doi: 10.7690/bgzdh.2025.12.008

基于可信密码模块的电力物联网边缘侧信息安全传输方法

孙艳玲，朱晨光，高群伟，赵世伟
（平高集团有限公司，河南 平顶山 467000）

摘要：针对电力物联网边缘侧信息安全传输，提出基于可信密码模块的传输方法。构建 SG-Edge 可信边缘计算框架，实现在确保传输任务安全性约束条件下的信息传输执行效率优化。结合 USBKey 双因素、TCM 认证机制，通过量化处理，度量信息传输信道安全性。通过多轮复合加密过程逆操作，生成可信密钥，保证无线信道互易性。计算初始相干时间，使得调整后的训练序列长度能够在相干时间段内完成数据安全传输。实验结果表明，该方法在 12:00～21:00 时间段内三相电流与实际数据仅存在最大为 10、4 和 5 A 的误差，相比于其他方法传输误差最小，说明使用该方法能够保护边缘侧信息传输安全。

关键词：可信密码模块；电力物联网；边缘侧信息；安全传输
中图分类号：TP309　　**文献标志码：**A

Information Security Transmission Method for Edge Side of Power IoT Based on Trusted Cryptographic Module

Sun Yanling, Zhu Chenguang, Gao Qunwei, Zhao Shiwei
(*Pinggao Group Co*., *Ltd*., *Pingdingshan* 467000, *China*)

Abstract: A transmission method based on trusted cryptographic modules is proposed for secure information transmission on the edge side of the power IoT. The SG-Edge trusted edge computing framework is constructed to optimize the execution efficiency of information transmission under the constraint of ensuring the security of transmission tasks. By combining USBKey dual-factor and TCM authentication mechanisms, the security of the information transmission channel is measured through quantitative processing. Through multiple rounds of composite encryption process inverse operations, a trusted key is generated to ensure the reciprocity of wireless channels. The initial coherence time is calculated so that the adjusted training sequence length can complete secure data transmission within the coherence time period. The experimental results show that the method has errors of up to 10, 4, and 5 A between the three-phase current and actual data during the time period from 12:00 to 21:00. Compared with other methods, the transmission error is minimal, indicating that the use of this method can protect the security of information transmission on the edge side.

Keywords: trusted cryptographic module; power IoT; edge-side information; secure transmission

0　引言

电网的安全、高效和有序运行是国家稳定和健康发展的重要保障。在海量数据时代，各类网络攻击无处不在。因为电网的最终设备非常巨大，这就导致了电网受到恶意攻击的可能性非常高，数据的安全性问题越来越突出。当电力物联网受到外界攻击时，极有可能造成对电网的经营与管理出现错误，进而造成整个电网崩溃。当前，对电力数据安全问题研究已成为国内外相关学者关注的焦点。文献[1]提出了多元速率兼容低密度奇偶校验的传输方法，该方法使用的是以自适应的调制与编码机制为基础的隐私保护算法，并与信道隐私保护算法相结合，通过采用“过窄”的安全间隔，降低了接收误码率，确保了信息传输的安全性；然而，使用该方法容易把当前的文件全部覆盖，无法实现对文件的无损压缩，存在占用资源多、压缩程度有限等缺陷，所以不适合使用；文献[2]提出了基于扩展贝叶斯分类的传输方法，该方法通过构建一种新型的增强型贝叶斯分类器，基于异常检测的结果，对所辨识的涉密信息进行安全性检验，并对所辨识的涉密信息进行安全性判定；然而，这种方法密码计算任务是以单个虚拟机为关键设备实现的，缺少对多个加密级别的任务间分离。为满足电网物联网中的数据安全传输要求，笔者提出了基于可信密码模块的电力物联网边缘侧信息安全传输方法。构建 SG-Edge 可信边缘计算框架，通过可信密码模块满足不同边缘侧信息安全传输服务需求。

1　SG-Edge 框架的安全传输决策量确定

构建基于 SG-Edge 的可信边缘计算框架，实现边缘侧信息传输的最优。将信息传输至指定可信模

收稿日期：2024-10-18；**修回日期：**2024-11-18
第一作者：孙艳玲（1980—），女，河南人，硕士。

块，以达到多端数据传输的个性化需求。

1.1 SG-Edge 可信边缘计算框架构建

针对电网中对边界计算的需求，提出一种适用于电网中边界计算的可信边缘计算框架 SG-Edge，并从安全运行、硬件保障等方面进行研究，以确保边界算法的安全可靠[3]。在对开放性、可靠性、安全性以及云边协作等方面的要求进行了全面考虑，并将其与 EdgeX 的设计思想相结合，从而对 SG-Edge 进行了具体的设计和实施，如图 1 所示。

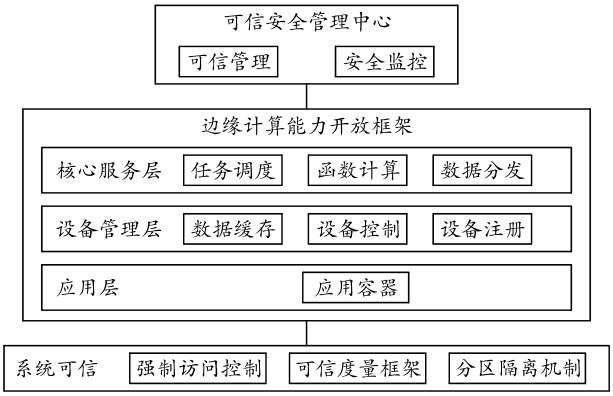


图 1 SG-Edge 可信边缘计算框架

由图 1 可知：系统可信层主要包括了通过密码技术来构建的信任基础，通过使用了硬件特点来构建的信任启动与信任隔离技术[4]；应用层操作系统采用的是 3 权分立模式，能够实现磁盘加密、双因子认证；设备管理层在安全等级保护的基础上，实现了对用户的安全控制、对用户的信任度测度和对用户的远程认证；核心服务层参考了安全等级保护 2.0 的要求，通过安全等级保护，实现了对使用者的可信度测度和对使用者的远程认证[5-7]。

随着对电力系统关键组成部分的实时监测，电力系统中的边缘设备(例如，边界层“大脑”)对安全等级的要求越来越高，包括可靠启动、安全升级、安全保护、安全监控等[8]。基于此，从 2 个角度对目前已存在的安全与可靠问题进行了详细的分析。通过对业务活动中软件和业务之间相互作用的研究，建立一套以业务活动为核心的作业可信性度量体系。

1.2 基于任务调度的安全传输决策量确定

根据电网业务承载类型、计算资源等特性，对特定的物理/虚拟加密算法进行优化，以适应各类网络安全业务的个体化需要，并将计算工作配置在优化的计算节点上。针对高安全、高资源消耗、高安全性、高效率的大型任务，开展相关关键算法的研究。该虚拟密码模块寄存服务器被独立地配置，并且是唯一的[9]。该安全口令任务调度被定义成一个映射函数，该映射函数是从服务任务到操作节点，将第 i 个任务分配到一个虚拟加密模块中，通过专用物理密码模块二进制变量转换，分配到第 0 号宿主机中[10]。对于专用物理密码模块的二进制变量，可用如下公式表示：

$$x_{ij}^{P}=\begin{cases}1 & \text{任务被分配}\\ 0 & \text{任务未被分配}\end{cases}; \tag{1}$$

$$x_{ij}^{V}=\begin{cases}1 & \text{任务被分配}\\ 0 & \text{任务未被分配}\end{cases}。 \tag{2}$$

式中：x_{ij}^{P} 为第 i 个任务的第 j 个专用物理密码机二进制变量；x_{ij}^{V} 为第 i 个任务的第 j 个虚拟密码机二进制变量[11]。

当第 i 个任务被分配到专用物理密码模块、虚拟密码模块时，SG-Edge 可信边缘计算框架的安全决策量可表示为：

$$C_i=\begin{cases}1.0 & x_{ij}^{P}=1\\ 0.5 & x_{ij}^{V}=1\end{cases}。 \tag{3}$$

对于任务最大安全性能目标函数，可表示为：

$$\sum_{i=1}\sum_{j=1}x_{ij}^{P}R_{ij}W(t_{ij})\leqslant Omn。 \tag{4}$$

式中：R_{ij} 为节点出口任务；$W(t_{ij})$为最早完成时间求解的函数；O 为密码资源总量。通过任务调度结果，能够确定电力物联网边缘侧信息安全传输决策量[12]。

2 基于可信密码模块的信息安全传输

通过对专用物理密码模块进行二值化处理，为 SG-Edge 的可信任边界计算提供支持。利用对数据进行定量的分析，将不同的信道特性转换成不同比特流，从而对数据进行有效保密。通过调节训练序列长短，实现电力物联网边缘侧信息安全传输。

2.1 可信密码模块边缘侧信息传输信道安全性度量

可信密码模块作为最基本、最安全、最可靠的信任根，在保证数据安全的前提下，对数据进行加密处理。可信密码模块下发布的口令也是最基本、最安全、最可靠的口令，拥有一定的数据存储能力[13]。在边缘侧信息可信度量过程中，边缘侧信息度量模块利用 USBKey 的双因素认证方式和 TCM 身份验证方式，依据边缘侧信息获取身份验证和权限获取[14]。

利用可信密码模块进行的边缘侧信息传输信道安全性度量流程，如图 2 所示。

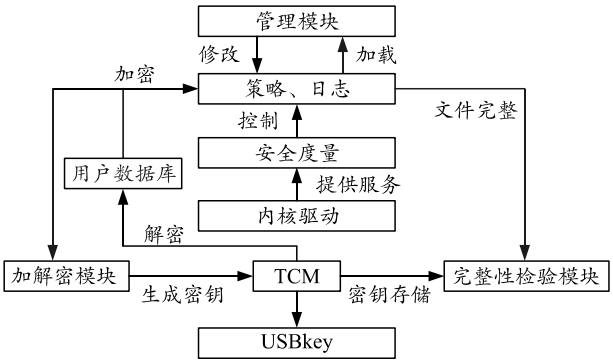


图 2　边缘侧信息传输信道安全性度量流程

在使用了一个合适的 USBKey 后，使用者便可以使用信任的口令来获取解密密钥。采用信任口令模型对用户数据库进行解码，并将其作为边缘侧信息度量模块提供相关信息[15]。

通过量化处理可将合法通信双方 *A* 端、*B* 端提取的信道特征转化为比特流，其中 *A* 端和 *B* 端使用如下公式计算量化门限：

$$\lambda_n^+ = z_n + \iota\delta_n ; \tag{5}$$

$$\lambda_n^- = z_n - \iota\delta_n 。 \tag{6}$$

式中：z_n 为 n 个平均值；δ_n 为 n 个方差；ι 为量化因子。当通信信道安全性较低时，量化因子取值将增大，此时 2 个量化门限间隔范围也会随之增大；反之，则减小。定义一个度量器 $P(t)$，可用如下公式来表示：

$$P(\lambda)=\begin{cases}0 & \lambda \leqslant \lambda_n^- \\ 1 & \lambda \geqslant \lambda_n^+\end{cases} 。 \tag{7}$$

式中 *A* 端和 *B* 端将量化值作为度量器的输入，其输出结果为量化后的信息流。当量化值大于 λ_n^+ 时，则度量结果为 1，说明信道安全；当量化值大于 λ_n^- 时，则度量结果为 0，说明信道不安全。

2.2　基于可靠密钥的信息安全传输

在可信密码模块的加密过程中，通过对密钥进行扩充来实现对密钥序列的扩充，从而实现了对密钥序列的扩充。假设该密码体系是一个具有初始值的字符，那么需先处理该密码体系中的一个关键数组，再用下面的表达式将该密码体系中的一个不是 4 位的单位转换成如下数学形式：

$$Q[k]=Q[k-1]\oplus[k-4]。 \tag{8}$$

采用 *S* 盒替换法对每个字符进行多循环合成，从而完成了对该字符的反运算，达到了对字符还原的目的。*A* 端和 *B* 端获取的公共信道响应相同。如果 *A* 端和 *B* 端距离超过电磁波的长度，那么就无法获取与安全传输信道相似的特征，也就无法安全传输数据；因此，*A* 端和 *B* 端通过可信密钥来进行信息安全传输，如图 3 所示。

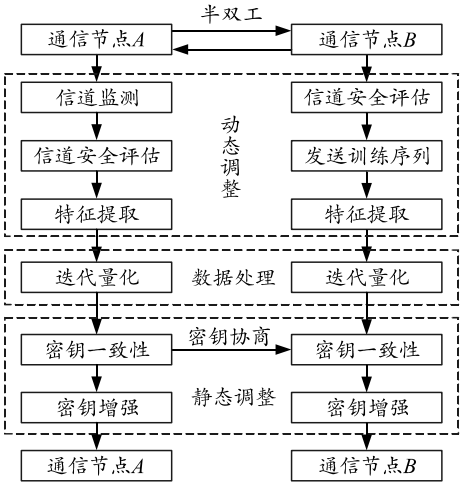


图 3　可信密钥生成流程

对于 *A* 端接收到 *B* 端发送的信号，以及 *B* 端接收到 *A* 端发送的信号，可用如下公式表示：

$$y_{AB}=\eta_{AB}x(t)+\mu_{AB}(t); \tag{9}$$

$$y_{BA}=\eta_{BA}x(t)+\mu_{BA}(t)。 \tag{10}$$

式中：η_{AB}、η_{BA} 分别为 t 时刻下 *A* 端到 *B* 端以及 *B* 端到 *A* 端的信道响应结果；$\mu_{AB}(t)$、$\mu_{BA}(t)$ 分别为 t 时刻下通信信道的加性噪声。

当 2 个通信节点相互向对方发送用于检测信道的训练序列时，如果数据的传输距离超过了相关的时间，就会产生一种畸变现象。在信道监测过程中，信道传输的相关时间将直接影响到信道传输的数据量，进而对信道传输的数据量产生影响。为了从根本上保障信道的互易性，需要根据信道相关时间变化，对训练数据进行实时调节。

对于 *A*、*B* 2 个通信方，设双方通信时间为 t_{AB}，相干时间为 t_C，两者的比值与信道互易性相关。当两者比值大于 1，说明通信时间、相干时间与信道无关；当两者比值小于等于 1，说明通信时间、相干时间与信道有关，且该比值越小，信道通信可靠性越高。基于高级加密的可信信息安全传输，其具体步骤如下所示：

步骤 1：*A* 端向 *B* 端发送初始待传输序列，*B* 端接收后使用如下公式，计算初始相干时间。

$$t_C=1/\eta_{\max}。 \tag{11}$$

式中 $\eta_{\max}$ 为最大多普勒频移。

步骤 2：*B* 端将步骤 1 计算出来的初始相干时

间代入如下公式，可表示为：

$$t_{AB}=\alpha t_C。\tag{12}$$

步骤 3：若 $2t_0<t_{AB}$，则不需对该起始序列进行动态调节。若 $2t_0\geqslant t_{AB}$，则应将该起始的训练序列的长短缩短到 L。

步骤 4：B 端请求 A 端重新发送长度为 L 的序列，并由此进行可信密码模块边缘侧信息传输信道安全性度量。

步骤 5：对 A、B 2 端反复进行以上过程，保证在相干时间段内实现对所需的信息的保密传输。

3　实验

3.1　实验过程监控装置

系统采用分层分布式体系结构，在垂直方向上划分为：监测、通信网络和现场监控层 3 个层次。监测层由 1 个技术台和 1 个远动通信台组成，软件部分具备 1 个良好的人机接口，通过一种能够被自动计算的方式，将通信管理机上采集到的各类现场的各类数据，用图表、数显、声音等方式，将工作状态展示出来。在电能计量管理功能中，对多种不同的报告形式进行了合理的分析，并对报告中的数据进行了详细计量，建立起了一个完整的计量体系，使用者可以在其中进行查询和印刷，这给操作带来了很大的便利，同时还提升了工作效率。实验过程监控装置，如图 4 所示。

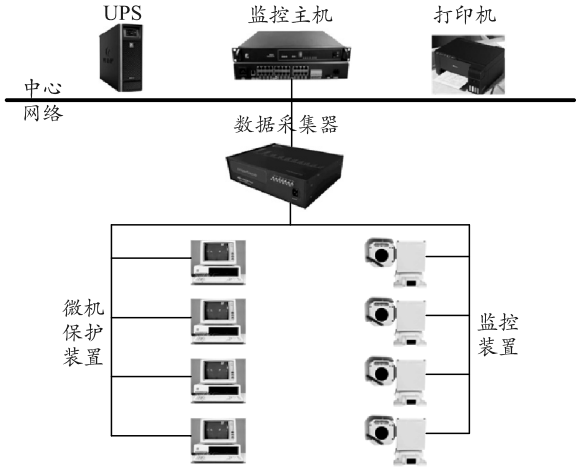
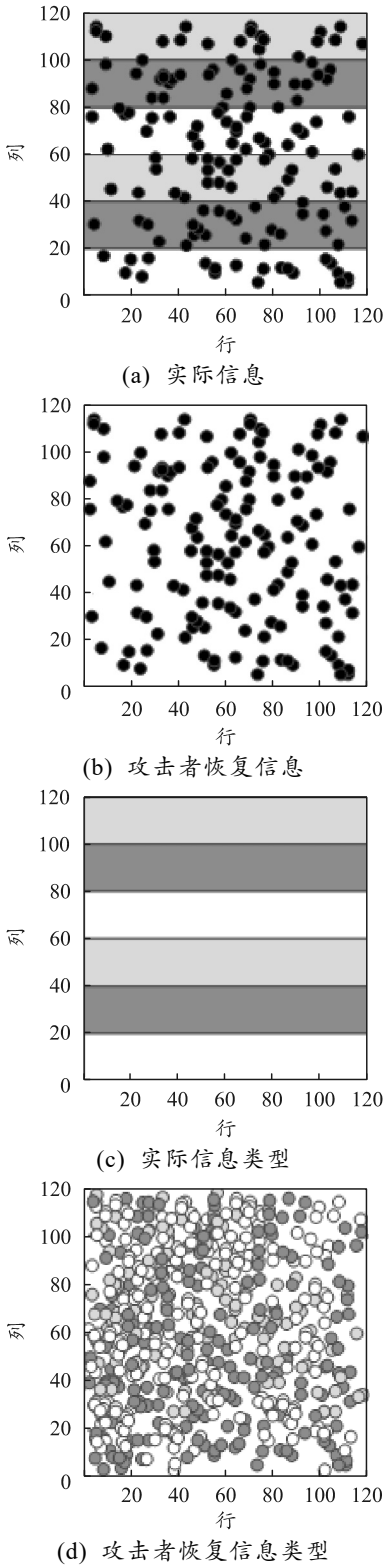


图 4　实验过程监控装置

利用高精度智慧仪器对电能展开理性的管制和报警，从而可以快速地发现异常电力物联网边缘侧信息，并进行相应的解决。

3.2　验证所研究方法安全性

假设通信链路上，存在着一名攻击者，能够窃取到所有的电能传输数据，并且对数据恢复有着一定的了解，那么攻击者就能够窃取到某电能表传回的所有信息。为了验证所研究方法的有效性，测试了所研究方法对边缘侧多种信息的安全传输情况，如图 5 所示。



(a) 实际信息

(b) 攻击者恢复信息

(c) 实际信息类型

(d) 攻击者恢复信息类型

图 5　实际数据、类型和攻击者恢复数据、类型

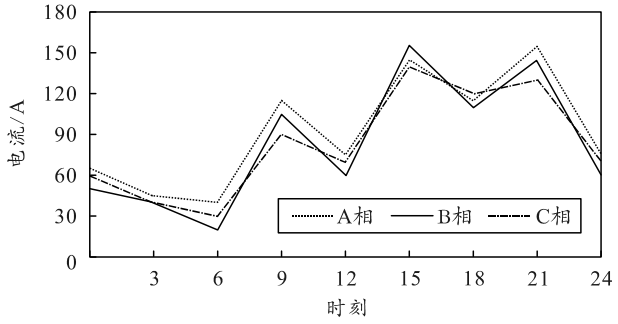
对于图 5(a)、(b)可知：图 5(a)中存在清晰分界

线，能够辨识边缘侧信息类型，而经过所研究方法处理后的图 5(b)则不存在分界线，无法辨识边缘侧信息类型。

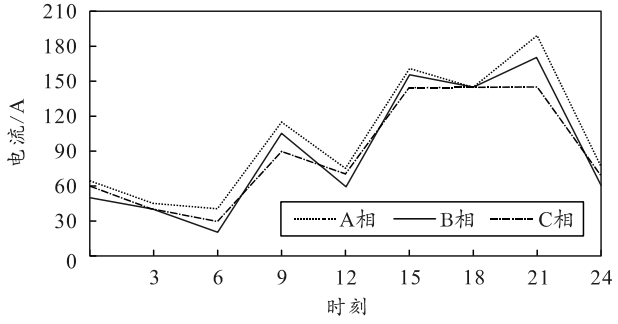
对于图 5(c)、(d)可知：图 5(c)中清晰显示不同种类边缘侧信息类型，而经过所研究方法处理后的图 5(d)无法精准辨识边缘侧信息类型。因此，使用这种方法来对原始电能数据的电能类别属性进行分析。即使被攻击者截获并还原了使用者的信息，也无法从信息中推断出使用者的真实信息及信息所涵盖的范围，可以避免使用者信息被窃取而导致使用者信息泄漏。

3.3　验证所研究方法对边缘侧信息的保护能力

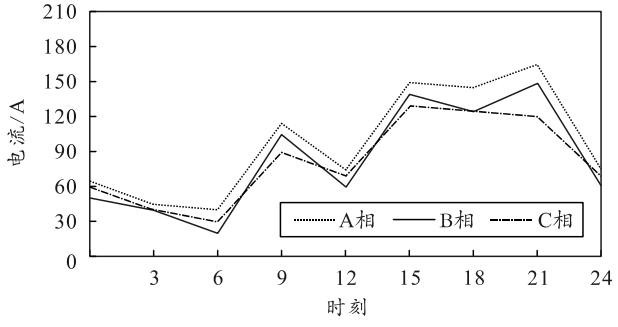
以三相电流数据为研究对象，使用所研究方法与多元速率兼容低密度奇偶校验方法、基于扩展贝叶斯分类方法，对比分析边缘侧三相电流数据传输精准度，以此作为验证边缘侧信息保护能力的依据，对比结果如图 6 所示。



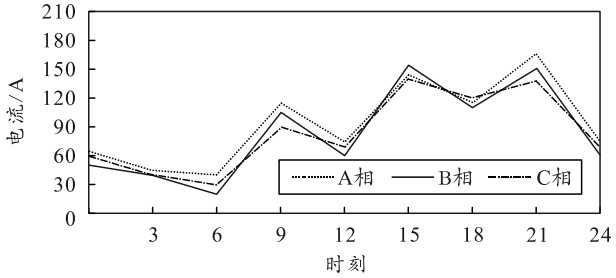
(a) 实际数据



(b) 多元速率兼容低密度奇偶校验



(c) 扩展贝叶斯分类



(d) 所研究方法

图 6　不同方法边缘侧三相电流数据传输精准度对比分析

由图 6(a)可知：00:00～12:00 时间段内，三相电流始终低于 120 A；12:00～21:00 时间段内，三相电流出现了最大值，分别为 A 相 155 A、B 相 145 A、C 相 130 A。

由图 6(b)可知：00:00～12:00 时间段内，三相电流始终低于 120 A，该时间段内的数据与实际数据完全一致；12:00～21:00 时间段内，三相电流与实际数据不一致，A 相、B 相、C 相对应的最大值与实际数据分别存在 38、33、10 A 的误差。

由图 6(c)可知：00:00～12:00 时间段内，三相电流始终低于 120 A，该时间段内的数据与实际数据完全一致；12:00～21:00 时间段内，三相电流与实际数据不一致，A 相、B 相、C 相对应的最大值与实际数据分别存在 15、15、5 A 的误差。

由图 6(d)可知：00:00～12:00 时间段内，三相电流始终低于 120 A，该时间段内的数据与实际数据完全一致；12:00～21:00 时间段内，三相电流出现了最大值，该时间段内的三相电流与实际数据分别存在最大为 10、4、5 A 的误差。

通过上述分析结果可知：使用所研究方法边缘侧信息传输结果与实际结果误差最小，说明使用该方法能够保护边缘侧信息传输安全。

4　结束语

针对传统方法存在的无法安全传输问题，提出了基于可信密码模块的电力物联网边缘侧信息安全传输方法，该方法在研究保障信息安全方面取得了如下结论：

1) 在保证通信安全的前提下，建立 SG-Edge 的可信边缘计算框架，以最大限度地提高通信系统的性能。将数据传送到特定的实体与虚拟加密模块中，以实现对多端数据传送的个体化要求。

2) 通过对专用物理密码模块进行二值化处理，为 SG-Edge 的可信边缘计算框架提供支持。

（下转第 58 页）