

基于量子加密算法的电力物联网网关数据安全采集方法

张静鑫, 陈 超, 张 平

(安徽明生恒卓科技有限公司, 安徽 合肥 230039)

摘 要: 为了实现电力物联网网关数据安全、高效率采集, 提出基于量子加密算法的电力物联网网关数据安全采集方法。通过分析电力物联网体系架构, 明确电力物联网网关数据的生成逻辑; 基于特定架构层次, 提取网关数据属性特征向量; 基于量子加密算法, 通过特征向量选择二维 Henon 混沌映射方式获取原始量子密钥; 对不同量子态下的原始密钥进行编码处理, 输出具有安全密钥信息的比特序列; 基于输出安全密钥进行加解密、用户验证操作、同步二次加密与数据采集指令执行, 在数据传输与通信过程中实现电力物联网网关数据的安全采集。实验结果表明, 设计方法有效处理JSON、XML、Protobuf等多种格式的网关数据, 整体数据加密时间较短, 均未超过 180 ms。数据平均丢包率在 0.07~0.14 之间浮动、平均吞吐量最高值达到 8.2×10^3 , 具有较高的数据采集安全性与采集效率。

关键词: 量子加密; 电力物联网; 网关数据; 安全采集

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2025022

Secure Data Collection Method Based on Quantum Encryption Algorithm for Power IoT Gateway

ZHANG Jingxin, CHEN Chao, ZHANG Ping

Anhui Mingsheng Hengzhuo Technology Co., Ltd., Hefei 230039, China

Abstract: In order to realize the secure and high-efficiency collection of electric power IoT gateway data, the secure collection method of electric power IoT gateway data based on quantum encryption algorithm is proposed. By analyzing the architecture of electric power IoT, the generation logic of electric power IoT gateway data is clarified. Based on the specific architectural level, the attribute feature vector of the gateway data is extracted. Based on the quantum encryption algorithm, the original quantum key is obtained by selecting the two-dimensional Henon chaotic mapping method through the feature vector. The original keys in different quantum states are encoded and processed to output the bit sequences with the information of security key. Based on the output security key, encryption, decryption, user authentication operation, synchronized secondary encryption and data acquisition instruction execution are carried out to realize the secure data acquisition of electric power IoT gateway data in the process of data transmission and communication. The experimental results show that the designed method can effectively handle gateway data in various formats such as JSON, XML, Protobuf, etc. The overall data encryption time is short, not exceeding 180 ms. The average packet loss rate of the data fluctuates from 0.07 to 0.14, and the highest average throughput value reaches 8.2×10^3 , which provides high data collection security and collection efficiency.

Keywords: Quantum encryption, power IoT, gateway data, secure collection

0 引言

电力物联网网关作为连接和管理各种传感器和终端设备的核心组件, 通过集成嵌入式系统、智能传感器、

智能控制与大数据分析处理等技术^[1-3], 连接电力物联网感知层与网络层, 实时采集电网设备的运行状态、电量质量、环境信息等数据。同时, 通过对原始数据进行预处理、筛选、分类和聚合, 有效实现了电力设备间的数

据传输和通信,支撑物联网体系中上层应用的稳定运行。由此可知,电力物联网网关数据采集与传输逐渐成为当前电力研究领域的重要发展课题。

招景明等^[4]专注于边缘计算模型在数据处理与分析中的优势,提出新型系统架构与任务调度策略,构建了一个云边端协同的电力数据采集系统,通过实例验证该系统能有效实现实时处理、隐私保护、能耗优化,并减轻数据通信带宽压力。尽管研究提出的方案旨在解决实时处理和响应问题,但在处理实时性与隐私保护之间的平衡时可能面临挑战。特别是在涉及敏感数据的场景下,如何确保数据的实时处理同时保证数据的隐私安全是一个需要重点关注的问题。唐秋杭等^[5]提出了一种基于载波通信的电力终端数据采集检测技术,通过改进硬件设计、增加电力载波模块以及结合缩位算法进行数据校验,有效提升了电力数据采集的成功率和准确性,实现了对不同厂商载波通信模块通信能力的有效检测。赵睿林等^[6]提出一种基于MQTT协议的电力物联网网关数据采集算法,通过联合云平台与数据传输协议,优化网关数据通信性能,有效实现智能电力网关数据的实时采集与分析,但该方法在数据采集过程中,缺乏身份认证环节,存在一定的安全性风险。赵丙镇等^[7]基于区块链,提出一种电力物联网信任网关设计与数据采集方法。基于区块链的共识机制,构建分布式的动态网关结构,有效实现主网关设计与网关数据的采集,但在数据采集与主网关设计过程中,过度侧重网关安全性分析,数据采集效率有待提升。

在电力物联网中,网关作为数据采集的枢纽,承担着与各种传感器、设备建立连接、读取数据、处理数据并传输到服务器或云平台的重要任务。然而,在数据采集和传输过程中,数据的安全性是首要考虑的问题。量子加密技术基于量子力学的不确定性原理和不可克隆定理,能够实现密钥的安全分发和信息的可靠传输^[8-10]。在电力物联网领域,量子加密技术的应用将极大提升数据安全采集的可靠性,有效防御黑客攻击和窃听,保护电力系统的信息安全。因此,提出基于量子加密算法的电力物联网网关数据安全采集方法。通过结合量子加密技术和电力物联网网关技术,构建一种高效、安全的数据采集系统,实现对电力物联网数据的实时、可靠、安全的采集和传输。这不仅能够提升电力系统的稳定性和可靠性,还能够为电力系统的智能化、自动化运行管理提供强有力的支撑手段。

1 电力物联网网关数据安全采集

1.1 电力物联网体系架构分析

电力物联网网关作为连接感知层和网络层的重要枢纽,其利用电力线载波通信、无线通信等技术连接智能电表、智能断路器等电力物联网终端,实现电力物联网数据的采集、传输与通信。

而为了提升电网的智能化水平和管理效率,电力物联网网关基于多种通信协议和通信传输标准,实现协议转换功能,支持不同设备之间的协议转换和标准化,实现电网设备的互联互通和智能交互^[11-13]。同时,网关通过多接口与多个子网络对接,根据实际需求配置多个同制式的网关接口单元,基于单体制交互与异构体制交互等通信工作模式,对电网设备进行远程控制与协同管理,在实现设备间数据采集、通信的过程中,有效降低运维成本与人力投入。电力物联网体系架构如图1所示。

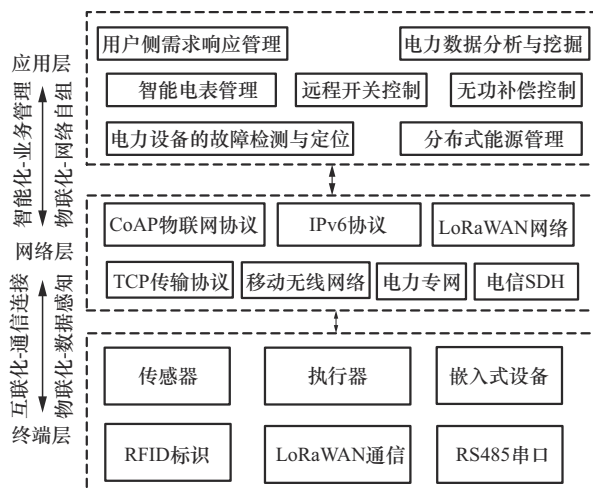


图1 电力物联网体系架构

由图1可知,电力物联网体系架构主要由应用层、网络层、终端层等层次构成。其中,电力物联网网关主要存在于网络层与终端层连接端口处。在网关执行过程中,网关需要从终端层收集各种电力设备传感数据,包括电力设备的状态数据、实时数据等,在进行数据清洗、格式转换和异常值处理等操作后,通过网关网络传输协议将采集数据传输至网络层,进而实现应用层的电力物联网的业务功能。由此可知,电力物联网网关,主要是将终端设备与上层系统连接起来,基于数据采集、传输、处理和等功能,完成数据应用指令。

网关应用原理主要为由待接入设备(终端层)向区域网关发送申请命令,传输电力设备端口型号、ID与运

行服务状态。在接收申请命令后，由局域网将包含传感设备的命令传输至主网关，基于公式算法进行设备身份信息验证，实现网关接入认证与安全通信。

1.2 数据属性特征向量提取

电力网终端层设备的多样性（包括传感器类型、接口类型、信息速率和信息格式等）直接导致了数据采集过程中的复杂性。数据属性特征向量提取作为一种有效的数据处理手段，可以很好地应对这种复杂性。通过提取数据的关键特征并构建特征向量，可以消除不同设备之间的差异，使得采集到的数据能够以一种统一、标准化的形式进行后续处理和分析。

提升树算法（集成学习算法）通过逐步拟合残差来构建决策树，能够很好地捕捉数据中的复杂模式和非线性关系，从而适应不同类型的电力物联网数据。因此，本文基于梯度提升树算法（集成学习算法），通过迭代地构建一系列回归树，判断树结构中树节点的特征相关性^[14-16]。

假定终端层需采集数据的回归树函数为 $F(A)$ ，则电力物联网网关终端层数据特征可表示为

$$F(A) = f(A) \left[F_1 \left(f' \sqrt{A_z} - \frac{N}{A_z} \right) \right] \quad (1)$$

$$A_z = F(A) + \left(f' \sqrt{A_z} - \frac{N}{A_z} \right)^{z'} \quad (2)$$

式中， $f(\cdot)$ 表示决策树预测损失函数； F_1 表示 $f(\cdot)$ 的负梯度； f' 表示回归树叶节点得分计算参量； A_z 表示终端层待采集数据的回归树结构，且 $A_z = [1, 2, 3, \dots, N']$ ； z 表示树叶节点； N 表示 z 的总量。

由式(1)的运算原理可知，在根据特征参数排序执行迭代操作的过程中，当 A_z 计算为固定数值，且满足 F_1 （基于多次迭代预测后新回归树的目标值）时，可以用 f' 值评价回归树结构中叶节点所代表的特征节点是否具有相关性。当 $f' > F_1$ 时，判断回归树结构中的 z 为相关特征节点 z' ，若 $f' \leq F_1$ 时，判断叶节点 z 为不相关特征节点，需要消除该特征参数。

利用自编码器中的编、解码模块对输出的 z' （包含需要采集的终端层电力物联网网关数据特征信息）进行数据降维处理，提取采集电力物联网网关数据特征向量，滤除终端层需要采集数据的冗余信息。编解码过程可以表示为

$$z'_B = \hat{f}(z') + \sum_{b=1}^2 z'_0 \left(\varpi_{z'} + \frac{1}{\rho} \right)^b \quad (3)$$

$$z'_D = \hat{f}(z') + \sum_{b=1}^2 \sqrt[b]{z'_0 - z'_B} \left(\varpi_{z'} + \frac{1}{\rho} \right)^{b-1} \quad (4)$$

式中， z'_B 表示编码模块处理后的低维数据特征向量； $\hat{f}(\cdot)$ 表示ReLU激活函数； b 表示输出数据的重构误差； z'_0 表示待输入数据编码向量； $\varpi_{z'}$ 表示自编码器映射低维隐藏空间的权重系数； ρ 表示自编码器映射低维隐藏空间的偏置系数； z'_D 表示解码模块处理后的低维数据特征向量。

将训练数据输入自编码器中，通过编码器和解码器得到重构数据 z'_D 。设置 z'_D 的属性特征均值为0（特征向量收敛方差值均处于同一阶级），对 z'_D 中的属性特征进行规范化处理

$$z' = \frac{z'_D - \tilde{z}_{\min}}{\tilde{z}_{\max} - \tilde{z}_{\min}} \quad (5)$$

式中， z' 表示属性规范化处理后的数据特征向量； $\tilde{z}_{\max}$ 表示数据特征最大取值； $\tilde{z}_{\min}$ 表示数据特征最小取值。

为了最小化输出数据与原始输入数据之间的差异。使用均方误差（Mean Squared Error, MSE）作为自编码器的损失函数，其形式如下

$$\delta = \frac{(z'_D - z')^2}{N} \quad (6)$$

式中， N 是数据样本的数量。

然后，使用反向传播算法计算损失函数关于网络参数的梯度，并将梯度传播回网络中的每一层。在此基础上，使用梯度下降法更新自编码器的权重系数和偏置系数。重复执行前向传播、反向传播和参数更新，直到达到预设的训练轮次或损失函数收敛到一定的精度。

基于此，输出 z' ，有效滤除冗余数据，避免数据属性特征的覆盖情况。

1.3 基于量子加密算法的数据安全采集与通信设计

为了实现电力物联网网关数据安全采集，本文基于量子加密算法，通过生成与分配量子密钥，对网关数据进行加解密，并基于用户验证操作，提取需要进行二次加密的网关数据，以此在数据传输与通信过程中实现电力物联网网关数据的安全采集。

考虑到 z' 在不同维度之间存在一定相关性，并且所代表的数在传输时具有实时性和带宽要求。因此，利用二维Henon混沌映射对 z' 进行非线性映射，生成具有高度随机性和复杂性的序列^[17-19]，确保生成密钥的安全性。同时，针对网关数据的采集和安全传输，利用二维Henon

混沌映射可以提升对初始条件的微小变化敏感性。即使在初始条件偏移的情况下,生成的随机序列也能够满足数据采集与实时传输的安全性平衡性(带宽消耗)。 $\mathbf{z}'$ 的混沌映射状态可表示为

$$x_{z'} = c_1 x_{z'+1} + \frac{c_3 - 1}{2c_2 x_{z'-1}} \quad (7)$$

$$y_{z'} = c_1 y_{z'+1} + \frac{c_3 - 1}{2c_2 y_{z'-1}} \quad (8)$$

式中, $x_{z'}$ 与 $y_{z'}$ 分别表示 $\mathbf{z}'$ 在二维坐标系中的空间点位混沌映射状态; c_1 表示混沌映射方程中的离散动力学参数^[20-22]; c_2 表示Henon映射中混沌行为控制参数; c_3 表示Henon映射中混沌轨迹控制参数。

在获取混沌映射方程式(7)~式(8)后,获得混沌序列 $\{x_{z'}\}$ 与 $\{y_{z'}\}$ 。假定二维空间中量子初始点 (x_0, y_0) ,将其作为量子加密算法的原始密钥输入到方程中进行迭代,当 c_1 出现周期窗口与周期分叉现象时(周期轨道发生从无到有的稳定性周期运动,同时周期轨道从一个稳定周期逐渐分裂为两个周期相同但轨道略异的周期2轨道),表示 $\mathbf{z}'$ 所代表的网关数据进入混沌状态。此处出现周期窗口与周期分叉现象时的迭代次数设置为 C ,则对 $\{x_{z'}\}$ 与 $\{y_{z'}\}$ 进行二进制序列转化后的原始量子密钥可表示为^[23-25]

$$kx_{z'} = x_{z'1}^2, x_{z'2}^2, x_{z'3}^2, \dots, x_{z'C}^2 \quad (9)$$

$$ky_{z'} = y_{z'1}^2, y_{z'2}^2, y_{z'3}^2, \dots, y_{z'C}^2 \quad (10)$$

式中, $kx_{z'}$ 与 $ky_{z'}$ 表示生成的原始量子密钥。

假定电力物联网系统中量子密钥的分配涉及 Δ_1 (密钥获得者)、 Δ_2 (密钥使用者)与 Δ_3 (密钥盗取者),且 $kx_{z'}$ 与 $ky_{z'}$ 中存在逆序基与 45° 对角偏振基两种量子态^[26-27],则需要基于二进制编码方式,将编码基准值设置为0和1。对不同量子态的密钥进行编码处理,输出具有安全密钥信息的比特序列(安全量子密钥) $\{\delta'_0 kx_{z'}\}$

$$\{\delta'_1 kx_{z'}\} = 1 - \frac{1}{\sqrt{2}}(\eta'_1 - \eta'_0) \quad (11)$$

$$\{\delta'_0 kx_{z'}\} = 1 - \frac{1}{\sqrt{2}}(\eta'_1 + \eta'_0) \quad (12)$$

式中, $\{\delta'_1 kx_{z'}\}$ 与 $\{\delta'_0 kx_{z'}\}$ 表示输出的安全量子密钥; δ'_1 表示编码为1的逆序基态下的加密运算符,代表的密钥分发协议为BB84协议; δ'_0 表示编码为0的逆序基态下的加密运算符,代表的密钥分发协议为B92协议; η'_1 表示编码

为0的 45° 对角偏振基态下的加密运算符,代表BBM92协议; η'_0 表示编码为0的 45° 对角偏振基态下的加密运算符,代表E91协议。

根据 $\{\delta'_1 kx_{z'}\}$ 与 $\{\delta'_0 kx_{z'}\}$,对 $\mathbf{z}'$ 所代表的电力物联网网关数据进行安全采集,具体实现流程如图2所示。

依据图2根据 $\{\delta'_1 kx_{z'}\}$ 与 $\{\delta'_0 kx_{z'}\}$ 对电力物联网网关数据进行加解密、用户验证操作、同步二次加密与数据采集指令执行,在数据传输与通信过程中实现电力物联网网关数据的安全采集。

2 实验分析

2.1 实验设置

为了验证设计算法的实际应用性能,以某电力企业SCADA系统与AMI系统中的电力物联网网关数据为实验对象,数据采集范围共涉及600个数据点,包含多种传感器终端设备上传的电力物联网数据,具体见表1。

本文利用OMNeT++软件对数据采集范围内的局域网络进行仿真,仿真环境参数如下:网络类型为无线传感网络(WSN),链路类型为多径信道,链路频带宽度为15 MHz,仿真误码率为0.02%,队列类型为FIFO队列,队列数据包上限为65个,CBR流量的时间间隔为0.6 s,模拟时间为15 s,TCP数据包大小为1 500 B。

仿真实验过程中涉及的具体实验设备型号与性能参数见表2。

(1) 利用OMNeT++软件搭建了仿真环境,模拟无线传感网络。在仿真环境中,配置网络参数包括链路类型为多径信道、链路频带宽度为15 MHz、仿真误码率为0.02%等,以模拟真实的电力物联网网络环境。

(2) 将量子密钥分发设备(QKD-2000)和网络安全设备(Cisco ASA 5516-X)等实验设备模拟或集成到仿真环境中,确保数据传输的安全性。其中,QKD-2000负责量子密钥的分发,保证数据在传输过程中使用的密钥安全可靠;而Cisco ASA 5516-X则提供网络安全防护,防止数据被非法访问或篡改。

(3) 在数据采集过程中,嵌入式测量和控制系统(cDAQ-9174)负责从传感器终端设备中采集数据,并将数据发送到电力物联网网关。利用量子加密算法对数据进行加密,并通过WSN传输到中央服务器。在传输过程中,利用TCP协议确保数据的可靠传输,并通过设置CBR流量的时间间隔和队列类型(FIFO)等参数,优化数据传输性能。

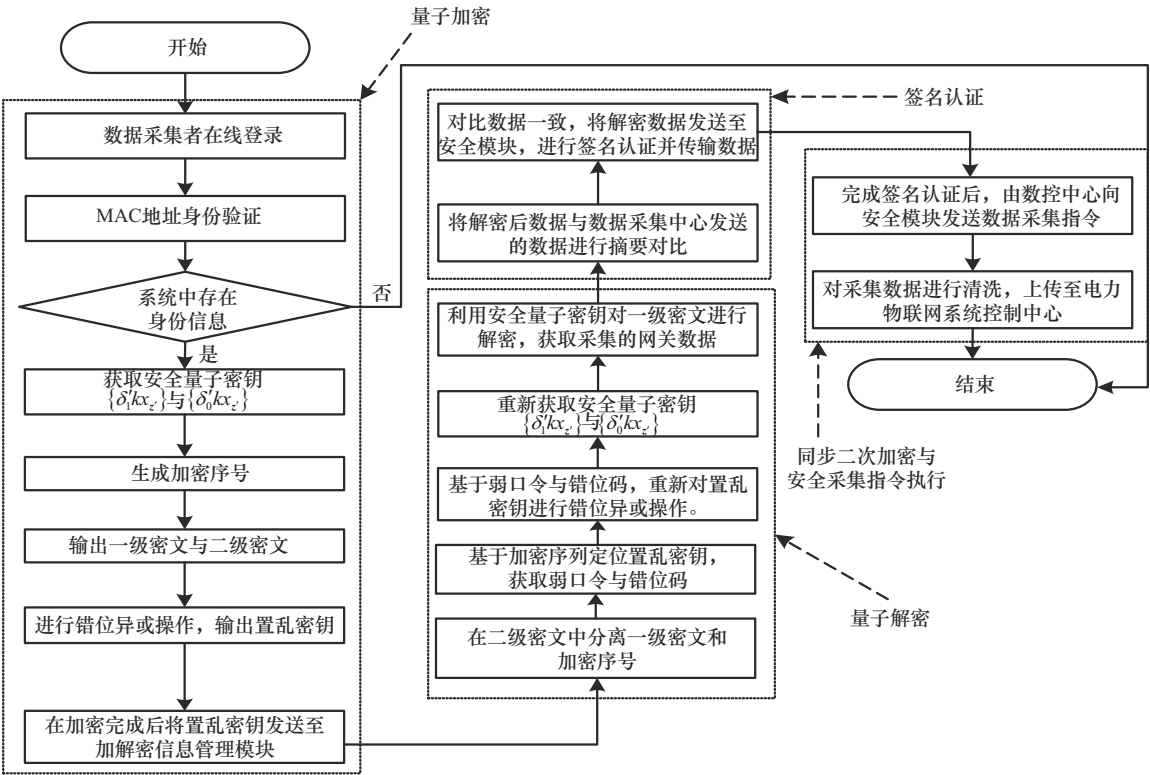


图 2 基于量子加密算法的网关数据安全采集流程

表 1 电力物联网数据		
数据类型	时间范围	数据量
实时电力参数 (电压、电流等)	1 小时(每秒 1 次采样)	10 MB
历史电量消耗数据 (日/月/年)	1 年(每日记录)	500 MB
事件数据 (故障告警、设备状态变化)	1 个月(每日平均 100 条记录)	10 MB
传感器诊断信息	每周上传一次	50 MB
智能电表读数(实时)	1 小时(每分钟 1 次采样)	20 MB
视频监控数据 (电网关键区域)	24 小时(高清分辨率)	5 GB

在上述设置的基础上，将设计方法应用前作为对比，对表 1 中的数据进行加密并在加密后模拟黑客攻击。由此，以加密时间和黑客攻击过程中数据的安全性作为评估指标，测试量子加密算法的效果。数据量子加密测试结果如图 3 所示。

基于图 3 (a)，参考不同数据格式所对应的编码方式、嵌套结构、结构化标签与元数据（代表数据大小、可读性和解析速度评价）可知，利用设计方法可以对不同格式的电力物联网网关数据进行加密，且加密时间虽然根据数据格式特征存在差异，但整体加密时间均未超过 120 ms，表明设计方法能够有效处理多种格式的网关数据。

表 2 实验设备型号与性能参数		
设备名称	设备型号	性能参数
量子密钥 分发设备	QKD-2000	最大密钥分发速率: 10 Mbit/s 传输距离: 100 km
网络安全设备	Cisco ASA 5516-X	最大吞吐量: 1 Gbit/s 最大连接数: 250 000 个 内存: 8 GB 接口类型: Gigabit Ethernet
嵌入式测量和 控制系统	cDAQ-9174	模拟输入通道数量: 可选 16、32 通道 采样速率: 可选 100 kS/s、500 kS/s 等 分辨率: 16 位 硬件接口: Ethernet、USB 等
服务器	PowerEdge R740	处理器: Intel Xeon Silver 4110 内存容量: 32 GB 网络接口: 以太网、光纤通道等
网络安全 分析工具	Wireshark	支持协议: IP、TCP、UDP、HTTP、 HTTPS、DNS 等 软件版本: v3.6.0 存储文件格式: pcap、pcapng 等

基于图 3 (b) 可知，数据大小对于加密时间具有显著影响。随着数据大小的提升，利用设计方法所产生的加密时间也持续增加，当数据量为 0~10 B 时，量子加密

时间为最低值 120 ms, 当数据量为 40~50 B 时, 量子加密时间达到最大值 178 ms, 但整体数据加密时间均未超过 180 ms。

分析图 3 (c) 可知, 基于量子加密算法应用后, 即使遭受黑客攻击, 也可以保证不同类型数据的安全性在 99% 以上。

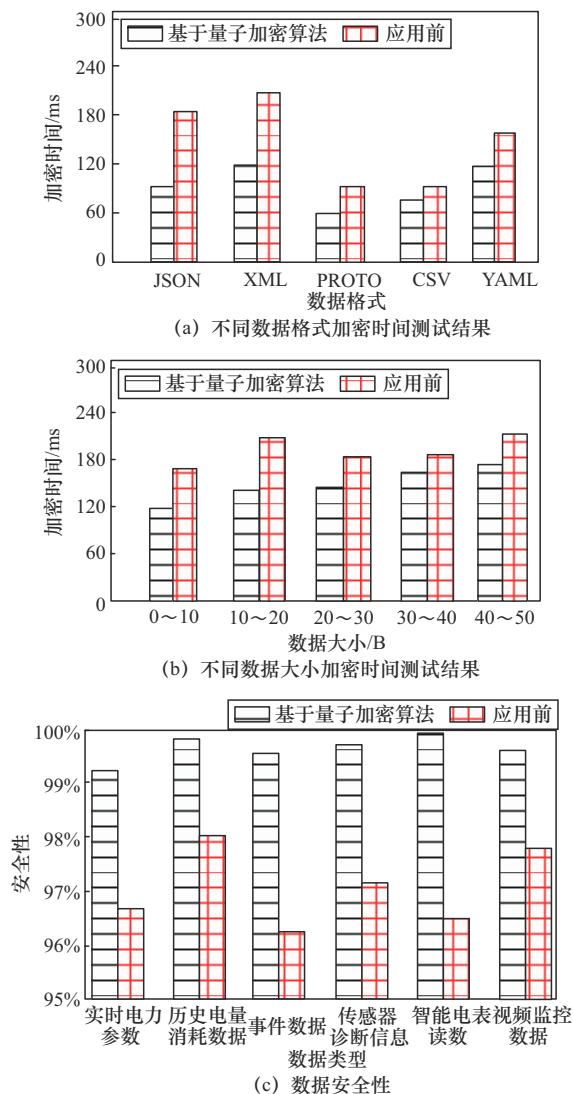


图3 数据量子加密测试结果

综上所述, 量子加密算法利用量子态的叠加性和纠缠性, 可以同时处理多个计算任务, 从而实现高效的加密和解密操作。这相比传统加密算法, 在处理大规模数据时具有显著的速度优势。此外, 量子加密算法对不同量子态下的原始密钥进行编码处理, 能够生成具有安全密钥信息的比特序列。这种编码过程增加了密钥的复杂性和多样性, 进一步提高了数据传输的安全性。因此,

量子加密算法应用后, 不仅可以有效提高数据加密时间, 还可以保证数据的安全性。

2.2 结果与分析

结合图 3 数据格式分析结果, 随机遍历 300 个数据节点, 利用 C++ 语言与 MQTT 协议将同属格式网关数据打包为不同大小的数据包。为了验证利用设计算法进行电力物联网网关数据采集的安全性和可靠性, 将参考文献 [4] 方法和参考文献 [5] 方法作为对比方法, 设置数据传输丢包率为评价指标。如果丢包率较高, 说明数据传输过程中存在数据丢失的问题, 可能导致数据不完整或准确性下降, 影响数据采集安全性。不同算法的数据传输丢包率测试结果如图 4 所示。

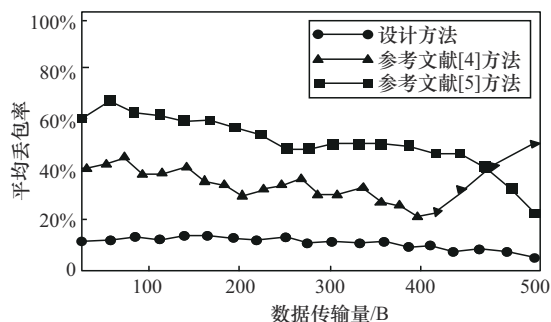


图4 数据传输丢包率测试结果

由图 4 可知, 利用设计方法进行电力物联网网关数据采集与传输, 随着数据传输量的增加, 平均丢包率在 7%~14% 之间浮动, 丢包率均低于其他两种方法, 表明利用设计方法在数据传输采集过程中能够较好地保证数据的完整性和准确性, 采集方法的安全性较高。

将数据传输吞吐量作为评价指标, 测试电力物联网网关数据采集效率。如果吞吐量较低, 说明方法对于网关数据处理能力较弱, 可能导致数据传输时延或阻塞, 数据传输与处理速度较慢, 数据采集方法的实时性和效率较低, 数据传输吞吐量测试结果如图 5 所示。

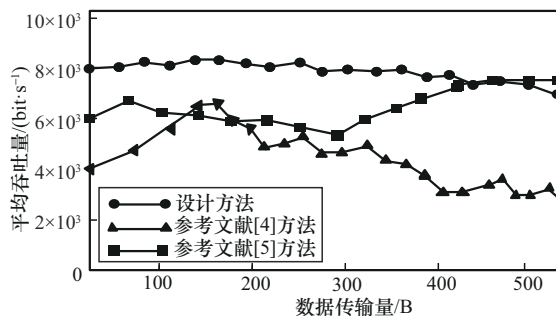


图5 数据传输吞吐量测试结果

由图5可知,随着数据传输量(采集过程中)的增加,利用设计方法所获取的平均吞吐量最高值为 8.2×10^3 bit/s、最低值为 7.8×10^3 bit/s,整体吞吐量均高于其他两种方法。表明设计方法具有较强的数据处理能力,能够快速地对传输数据,减少了数据传输的时延和阻塞情况,有效提高数据采集的效率。

3 结束语

基于量子加密算法,设计一种电力物联网网关数据安全采集方法,能够高效、稳定地采集与传输网关数据,并且能够有效确保数据采集过程中的安全性。实验结果表明,设计方法能够有效处理多种格式的网关数据,整体数据加密时间较短,并且在数据传输采集过程中能够较好地保证数据的完整性和准确性,确保网关数据的高效率采集。

参考文献:

- [1] 陈彬,徐欢,奚建飞,等.基于密码学累加器的电力物联网设备接入管理[J]. 计算机科学, 2022, 49(S2): 750-755.
CHEN B, XU H, XI J F, et al. Access management of power Internet of Things equipment based on cryptographic accumulator[J]. Computer Science, 2022, 49(S2): 750-755.
- [2] 刘晟.面向电力物联网的通信技术研究[J]. 通信电源技术, 2023, 40(2): 162-164.
LIU S. Research on communication technology for power Internet of Things[J]. Telecom Power Technology, 2023, 40(2): 162-164.
- [3] 江浩.基于AIE模式的电力物联网加密通信认证系统设计[J]. 电子设计工程, 2022, 30(1): 151-154.
JIANG H. Design of encrypted communication authentication system for power Internet of Things based on AIE mode[J]. Electronic Design Engineering, 2022, 30(1): 151-154.
- [4] 招景明,张捷,宋鹏,等.一种高效的基于云边端协同的电力数据采集系统[J]. 电网与清洁能源, 2022, 38(5): 49-55.
ZHAO J M, ZHANG J, SONG P, et al. An efficient method of electric power data acquisition system based on cloud edge collaboration[J]. Power System and Clean Energy, 2022, 38(5): 49-55.
- [5] 唐秋杭,李涛,陈华东.基于载波通信的电力终端数据采集检测技术研究[J]. 电网与清洁能源, 2022, 38(3): 74-79.
TANG Q H, LI T, CHEN H D. Research on data acquisition and detection technology of power terminal based on carrier communication[J]. Power System and Clean Energy, 2022, 38(3): 74-79.
- [6] 赵睿林. MQTT协议在智能电力网关中的实现[J]. 电器与能效管理技术, 2021(7): 83-87.
ZHAO R L. Realization of MQTT protocol in intelligent power gateway[J]. Electrical & Energy Management Technology, 2021(7): 83-87.
- [7] 赵丙镇,王栋,钱雪,等.基于区块链的电力物联网信任网关设计与实现[J]. 中国电力, 2021, 54(7): 192-197.
ZHAO B Z, WANG D, QIAN X, et al. Design and implementation of blockchain-based trust gateway for power Internet of Things[J]. Electric Power, 2021, 54(7): 192-197.
- [8] 王朴,陈泽西,毋凡,等.基于Logistic混沌的电力线载波频谱分组量子加密算法[J]. 沈阳工业大学学报, 2023, 45(3): 319-323.
WANG P, CHEN Z X, WU F, et al. Grouped quantum encryption algorithm based on Logistic chaos for power line carrier spectrum [J]. Journal of Shenyang University of Technology, 2023, 45(3): 319-323.
- [9] 高艺恬,陈立全,屠天扬,等.基于BRLWE的物联网后量子加密技术研究[J]. 网络与信息安全学报, 2022, 8(5): 140-149.
GAO Y T, CHEN L Q, TU T Y, et al. Post-quantum encryption technology based on BRLWE for Internet of Things[J]. Chinese Journal of Network and Information Security, 2022, 8(5): 140-149.
- [10] 庾亮.基于量子加密技术的音频信息加密方法[J]. 信息记录材料, 2023, 24(4): 217-219.
YU L. Audio information encryption method based on quantum encryption technology[J]. Information Recording Materials, 2023, 24(4): 217-219.
- [11] 冷迪,邱子良,黄建华,等.基于区块链技术的电力物联网网关入侵检测方法[J]. 长江信息通信, 2023, 36(1): 120-121.
LENG D, QIU Z L, HUANG J H, et al. Intrusion detection method of power Internet of Things gateway based on blockchain Technology[J]. Changjiang Information & Communications, 2023, 36(1): 120-121.
- [12] 龙凤,饶玮.基于DES算法的电力物联网信任网关数据远传加密[J]. 长江信息通信, 2024, 37(2): 23-24.
LONG F, RAO W. DES algorithm-based data teleportation encryption for power IoT trust gateway[J]. Changjiang Information & Communications, 2024, 37(2): 23-24.
- [13] 赵丙镇,王栋,钱雪,等.基于区块链的电力物联网信任网关设计与实现[J]. 中国电力, 2021, 54(7): 192-197.
ZHAO B Z, WANG D, QIAN X, et al. Design and implementation of blockchain-based trust gateway for power Internet of Things[J]. Electric Power, 2021, 54(7): 192-197.
- [14] 袁科,黄雅冰,杜展飞,等.基于混合梯度提升决策树和逻辑回归模型的分组密码算法识别方案[J]. 工程科学与技术, 2022, 54(4): 218-227.
YUAN K, HUANG Y B, DU Z F, et al. Block cipher algorithm identification scheme based on hybrid gradient boosting decision tree and logistic regression model[J]. Advanced Engineering Sciences, 2022, 54(4): 218-227.
- [15] 曲洪权,王征一,盛智勇,等.基于梯度提升决策树算法的光纤入侵信号分类[J]. 激光与光电子学进展, 2022, 59(23): 106-113.

- QU H Q, WANG Z Y, SHENG Z Y, et al. Fiber intrusion signal classification based on gradient boosting decision tree algorithm [J]. *Laser & Optoelectronics Progress*, 2022, 59(23): 106-113.
- [16] 邹鑫, 罗涓. 用梯度提升决策树实现电力负荷非线性影响因素分析[J]. *电力科学与工程*, 2024, 40(3): 10-19.
- ZOU X, LUO J. The analysis of nonlinear influence factors of electric power load realized by gradient lifting decision tree[J]. *Electric Power Science and Engineering*, 2024, 40(3): 10-19.
- [17] 张秋余, 宋宇杰. 基于改进 Henon 映射和超混沌的双重语音加密算法[J]. *电信科学*, 2021, 37(12): 11-24.
- ZHANG Q Y, SONG Y J. A dual speech encryption algorithm based on improved Henon mapping and hyperchaotic[J]. *Telecommunications Science*, 2021, 37(12): 11-24.
- [18] 佟晓筠, 毛宁, 张森, 等. 基于 Henon 映射与改进的提升小波变换图像加密算法[J]. *信息网络安全*, 2022, 22(9): 31-39.
- TONG X J, MAO N, ZHANG M, et al. Image encryption algorithm based on Henon mapping and improved lifting wavelet transform[J]. *Netinfo Security*, 2022, 22(9): 31-39.
- [19] 张秋余, 宋宇杰. 基于改进 Henon 映射和超混沌的双重语音加密算法[J]. *电信科学*, 2021, 37(12): 11-24.
- ZHANG Q Y, SONG Y J. A dual speech encryption algorithm based on improved Henon mapping and hyperchaotic[J]. *Telecommunications Science*, 2021, 37(12): 11-24.
- [20] 杨轶, 荣锋, 武志刚. 改进混沌方程及其在保密 VoIP 系统中的应用与实现[J]. *电讯技术*, 2022, 62(7): 971-977.
- YANG Y, RONG F, WU Z G. Improved chaotic equation and its application and realization in a secure VoIP system[J]. *Telecommunication Engineering*, 2022, 62(7): 971-977.
- [21] 王佳音, 宋大全, 侯梦瑜, 等. 基于有效精度的 Logistic 混沌方程计算轨道偏离研究[J]. *牡丹江师范学院学报(自然科学版)*, 2022 (3): 17-21.
- WANG J Y, SONG D Q, HOU M Y, et al. Research on computing orbit deviation in the logistic chaotic equation based on effective precision[J]. *Journal of Mudanjiang Normal University (Natural Sciences Edition)*, 2022(3): 17-21.
- [22] 杜鑫昌, 高瑜翔, 曹远杰, 等. 改进混沌方程及压缩感知理论图像加密算法[J]. *计算机与现代化*, 2022(4): 115-120.
- DU X C, GAO Y X, CAO Y J, et al. Improved image encryption algorithm based on chaotic equation and compressed sensing theory [J]. *Computer and Modernization*, 2022(4): 115-120.
- [23] 张光伟, 白建东, 颜琦, 等. 连续变量量子密钥分发系统中动态偏振控制研究[J]. *物理学报*, 2024, 73(6): 18-26.
- ZHANG G W, BAI J D, XIE Q, et al. Research on dynamic polarization control in continuous variable quantum key distribution systems[J]. *Acta Physica Sinica*, 2024, 73(6): 18-26.
- [24] 孙羽, 党仁, 周虎, 等. 基于区块链的量子密钥分发在云存储的应用研究[J]. *软件工程*, 2024, 27(1): 14-18.
- SUN Y, DANG R, ZHOU H, et al. Research on the application of blockchain-based quantum key distribution in cloud storage[J]. *Software Engineering*, 2024, 27(1): 14-18.
- [25] 张一辰, 边一铭, 王恒, 等. 面向城域接入的连续变量量子密钥分发技术[J]. *信息通信技术与政策*, 2023(7): 53-59.
- ZHANG Y C, BIAN Y M, WANG H, et al. Continuous-variable quantum key distribution for metropolitan and access networks[J]. *Information and Communications Technology and Policy*, 2023(7): 53-59.
- [26] 王朴, 陈泽西, 毋凡, 等. 基于 Logistic 混沌的电力线载波频谱分组量子加密算法[J]. *沈阳工业大学学报*, 2023, 45(3): 319-323.
- WANG P, CHEN Z X, WU F, et al. Grouped quantum encryption algorithm based on Logistic chaos for power line carrier spectrum [J]. *Journal of Shenyang University of Technology*, 2023, 45(3): 319-323.
- [27] 黄红梅. 基于量子密钥分发和像素置乱的图像加密方法研究[J]. *激光杂志*, 2023, 44(1): 96-102.
- HUANG H M. Research on image encryption method based on quantum key distribution and pixel scrambling[J]. *Laser Journal*, 2023, 44(1): 96-102.

[作者简介]



张静鑫 (1978-), 男, 本科, 助理工程师, 主要研究方向为电力设备、数据安全、加密算法、物联网等。

陈超 (1979-), 男, 硕士, 中级工程师, 主要研究方向为电力设备、量子加密等。

张平 (1980-), 男, 本科, 助理工程师, 主要研究方向为电力设备、计算机软件工程、物联网网关等。