

# An Energy Theft Detection Scheme of Smart Grid

Ting Ma<sup>1,2,3</sup>, Nianrong Zhou<sup>1,2</sup>, Feng Gao<sup>1,2</sup>, Mengyin Ren<sup>3</sup>, Hong Wen<sup>3</sup>

<sup>1</sup>Yunnan Power Grid Corporation, Kunming

<sup>2</sup>Yunnan Yundian Tongfang Technology Co., Ltd, Kunming

<sup>3</sup>National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu  
Email: sunlike@uestc.edu.cn

Received: Nov. 5<sup>th</sup>, 2013; revised: Nov. 26<sup>th</sup>, 2013; accepted: Dec. 2<sup>nd</sup>, 2013

Copyright © 2013 Ting Ma et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. In accordance of the Creative Commons Attribution License all Copyrights © 2013 are reserved for Hans and the owner of the intellectual property Ting Ma et al. All Copyright © 2013 are guarded by law and by Hans as a guardian.

**Abstract:** The growing power theft has caused serious economic losses to our country with the development of smart grid. This paper proposes an energy theft detection scheme based on the existing research achievements, which improves the detection efficiency by line loss classification and power utilization abnormality detection.

**Keywords:** Smart Grid; Energy Theft Detection; Line Lose

## 一种智能电网窃电检测方案设计

马 婷<sup>1,2,3</sup>, 周年荣<sup>1,2</sup>, 高 峰<sup>1,2</sup>, 任梦吟<sup>3</sup>, 文 红<sup>3</sup>

<sup>1</sup>云南电网公司技术分公司, 昆明

<sup>2</sup>云南云电同方科技有限公司, 昆明

<sup>3</sup>电子科技大学通信抗干扰国家级重点实验室, 成都

Email: sunlike@uestc.edu.cn

收稿日期: 2013 年 11 月 5 日; 修回日期: 2013 年 11 月 26 日; 录用日期: 2013 年 12 月 2 日

**摘 要:** 随着智能电网的发展, 智能电网中的窃电行为屡禁不止, 对国家造成严重经济损失。文本在现有窃电检测研究成果的基础之上, 提出一种窃电检测方案。该方案通过线损分级过滤和用电异常过滤来提高检测效率, 为反窃电工作提供参考。

**关键词:** 智能电网; 窃电检测; 线损

### 1. 引言

随着智能电网的建设, 以智能电表为代表的先进计量设备在电网中大量应用, 实现了远程抄表、负载控制、双向数据通信等功能。然而智能电表的使用也带来了新的窃电风险, 例如, 远程抄表代替抄表员上门抄表使得电力部门对用户用电检查减少; 针对智能电表的高科技窃电技术层出不穷, 手段隐蔽且检测困难等。所以, 亟需建立有效的窃电检测方案。

目前已有很多关于窃电检测方法的研究, 例如, 文献[1,2]提出根据电力负荷管理系统进行数据异常分析来检测用电异常信息, 但检测精度不高; 文献[3]提出通过求解用户窃电因子来锁定窃电用户, 该方法检测精度高, 但计算量较大。

本文在一种隐私保护的分布式窃电检测算法的基础上, 结合台区窃电严重程度分级方法和用电异常检测来减少计算量, 设计窃电检测方案。

## 2. 一种分布式窃电检测算法<sup>[3]</sup>

文献[3]首次提出了一种用户隐私保护的分布式窃电检测算法，该算法通过建立线性系统方程组，通过分布式 LU 分解和 QR 分解求解用户窃电因子来判断用户是否有窃电行为。

### 2.1. 智能电网网络结构

图 1 所示为智能电网网络结构图。每个居民用户都安装了智能电表，每个计量集中器区域内的所有智能电表通过 NAN 网络与计量集中器连接。集中器对区域内智能电表进行实时监控、采集用电信息、记录用电异常等。更重要的是，集中器可以记录该区域用电量，只要估算出区域线损值，则集中器记录值与线损值之差就是区域内实际用电量。

### 2.2. 窃电检测线性方程组的建立

假设每个集中器都安装了一个智能电表可以监控在其服务区域内的总用电量，且每个用户都装有一个智能电表，电力公司可以随时获得用户实时电能消费情况。在一个 NAN 网络中有  $n$  个用户和一个集中器，共有  $n+1$  个电表。设电表读数的采样周期为  $SP$ ，在时刻  $t_i$ ，第  $j$  个电表的读数记为  $p_{t_i,j} (1 \leq j \leq n)$ ，而集中器电表值与区域线损之差为  $\overline{P}_{t_i}$ ，代表区域内实际用电量。

对每个用户定义大于零的窃电因子  $k_j (1 \leq j \leq n)$ ，则  $k_j \cdot p_{t_i,j}$  代表用户  $j$  在时间范围  $t_i - SP \sim t_i$  内的真实用电量，则 NAN 区域内  $n$  个用户用电总和等于集中器的用电量，则  $k_1 p_{t_i,1} + k_2 p_{t_i,2} + \dots + k_n p_{t_i,n} = \overline{P}_{t_i}$ 。对  $n$  个用户进行  $n$  次采样，选取  $n$  个不同的  $\overline{P}_{t_i}$  值，则可以得到  $n$  阶线性独立方程组：

$$\begin{cases} k_1 p_{t_{i,1}} + k_2 p_{t_{i,2}} + \dots + k_n p_{t_{i,n}} = \overline{P}_{t_i} \\ \dots \\ k_1 p_{t_{i,n,1}} + k_2 p_{t_{i,n,2}} + \dots + k_n p_{t_{i,n,n}} = \overline{P}_{t_{i,n}} \end{cases} \quad (1)$$

求解上述方程组可以求解出  $n$  个窃电因子：若  $k_j (1 \leq j \leq n) = 1$ ，则用户无窃电行为；若  $k_j (1 \leq j \leq n) > 1$ ，则为窃电用户；若  $k_j (1 \leq j \leq n) < 1$ ，则电表故障。

### 2.3. 线性方程组求解

文献[3]基于 LU 分解和 QR 分解提出了 LUD、

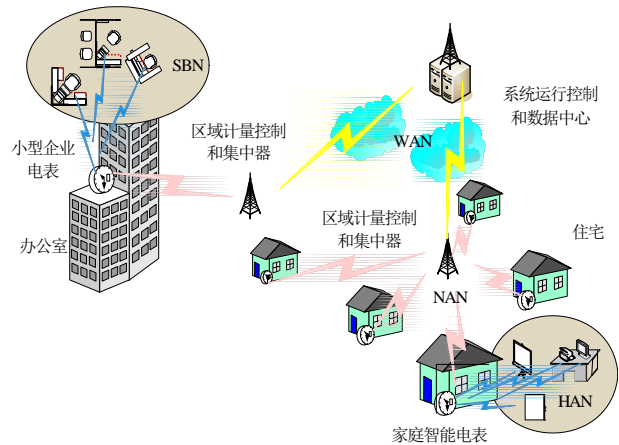


Figure1. Smart grid network  
图 1. 智能电网网络结构

LUPD 和 QRD 三种分布式求解算法，通过复杂度计算和仿真分析，其性能如下：

- (1) LUD 算法复杂度最低，在  $n \leq 25$  时解稳定；
- (2) LUPD 算法复杂度较高，在  $n \leq 300$  时解稳定；
- (3) QRD 算法复杂度最高，在  $n \leq 300$  时解稳定。

## 3. 一种台区窃电严重程度分级方法<sup>[4]</sup>

文献[4]提出了一种基于线损率标杆值的居民台区窃电严重程度分级方法，进而建立台区窃电严重程度的四级量化界定方案。该方案将居民台区窃电严重程度划分为四个等级：等级 I 为重度窃电台区；等级 II 为中度窃电台区；等级 III 为轻度窃电台区；等级 IV 为无窃电台区。通过等级划分，对重度和中度窃电台区进行重点稽查，可以提高反窃电效率。

## 4. 窃电检测方案设计

本文将文献[3]提出的中小型 NAN 网络窃电检测算法与文献[4]提出的居民台区窃电严重程度分级方案相结合，并通过用电异常过滤及区域线损过滤等筛选出重点检测用户，再根据目标用户数量选择 LUD 或 LUPD 算法锁定窃电用户。本文提出了两种窃电检测方案：方案一不进行用电异常过滤；方案二则增加了用电异常过滤。

### 4.1. 窃电检测方案一

图 2 所示为窃电检测方案一的流程图，其检测步骤如下：

第一步，对各个台区进行线损分级，III/IV 级台

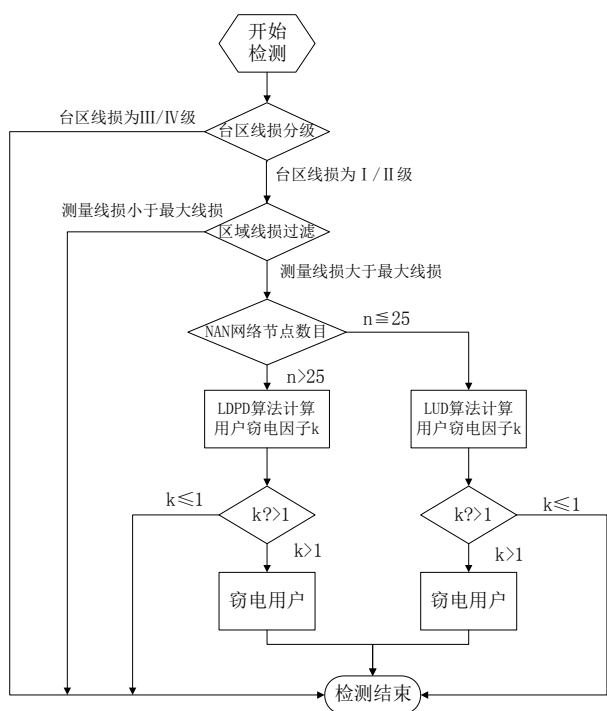


Figure 2. Energy theft detection scheme one  
图 2. 窃电检测方案一

区为轻度窃电和无窃电的台区，保持原有的用户举报制度，不对其进行特别稽查；I/II 级台区为重度和中度窃电的台区，对其进行下一步过滤。

第二步，对 I/II 级台区进行计量集中器区域线损过滤。计算和测量台区内每个集中器区域的线损值，当测量线损值大于计算最大线损值时，则认为该集中器区域存在窃电行为，对其进行下一步计算检测。

第三步，根据集中器区域 NAN 网络节点数选取相应的窃电检测算法，计算用户窃电因子，从而锁定窃电用户。

该方案通过台区线损分级过滤和集中器区域线损过滤将检测范围锁定到集中器区域，从而降低检测的计算量，但在集中器区域内没有对用户进行用电异常过滤。

#### 4.2. 窃电检测方案二

图 3 所示为窃电检测方案二流程图，它在方案一的基础之上增加区域用户用电异常过滤来进一步缩小检测范围，其检测步骤如下：

第一步与第二步同方案一。

第三步，在集中器区域内进行用户用电异常过滤<sup>[2,5]</sup>筛选出异常用户。

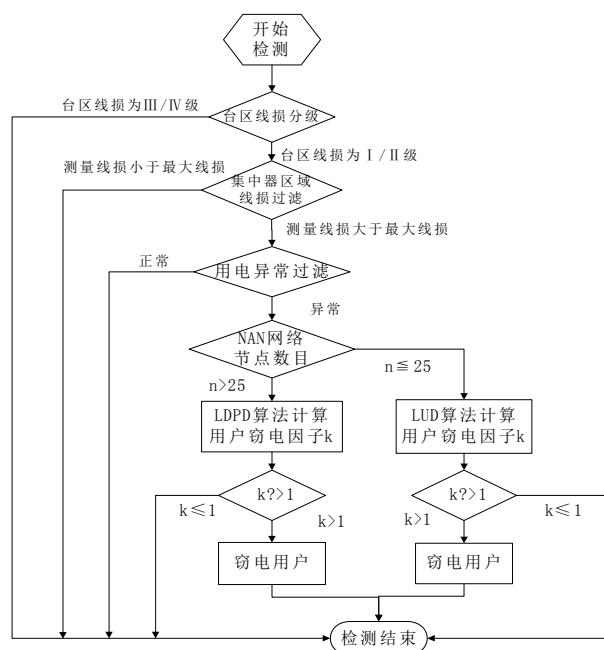


Figure 3. Energy theft detection scheme two  
图 3. 窃电检测方案二

第四步，根据 NAN 网络异常节点数目来选择相应的检测算法，计算用户窃电因子，从而锁定窃电用户。

方案二依赖于用电异常筛选技术的发展，该方案在 NAN 网络节点数目与用电异常检测之间寻求折中。目前主要通过电力负荷管理系统来筛选用电异常事件。反窃电相关异常主要包括：计量箱封印管理、电压缺相(表计/终端)、电表示度下降、需量手动清零、电压回路逆相序、电流反极性、CT 二次侧短路、差动异常<sup>[5]</sup>。此外，电力负荷管理系统还能自动筛选出可信度较高的用电异常事件，筛选原则为<sup>[2]</sup>：

- (1) 重要的用电异常事件报警，如缺相、断相、三相电流不平衡、电流反极性、电能表停走等；
- (2) 电量差率统计，即通过负荷管理终端计量的电量与电能表计量的电量进行比较，筛选出差率大于 5% (可自定义)或以上的用户；
- (3) 失压失流检查，即在自定义时段，筛选出某两相或单相电压(电流)数据为零且持续时间超过 12 h (可自定义)的用户。

#### 4.3. 检测方案分析

文献[4]提出的台区线损分级方案可以更合理地对待台区线损进行分级，其测试结果如下<sup>[4]</sup>：

台区类型	重度窃电	中度窃电	轻度或无窃电	重度和中度所占比例
站/箱变	6	785	408	66.2%
杆变	22	637	144	82.1%

可以看出,仅通过台区线损过滤就能在一定程度上减少文献[3]中算法的计算量,加上区域线损过滤及异常检测能更大程度地提高窃电检测的效率。

## 5. 结束语

本文将一种分布式窃电检测算法与台区窃电严重程度分级方法结合,并通过用电异常过滤设计出一种窃电检测方案。该方案可以逐步缩小窃电检测范围,提高检测效率。此外,更精准的线损计算方法和用电异常过滤手段,以及计算能力更强的智能电表可

以提升该方案的检测准确率和效率。

## 参考文献 (References)

- [1] 邵洪涛 (2010) 电力负荷管理数据分析辅助稽查系统. *科技信息*, **35**, 1136-1137.
- [2] 陈伟樑 (2011) 电力系统窃电特点及反窃电技术分析. *机电信息*, **21**, 228-229.
- [3] Salinas, S., Li, M. and Li, P. (2012) Privacy-preserving energy theft detection in smart grids. *9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Seoul, 18-21 June 2012, 605-613.
- [4] 王帅, 辛洁晴, 陆斌, 翟鸞鸽, 盛继卿 (2013) 基于线损率标杆值的居民台区窃电严重程度分级方法. *华东电力*, **4**, 816-821.
- [5] 黄亚芬 (2012) 用电信息采集系统(负控终端)在智能电网中的应用探讨. 浙江大学, 杭州.