.

[21] 陆嘉歆. 基于深度学习的唤醒词识别效果比较研究[D]. 上海:上海师范大学,2021.

王森林(1999—),男,江苏仪征人,硕士研究生,主要研究方向:非侵入负荷监测技术下的隐私保护,1325225395@qq.com;

包永强(1973—),男,汉族,江苏江阴人,博士,教授,主要从事电力信号处理,音频取证等方面的研究,jybyq@163.com。