

基于区块链技术的电力共享数据动态溯源方法

黄振¹, 王涛², 邵志敏¹, 徐亭亭²

(1. 国网山东省电力公司信息通信公司, 山东 济南 250001;

2. 国网山东省电力公司潍坊供电公司, 山东 潍坊 261021)

摘要:为提升电力共享数据动态溯源效果,提出一种基于区块链技术的电力共享数据动态溯源方法。结合电力共享数据存储分发机制特征,利用动态溯源策略,基于区块链技术对其共享数据进行优化。首先,建立电力共享数据状态评估模型,确定溯源数据初始状态;然后,对其区块链下电力共享数据状态指标进行定义,统一溯源变量;最后,完成区块链电力共享溯源数据存储结构判定,准确输出溯源结果。测试结果表明:所提方法能够提升溯源精准度与效率,具有一定应用价值。

关键词:区块链;共享数据存储;动态溯源

中图分类号:TP311.13 文献标识码:A 文章编号:1003-7241(2025)03-0110-05

Dynamic Traceability Method of Power Sharing Data Based on Blockchain Technology

HUANG Zhen¹, WANG Tao², SHAO Zhi-min¹, XU Ting-ting²

(1. Information and Communication Company, State Grid Shandong Electric Power Company, Jinan 250001 China;

2. Weifang Electric Power Supply Company, State Grid Shandong Electric Power Company, Weifang 261021 China)

Abstract: In order to improve the dynamic traceability effect of power sharing data, this paper proposes a dynamic traceability method of power sharing data based on blockchain technology. Combined with the characteristics of the power sharing data storage and distribution mechanism, the dynamic traceability strategy is used to optimize its shared data based on blockchain technology as follows. First, the power sharing data state evaluation model is established to determine the initial state of the traceability data. Then, it defines the status indicators of power sharing data under the blockchain, and unifies the traceability variables. Finally, completes the determination of the traceable data storage structure of blockchain power sharing, and accurately outputs the traceable results. The test results show that the proposed method can improve the accuracy and efficiency of traceability, and has certain application value.

Keywords: blockchain; shared data storage; dynamic traceability

0 引言

区块链技术的应用能够为电力共享数据的安全提供有效保障,为各单位在生产经营活动中构建高效、安全可靠的信息网络通道,促进信息共享及业务协同。在实际电力数据共享信息的溯源过程中,电力数据在收集、处理、传输中会涉及大量复杂且需要保密的关键要素,比如电网企业内部业务系统之间、电网企业与其他单位数据交换产生数据链。因此电力共享数据在不同链路空间内的流通,需要多节点同步信任,这就造成现有溯源方法在溯源精准度与溯源完整性方面出现偏差,例如姜赫等人研究了一种数据驱动的电力系统动态模型参数误差溯源方法。定义了扰动深度指标以及轨迹差异度指标,用以评价元件受扰程度和轨迹差异度,基于指标及其约束条

件,给出了主要致差区域的识别方法,以此完成数据溯源^[1];张晓华等人研究了一种交直流混联电网连锁故障特征事件智能溯源及预测方法。通过将电网运行状态量和故障信息作为输入特征量,结合物理机理分析和皮尔逊系数法提取关键特征量等方法完成溯源^[2];庞传军等人研究了一种基于 Shapley 值的电力负荷预测结果溯源分析方法。利用合作博弈论中的 Shapley 值计算各类负荷影响因素对负荷预测结果的影响,对利用梯度提升决策树算法训练的负荷预测模型的预测结果进行溯源分析^[3]。为解决以上问题,本文提出一种基于区块链技术的电力共享数据动态溯源方法。

1 基于区块链技术的溯源参量优化与定义

1.1 建立电力共享数据状态评估模型

为了更加准确地溯源电力共享数据,需要对共享数据信息节点进行状态评估,并以模型的方式系统化整合

*基金项目:国网山东省电力科技项目资助(2021A-108)

收稿日期:2023-09-22

共享数据分发信息,保证信息的完整性与一致性^[4]。利用高完整度、高统一度评估数据提升信息溯源速度与准确性。具体实现过程及其相关参量计算如下。

首先,根据电网分布共享数据状态,构建共享模型,以此为构建共享数据状态评估模型的基础模型,因此电网共享模型数据的准确性非常重要,其参量直接关系到数据共享时间参量与其相关联收发状态参数的评估语义设定,时间参量误差越小,对应评估所得共享信息状态的精准度越高^[5-6]。基于上述分析,假设电网共享模型内共享数据序列,当前时间点所对应第*i*个共享节点状态信息参量出现的频率为*p_{1i}*;电网共享模型内的共享数据序列,下一时间点所对应第*i*个共享节点状态信息参量出现的频率为*p_{2i}*,则电网共享模型内全局时间点对应的共享数据准确率*Q₁*计算公式为:

$$Q_1 = \frac{\sum_{i=1}^n p_{1i} * p_{2i}}{\sqrt{\sum_{i=1}^n p_{1i}^2 * p_{2i}^2}} \quad (1)$$

式中,*n*代表模型内部全局时间量下共享数据序列中,不同时间点所对应的共享信息总量。为了确保电网共享模型数据每一共享节点信息的完整性与有效性,需要对其节点进行空字段数据验证,确认所有信息无空字段后,将其共享模型中共享接收单元数据对应的序列设定为*O*,则电力共享模型的接收数据序列完整率*Q₂*计算公式为:

$$Q_2 = \frac{\sum_{j=1}^n o(j)}{n} \quad (2)$$

式中,*j*代表共享模型接收部分的节点字段。基于式(2)所示的数据序列完整性计算公式,若共享数据序列中包含特征字段*O(j)=0^[7]*,则*j*属性字段可以判断为共享空字段,对应共享数据模型的完整性存在缺失,反之,共享数据模型对应序列满足完整性指标。进而可以对其数据序列构成节点信息进行归一初始优化。根据共享数据序列构成特征,将数据格式遵循第*k*中格式参量配置状态定义为*b_k*,且*k=1,2,⋯,m*,其中,*m*代表数据序列中任意一个共享节点信息配置指标变化系数,则电力共享模型中所有数据序列初始化指标率*Q₃*的计算公式为:

$$Q_3 = \frac{\sum_{k=1}^m b_k}{m} \quad (3)$$

将上述三个公式联立计算,即可得到电力共享数据状态评估模型。

1.2 区块链下电力共享数据状态指标定义

考虑到不同共享区块下的共享信息贡献程度各不相同,因此为了更好、更准确地表示每一区块上共享信息贡献程度,可以从能量的角度入手,将不同区块上的电力共

享节点贡献值转化为节点能量,以此实现状态指标的统一。

对于电力共享数据节点所对应的有功功率数据集,其共享样本协方差计算,可以通过矩阵构建来完成*N*个数据样本指标的整体计算,表达式为:

$$\eta_i = DCI_i = \frac{E(C_i)}{E(C_{sys})} \times 100\% \quad (4)$$

对于共享数据节点个体维数为*n × m*的矩阵*Z*,其个体共享节点在任意区块下的能量由Frobenius范数^[8]表示:

$$\eta_i = DCI_m = \frac{E(C_n)}{E(C_{sys})} \times 100\% \quad (5)$$

因此*C_{sys}*范数可作为模型整体共享节点共同贡献的能量总值,*n*代表任意区块链路空间下的节点数量,*m*代表数据时间序列的总数,同样的对于第*i*个区块链路空间下的电力共享信息能量贡献协方差矩阵可以表示为:

$$\eta_i = DCI_m = \frac{E(C_n)}{E(C_{sys})} \times 100\% \quad (6)$$

通过式(5)的Frobenius范数,可以求取*i*个区块链路空间下的电力共享信息能量贡献强度,表达式为:

$$\eta_{wAMS} = DCI_m = \frac{E(C_i)}{E(C_{sys})} \times 100\% \quad (7)$$

考虑到能量贡献深度值隶属于MSE(均方根)^[9-10],在整个能量转化表达过程中是唯一定值,因此存在部分维度的局限性。

为了避免局限性对后续溯源效果的影响,采用动态指标函数进行输出变量优化,并以百分比方式表示。全局动态指标函数可以表示为:

$$\xi = GDI(t) = \frac{\int_0^t \Delta z(\tau)^T R \Delta z(\tau) d\tau}{\int_0^t S_{ref}^2 d\tau} \times 100\% \quad (8)$$

式中, $\Delta z = [\Delta P \ \Delta Q]$; *R*代表权重矩阵;*S_{ref}*代表动态指标函数参考系数。 ξ 代表不同共享数据之间的二次差异值所对应的累积效应。

1.3 区块链电力共享溯源数据存储结构

在完成电力共享数据溯源信息指标定义后,根据不同区块空间下的数据存储结构,对其信息存储状态进行溯源分析,根据QTPB数据处理模型^[11],对不同区块链路空间下存储的共享数据进行溯源范围划分。利用跟踪识别技术对初始共享数据存储区块位置进行标定,同时,将共享溯源数据特征索引存储到对应特征区块链上,通过对模型的反复训练^[12],得到电力共享数据变化特征,结合哈希处理共享数据变化特征存储范围,计算得到不同区块链路空间下存储的电力共享数据实际变化哈希系数,计算公式如下:

$$\bar{R} = \omega - \sqrt{3N + \frac{1.3+1}{V}} \quad (9)$$

式中： \bar{R} 代表存储在不同链路空间层中的电力共享数据信息的实际变化哈希系数， ω 代表电力共享数据节点的溯源索引范围， N 代表溯源时间， V 代表置换系数。

利用对不同链路空间下电力共享信息特征的感知能力，对均值哈希系数对应节点进行溯源分析，根据相同空间分布变量下链路中共享信息节点存储强度与缩放比例存在的差异大小，实现对其电力共享信息的识别。在此过程中，需要将区块链空间存储信息分割成网格状，以网格为单位逐一分析，每一区块网格下的信息溯源特征计算为：

$$T(X, Y) = \sum_{t=0}^{m-1} (r_t - r_o) \quad (10)$$

式中： (X, Y) 代表存在差异特征的电力共享数据存储位置的区域坐标； r_t 代表该区域范围内第 t 个数据溯源特征系数； m 代表整个区块链划分的网络数量。式(10)计算所得为电力共享数据在一个链路空间网格下的中心点 o 与相邻网格区块链下的共享信息差异对比过程，所得对比结果为电力共享信息的特征系数数量，将其标记为 T 。根据每一网络区块链对比后的最终结果，对其进行特征系数数量 T 的二次处理，依据设定的溯源指标，对其对应存储区域进行特征划分，通过重新定义目标层级标准与极限标准，准确获得数据最终的溯源存储结构函数：

$$L = \frac{a + 2\sqrt{5}}{C} - 1 + 5\theta \quad (11)$$

式中： L 代表电力共享数据在区块链空间下的溯源目标节点核心系数； a 代表哈希异常比； C 代表溯源系数对应的定位距离； θ 代表差异特征最小系数。

至此，通过计算可以获得电力共享数据的溯源目标节点的核心位置，并通过对其差异特征距离的分析，提升溯源结果精准性、稳定性及可靠性。

2 应用测试

通过数据指标对比的方式，对其溯源方法进行可行性验证。对比过程中设置文献[1]、文献[2]方法作为差异化对比方法，分别记作溯源对比A与溯源对比B；提出方法记作溯源目标C，对比相同电力共享样本下不同溯源方法的溯源效果。

2.1 测试数据配置

设定150组电力共享数据作为测试样本，通过云端处理技术，对测试样本外围扰动数据进行清理，清理后的样本数据分发存储于测试空间，阻断第三方管理对样本数据的管理扰动。按照样本数据特征，将其共享信息、本源数据、溯源索引特征信息分别存储在不同的维度层级中。需要注意的是，不同存储层之间的交互为独立交互，数据流转方向为单向传输，因此不存在存储层级数据相

互扰动因素。

2.2 溯源特征识别率测试

在设定的150样本数据中，随机抽取50组不同共享特征信息的数据作为该测试样本，分别用对比溯源A、对比溯源B与溯源目标C三种不同方法对其进行共享溯源特征识别，测试结果如图1所示。

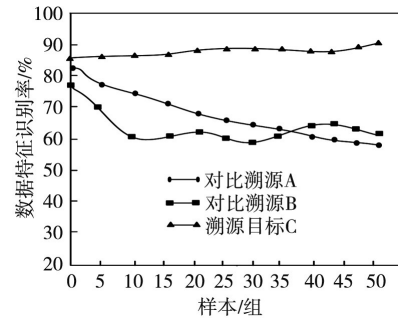


图1 不同溯源方法的电力共享数据溯源特征识别曲线

观察图1中3条曲线可以发现，对比溯源A对应曲线初始电力共享样本数据特征的识别率为83.6%，识别初始值位居第二，随着识别样本数量的增加，整体走势呈下降趋势，过程中没有较大波动，每一区域下的共享数据特征识别数值过渡较为平滑，最终收官识别率为58.9%。对比初始值与收官数值差值较大，可以判断对比溯源A在特征判断与识别指标上存在局部缺陷；对比分析位于其下部的对比溯源B曲线，初始识别率偏低，仅为76.5%，与对比溯源A整体趋势相同，但下降过程中出现多次波动，波动频率周期为3，符合线性特征，根据其波动位置的识别数值及其初始识别率与收官识别率差值分析，对比溯源B溯源特征识别率偏低，识别效果并不理想；对比分析溯源目标C曲线，初始识别率为87.3%，曲线呈上升趋势，其过程较为平缓，出现共享特征差异下的识别起伏，收官识别率为91.3%，初始特征识别率与收官特征识别率差值最小。

综上所述可以判定，溯源目标C的溯源特征识别效果最佳，各项溯源特征识别指标更贴近实际指标要求，故此，溯源目标C通过该指标性能测试。

2.3 溯源处理时间测试

将150组电力共享数据划分为15个测试包，每个测试包中包含30组电力共享数据，随机顺序释放测试包到测试存储空间，保证每个存储层中的数据溯源特征总量相同。对比溯源A、对比溯源B与溯源目标C三种不同方法逐一完成样本溯源操作，以溯源结果 $\geq 85\%$ 时所用时间为记录时间，经过统计后得到表1，对比分析数据得出测试结论。

纵向分析表1数据可以发现，3种溯源方法的15组测试包溯源处理时间相对稳定，说明对比溯源A、对比溯源B与溯源目标C均具备海量数据溯源处理能力；横向对比数据发现，3种溯源方法按照溯源时间由大到小的顺序排

列为:对比溯源B>对比溯源A>溯源目标C;则其溯源性能最佳的方法为溯源目标C。

表1 溯源处理时间测试结果统计

测试组	对比溯源A溯源处理时间/s	对比溯源B溯源处理时间/s	溯源目标C溯源处理时间/s
1	15.6	17.5	6.4
2	16.5	18.2	6.5
3	15.8	17.5	6.5
4	15.3	18.6	6.5
5	17.6	18.6	6.4
6	15.4	17.2	6.3
7	15.2	17.6	6.2
8	16.4	17.2	6.2
9	14.3	17.2	6.3
10	15.2	18.2	6.2
11	15.4	18.4	6.5
12	17.6	15.6	6.8
13	15.4	17.4	6.5
14	15.2	16.8	6.7
15	16.4	16.6	6.4

2.4 溯源完整度测试

分别对溯源样本的共享信息、本源数据、溯源索引特征信息进行溯源完整度测试,测试结果分别如图2—图4所示。

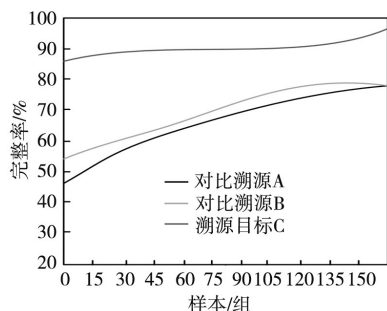


图2 共享信息溯源完整度测试结果

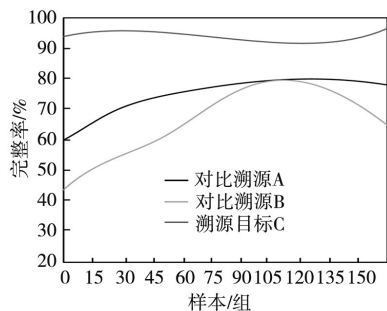


图3 本源数据溯源完整度测试结果

对图2中结果观察可知,对比溯源A所得样本共享信息的溯源完整度整体偏低,最大峰值为68.7%;对比溯源B略好于对比溯源A,但是整体增幅不大,最大峰值为73.6%;溯源目标C的完整度最高,虽然过程中出现小范围下滑,但是整体完整度值域控制较好,最大峰值为94.6%,由此可以判定溯源目标C在电力共享数据信息溯源性能方面

的表现,满足相关测试标准及要求。

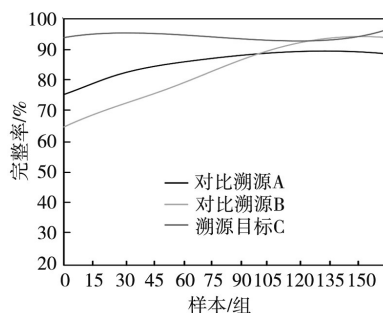


图4 溯源索引特征信息溯源完整度测试结果

通过对比图3中所示3种不同溯源方法所得溯源样本本源数据溯源完整度曲线可知,对比溯源A初始值较好,溯源过程较为平稳,且呈上升趋势,但整体溯源能力较为薄弱,后期溯源完整度略有下滑,最终数据本源溯源完整度为68.9%;对比溯源B初始效果较差,中期整体呈快速上升趋势,但稳定控制效果不佳,第110组样本时,出现溯源完整度数值下滑,最终溯源完整度为56.7%;溯源目标C整体变化与图3特征基本保持一致,故此,在数据本源完整度溯源测试中,溯源目标C仍是最佳溯源方法。

基于上述对比方法分析图4曲线,得到溯源索引数据的最佳溯源方法仍为溯源目标C,综合图3、图4测试结果,可以得到全局完整度溯源测试的最佳溯源方法为溯源目标C,由此可以证明设计方法的有效性。

3 结束语

根据电力共享数据存储特征,结合区块链空间结构,对其数据节点进行共享区块溯源优化,并取得了提升溯源精准度与整体溯源效率的效果。为区块链溯源多场景应用与研究,开辟了一条全新的设计思路。但是,随着区块链技术的不断发展,区块空间之间的联系变量会发生本质变化,对提出方法的溯源映射结构来说,存在局部结构变量与映射链路扰动因素,且隐蔽性较强。为了后期应用的稳定,可以尝试引入AI技术,对其结构进行空间变量的自我分析与自我学习,以此保证溯源参量的准确,方法时刻处于最佳状态。

参考文献:

- [1] 姜赫,安军,刘征帆,等.数据驱动的电力系统动态模型参数误差溯源方法[J].电测与仪表,2022,59(11):63-70.
- [2] 张晓华,徐伟,吴峰,等.交直流混联电网连锁故障特征事件智能溯源及预测方法[J].电力系统自动化,2021,45(10):17-24.
- [3] 庞传军,刘金波,张波,等.基于Shapley值的电力负荷预测结果溯源分析方法[J].电力自动化设备,2021(12):200-205.
- [4] 王晓庆,孙战伟,吴军红,等.基于数据要素流通视角的数据溯源研究进展[J].数据分析与知识发现,2022,6(1):43-54.
- [5] 杨斐斐,沈思好,申德荣,等.面向数据融合的多粒度数据溯

源方法[J]. 计算机科学, 2022, 49(5): 120-128.

[6] 刘炜, 张聪, 余维, 等. 基于Merkle山脉的数据可信溯源方法[J]. 计算机应用, 2022, 42(9): 2765-2771.

[7] 李孝冲, 敬伟, 王鹏, 等. 基于EEMD和BPNN的动态误差溯源研究[J]. 电子测量技术, 2021, 44(22): 69-74.

[8] 张学旺, 冯家琦, 殷梓杰, 等. 基于区块链的数据溯源可信查询方法[J]. 应用科学学报, 2021, 39(1): 42-54.

[9] 卢成伟, 吴铖洋, 钱博增, 等. 数控机床机电-刚柔耦合特性分析下的进给系统动态运动误差溯源方法[J]. 机械科学与技术, 2022, 41(10): 1577-1584.

[10] 王振乾, 朱珠, 任江华. 基于泛在电力物联网的电力运维平

台设计与实现[J]. 自动化技术与应用, 2022, 41(8): 76-79, 139.

[11] 刘涛, 李英俊, 邢峰, 等. 基于多变量自动回归的电力大数据异常值检测平台设计[J]. 自动化技术与应用, 2022, 41(10): 93-96.

[12] 姜赫, 安军, 刘征帆, 等. 数据驱动的电力系统动态模型参数误差溯源方法[J]. 电测与仪表, 2022, 59(11): 63-70.

作者简介: 黄振(1990-), 男, 硕士, 工程师, 研究方向: 电力信息通信、区块链应用、数据管理等。

(上接第95页)

仿真实验模拟了终端数量不同时本文SPA协议的运行时间(单包授权和安全接入), 具体如图6所示。为了对比分析, 分别采用FWKNOP协议、OPENSPA协议与本文所提方法进行对比, FWKNOP协议和OPENSPA协议的运行结果也展示在图6中, 对比图6中的三条曲线可以看出, 运行时间均随着终端数量的增大而增大, 而SPA协议的运行时间明显小于其他两种协议, 当终端数量达到20 000时, SPA协议的运行时间仅为FWKNOP协议和OPENSPA协议的71.43%和43.48%, 运行时间缩短明显, 由此可见, 本文采用的SPA协议更适合PIoT。

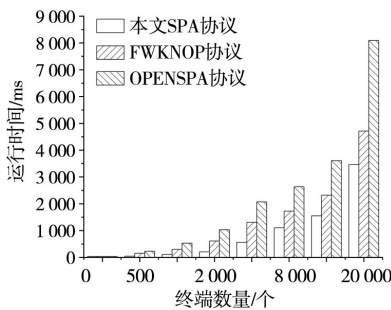


图6 三种协议测试对比

表2 资源消耗量对比

协议	SPA	FWKNOP	OPENSPA
资源消耗量/B	358	450	2 460

表2给出了三种协议在抓包分析过程中的资源消耗量, 由图3可知, SPA协议、FWKNOP协议和OPENSPA协议的资源消耗量分别为358 B、450 B和2 460 B, 显然SPA协议在抓包分析过程中的资源消耗量最少, FWKNOP协议虽然与SPA协议的消耗量相差不大, 但FWKNOP协议采用的是标准SHA和RSA算法, 安全性和快捷性不如SPA协议, 因为SPA协议采用的SM9算法进行加密签名, 既提高了安全性又能提升PIoT的通信效率。

4 结束语

本文在零信任机制的基础上, 将数据平面和控制平

面分离, 采用单包授权方式进行PIoT安全认证, 并在终端和业务之间进行双向加密, 提出了一种基于软件定义边界技术的PIoT安全防护方法。采用模拟终端和网关服务器进行仿真验证, 结果表明, 本文所提PIoT安全防护方法在终端处理时间和资源消耗量方面均优于其他方法, 验证了基于软件定义边界技术的PIoT安全防护方法的正确性和优越性。

参考文献:

[1] 景卫哲, 刘泽辉, 马东娟, 郭昱. 一种面向新型电力系统物联网信息传输安全的可靠密钥生成方法[J]. 山西电力, 2022(5): 68-72.

[2] 戴志辉, 杨鑫, 耿宏贤, 刘悦, 杨辉, 杨雨熹. 基于电力物联网的继电保护定值智能运维系统研究[J]. 电力系统及其自动化学报, 2023, 35(6): 50-58.

[3] KIMANI K, ODUOL V, LANGAT K. Cyber Security Challenges for IoT-based Smart Grid Networks[J]. International Journal of Critical Infrastructure Protection, 2019, 25(6): 36-49.

[4] 吴克河, 程瑞, 郑碧煌, 等. 电力物联网安全通信协议研究[J]. 信息安全, 2021, 21(9): 8-15.

[5] 马靖, 许勇刚, 增明, 等. 基于零信任框架的泛在电力物联网安全防护研究[J]. 网络安全技术与应用, 2020(1): 117-119.

[6] 花泉. 基于零信任机制的数据安全分层保护模式设计与应用[J]. 广播电视网络, 2022, 29(6): 96-98, 106.

[7] 于欣越, 孙刚, 张亚伟. 基于零信任的软件定义边界网络隐身技术研究[J]. 通信技术, 2021, 54(5): 1229-1234.

[8] 胡呈梅. 基于区块链技术的铁路项目档案管理信息系统设计[J]. 自动化技术与应用, 2023, 42(2): 114-116, 125.

[9] 汤煜, 翁秀玲, 王云峰. SHA-256哈希运算单元的硬件优化实现[J]. 中国集成电路, 2016, 25(5): 26-31.

作者简介: 阎峻(1985-), 男, 硕士, 高级工程师, 研究方向: 电力信息化、电力通信。