DOI:10. 20033/j. 1003-7241. (2026)02-0143-05

基于区块链技术的地下管线运维数据安全传输方法

刘　恪, 何智祥, 葛眠俊

(广东电网有限责任公司 佛山供电局, 广东 佛山 528000)

摘　要:为解决地下管线运维数据在传输中易受网络攻击和未授权访问威胁的问题,提出基于区块链技术的地下管线运维数据安全传输方法。采用递归的方式对当前节点的邻居节点进行查找,并将其放入堆栈中,构建出传输路径矩阵。并结合相邻路径之间的节点相交情况对路径可信度进行计算,筛选出安全程度较高的传输路径。结合密盒的正向操作以及逆向操作,对运维数据信息字节进行正反向变换处理,并结合行位移操作,提高字节变换的扩展性,实现数据加密处理。最后结合区块加密函数对区块进行加密处理,并结合区块连接以及加密操作实现数据传输,采用频率补偿值对输出的数据通信频率进行补偿与优化。对提出的方法进行了传输安全性的检验。最终的测试结果表明,采用提出的方法对地下管线运维数据进行传输时,数据泄露规模较小,具备较为理想的传输安全性。

关键词:区块链技术;地下管线;运维数据;安全传输;数据传输

中图分类号: TP393. 083　　**文献标志码**: A　　**文章编号**: 1003-7241(2026)02-0143-05

Safe transmission method of underground pipeline operation and maintenance data based on blockchain technology

LIU Ke[1], HE Zhixiang[2], GE Mianjun[3]

(Foshan Power Supply Bureau, Guangdong Power Grid Co., Ltd., Foshan 528000, Guangdong, China)

Abstract: To address the vulnerability of underground pipeline operation and maintenance data to network attacks and unauthorized access threats during transmission, a secure transmission method for underground pipeline operation and maintenance data based on blockchain technology is proposed. It uses recursive methods to search for neighboring nodes of the current node, and puts them on the stack to construct a transmission path matrix. And based on the intersection of nodes between adjacent paths, it calculates the credibility of the paths and selects the transmission paths with higher security levels. Combining the forward and reverse operations of the encryption box, the operation and maintenance data information bytes are subjected to forward and reverse transformation processing, and combined with row displacement operation to improve the scalability of byte transformation and achieve data encryption processing. Finally, the block is encrypted using a block encryption function, and data transmission is achieved by combining block connections and encryption operations. Frequency compensation values are used to compensate and optimize the communication frequency of the output data. The proposed method is tested for transmission security. The final test results indicate that when using the proposed method to transmit underground pipeline operation and maintenance data, the scale of data leakage is small, and it has relatively ideal transmission security.

Keywords: blockchain technology; underground pipelines; operation and maintenance data; secure transmission; data transmission

在数字经济的背景下,城市管理的数字化转型已成为必然趋势。随着城市地下管线的规模和复杂度不断增加,产生的运维数据量也在迅速增长。这些数据包括管线的运行状态、监测数据、维护记录等,对于保障管线的正常运行和及时响应故障至关重要[1]。地下管线运维数据的安全传输,直接关系到城市基础设施的安全稳定运行。传统的数据传输方法往往依赖于中心化的数据存储和管理系统,这些系统面临着数据篡改、丢失以及隐私泄露等风险。此外,由于地下管线网络的复杂性和庞大性,数据的实时性和准确性也难以得到保障。因此,研究一种安全、高效、可靠的数据传输方法,对于提升地下管线运维水平具有重要意义。

当前,国内外学者已经针对数据安全传输技术进行了较为深入的研究。例如,文献[2]利用复杂的加密算法和安全的通信协议,确保数据的机密性和完整性。然而,该方法的不足之处在于其实现过程较为复杂,需要较高的计算资源,这可能导致在资源受限的环境中数据传输效率降低。此外,过于复杂的加密算法也可能增加出错的可能性,进而引发数据安全问题。文献[3]采用了数据加密、身份认证和访问控制等多种技术手段,确保体测数据在物

收稿日期:2024-05-16;**录用日期**:2024-05-21

基金项目:广东电网科技项目(GDKJXM20220722;030600KK52220032)

作者简介:刘　恪(1995—),男,硕士研究生,工程师,研究方向:配网运维。

引用本文:刘恪, 何智祥, 葛眠俊. 基于区块链技术的地下管线运维数据安全传输方法[J]. 自动化技术与应用, 2026,45(2):143-146. (LIU Ke, HE Zhixiang, GE Mianjun. Safe transmission method of underground pipeline operation and maintenance data based on blockchain technology[J]. Techniques of Automation and Applications, 2026,45(2):143-146.)

联网环境中的安全传输。但是由于物联网环境的复杂性和多样性,该方法在应对各种潜在安全威胁时存在一定的局限性。例如,在面对高级持续性威胁(APT)攻击时,该方法可能无法有效识别和防御,从而导致传输安全性降低。文献[4]通过集成SSL协议和国密算法,实现了数据的加密传输和身份认证。但该方法在保障传输安全性的同时,也带来了一定的性能开销。由于SSL协议本身的复杂性,以及国密算法在处理大规模数据时的效率问题,可能导致传输速度降低,从而影响系统的实时性和可用性。文献[5]通过构建多通道传输网络,实现了数据的并行传输和冗余备份。但是由于多通道传输需要更多的网络资源和设备支持,数据并行传输的安全性可能会受到较大的威胁。

对此,本文以区块链技术为依托,将其应用至地下管线运维数据安全传输中,设计一种地下管线运维数据安全传输方法。该方法通过构建分布式数据存储网络,利用区块链的去中心化特性,实现对运维数据的分布式存储和加密传输。

1 方法设计

1.1 传输可信路径筛选

由于传输路径可信度对于数据传输的安全性有着较大的影响,同时对于地下管线运维数据来说,任何数据的丢失或篡改都可能对城市的正常运行造成严重影响,因此通过查找与筛选可信路径,对存在异常风险的路径进行识别[6]。假设在地下管线运维数据拓扑网络中,源节点以及目标节点分别为 a_0 和 a_1,可以将源节点放入堆栈中,通过特定的路径查找邻居节点,到达目标节点为止。基于上述递归过程,本文构建出的传输路径矩阵表达式为

$$\boldsymbol{R}=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1j} \\ r_{21} & r_{22} & \cdots & r_{2j} \\ \vdots & \vdots & \vdots & \vdots \\ r_{i1} & r_{i2} & \cdots & r_{ij} \end{bmatrix} \tag{1}$$

其中,r_{ij} 代表地下管线运维数据在进行传输过程中节点 i 到节点 j 之间的传输路径。在上述传输路径矩阵中,每个元素均可以代表一个地下管线运维数据的传输路径,但有些路径可能由于网络拥堵、延迟高或传输速度慢等原因,导致数据传输效率低下。因此本文通过计算路径之间的相交情况,对路径可信度进行计算,J_{ij} 假设代表两个传输路径之间的节点相交数量,那么路径可信度 D_i 计算公式为

$$D_i=\sum_{i=1}^{N}\frac{\left(\frac{J_{ij}}{N_{r_i}}+\frac{J_{ij}}{N_{r_j}}\right)}{2} \tag{2}$$

其中,N_{r_i} 和 N_{r_j} 分别代表地下管线运维数据传输路径 r_i 与路径 r_j 之间的相交阈值,K 代表传输路径矩阵中的元素总数。通过上述公式可以看出,本文所计算出的路径可信度在一定程度上代表了不同路径之间的相交程度,两条路径中节点相交程度越高,代表该路径越稳定,在数据传输过程中越不容易出现数据篡改或丢失的情况。因此通过对 D_i 设定一个筛选阈值 φ_{D_i},即可实现对传输可信路径的有效筛选[7]。

通过上述步骤即可完成对于地下管线运维数据传输可信路径的查找与筛选处理。通过采用递归的方式对当前节点的邻居节点进行查找,并将其放入堆栈中,构建出传输路径矩阵。并结合相邻路径之间的节点相交情况,对路径可信度进行计算,从而筛选出安全程度较高的传输路径。

1.2 运维数据同态加密处理

考虑到本文构建出的数据安全传输机制需要对数据进行加密处理,因此在筛选出可信传输路径后,本文结合同态算法,对运维数据进行加密处理。在数据加密开始之前需要进行初始化处理,并对数据字节进行转换,具体转换表达式为

$$p',q'=\begin{cases}\delta^{+}[p,q], & \text{加密操作}\\ \delta^{-}[p,q], & \text{解密操作}\end{cases} \tag{3}$$

其中,p 和 q 分别代表需要加密以及解密处理的地下管线运维数据信息字节,δ^{+} δ^{-} 代表密盒正向操作以及逆向操作,p',q' 代表字节转换结果。通过上述公式,可以将地下管线运维数据的字节分别进行正方向处理以及反方向处理,从而实现字节加解密处理[8]。为提高加密的安全效果,本文针对数据的待加密数据进行位移操作。将输入数据作为一个固定大小的字节矩阵进行处理,例如4×4的字节矩阵[9]。在第一行不变的基础上,将剩下行逐一向左侧移动不同数量的字节。具体行位移计算公式为

$$\begin{Bmatrix}p_0\\p_1\\p_2\\p_3\end{Bmatrix}=\begin{Bmatrix}p_{0,e}\\p_{1,e+1}\\p_{2,e+2}\\p_{3,e+3}\end{Bmatrix} \tag{4}$$

其中,e 代表字符串长度。那么数据解密对应的行位移计算公式为

$$\begin{Bmatrix}p_0\\p_1\\p_2\\p_3\end{Bmatrix}=\begin{Bmatrix}p_{0,e}\\p_{1,e-1}\\p_{2,e-2}\\p_{3,e-3}\end{Bmatrix} \tag{5}$$

通过上述步骤即可完成对于运维数据的同态加密处理,通过结合密盒的正向操作以及逆向操作,对运维数据信息字节进行正反向变换处理[10],并结合行位移操作,提高字节变换的扩展性,确保变换操作能够扩散到影响整个状态,提高数据加密效果[11]。

1.3 安全传输机制搭建

针对上述加密完成后的运维数据,本文结合区块链技术,通过对区块宽度进行定义,从而实现区块连接操作,并采用加密函数对待传输区块进行加密处理,实现地下管线运维数据的安全传输[12]。

假设在运维数据通信网络中,D 代表区块链宽度,那么可以对区块宽度进行如下定义。

$$D=\{i(x,y)\mid x\in I_1\cap I_,y\in I\} \tag{6}$$

其中，$i(x,y)$ 代表地下管线运维数据传输可信路径中的主区块，x 和 y 分别代表该区块下的横纵坐标，I 代表通信网络拓扑结构中的区块集合，I_1 和 I_s 分别代表已被验证过的区块以及待选区块[13]。以可信度较高的通信路径中心作为节点，对运维数据通信网络中传输区块加密函数 H，计算公式为

$$H = \frac{D}{2\Delta f}\sum_{i=1}^{N}\frac{|f_0 - f_1|^2}{e_i} \tag{7}$$

其中，Δf 代表统计时间内密钥区块的信息变化量，f_0 代表待传输数据的密文，f_1 代表数据明文，e_i 代表信息数据转化量。通过上述步骤，可以采用统一密钥的形式，对所有待传输的区块进行加密处理。由此，本文构建出的运维数据传输机制如下图所示。

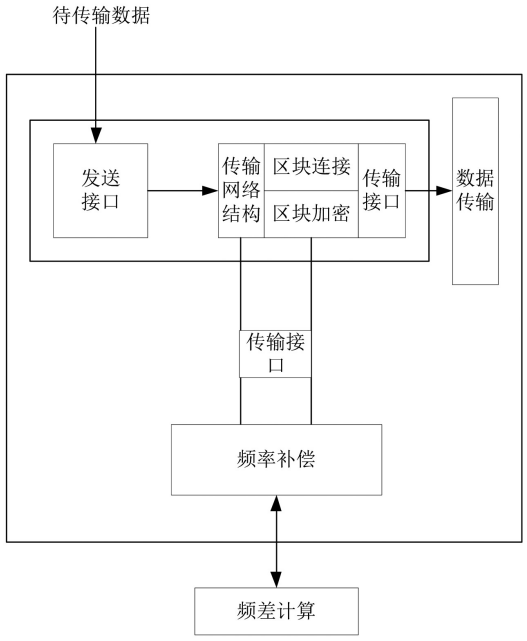

图 1　基于区块链技术的地下管线运维数据安全传输机制

Fig. 1　The secure transmission mechanism of underground pipeline operation and maintenance data based on blockchain technology

通过上述搭建出的传输机制可以看出，在结合区块连接操作以及区块加密操作实现数据传输的同时，本文还对运维数据在区块之间传递的频率补偿值进行计算，从而保障数据的安全性，t_i 假设代表运维数据信号在多个区块之间的传输时间，g_i 代表中心传输区块对应的载波频率，那么频率补偿值 Q_i 的具体计算公式为

$$Q_i = \frac{g_i}{t_i} \cdot D\cos\alpha \tag{8}$$

其中，α 代表传输信号在不同区块之间的入射夹角。通过上述步骤可以对传输频率补偿值进行计算，并以该计算结果对输出的频率进行补偿，因此可以有效优化数据安全传输效果[14]。

通过上述步骤即可完成对于数据传输机制的有效搭建。通过结合区块加密函数对区块进行加密处理，并结合区块连接以及加密操作实现数据传输，最后采用频率补偿值对输出的数据通信频率进行补偿与优化[15-16]，实现地下管线运维数据安全传输。

2　实验论证

为了证明本文提出的基于区块链技术的地下管线运维数据安全传输方法在实际传输效果方面优于常规的数据安全传输方法，在理论部分的设计完成后，构建实验环节，对本文方法的实际传输效果进行检验。

2.1　实验说明

为验证本文提出的基于区块链技术的地下管线运维数据安全传输方法在实际传输效果方面的优越性，本次实验选取了两组常规的数据安全传输方法作为对比对象，分别为基于边缘计算的数据安全传输方法，以及基于共识机制的数据安全传输方法。通过构建实验平台，采用三种传输方法对同一个地下管线运维数据集进行模拟传输，对比不同方法的实际传输效果。

2.2　实验对象

本次实验以某省的地下管道修建项目作为数据获取源，通过对该项目中的地下管线运维数据进行调取，从而构建出本次实验所需要的数据集。空间数据包括各类管线、管段、管件以及地面设施的空间位置和形状信息。属性数据涵盖了丰富的管线特征信息，如管线点点号、管线点平面坐标、地面及管顶或管底高程、管线点类别及特征、管线材质、管径或横断面、管线连接关系、埋设年代、权属单位等。管线类型数据包括排水、燃气、工业、给水、热力、电力和通信等各类地下管线的详细信息。每种管线类型均有独立的数据子集，以便进行针对性地分析和处理。运行状态数据包括管线的流量、压力、温度等实时监测数据，以及故障报警、维护记录等运维信息。对此，本文针对上述数据进行了分类整理，从而构建出了实验数据表，具体数据表形式如下所示。

表 1　实验数据表结构

Tab. 1　Experimental data table structure

字段名	类型	描述
sender id	string(20)	发送方 ID
receiver id	string(20)	接收方 ID
time	number(4)	数据传输时间
divide method	number(1)	数据分片传输方式
file name	string(250)	原始传输文件名
identification	number(4)	唯一标识发送方的待发送文件
group num	number(4)	冗余分组传输数量
group sn	number(4)	冗余分组传输序列号
group content	number(4)	冗余传输分片数据
group data length	number(4)	冗余传输分片长度

本次实验采用的区块链平台为 Hyperledger Fabric 2.3，作为区块链底层技术，支持智能合约的执行和数据安全传输。开发环境为 Python 3.9，同时利用 Postgre SQL 13 数

据库存储和管理地下管线运维数据。同时配备 Redis 6.2,作为缓存层,加速数据读取速度。在采用本文方法对运维数据进行模拟安全传输时,需要对本文算法的参数进行配置,具体配置情况如下表所示。

表 2 本文算法的参数配置

Tab. 2 Parameter configuration of the algorithm in this article

参数	参数配置
传输路径模拟总数/条	100
可信度筛选阈值 φ_{D_i}	0.75
字符串长度 e	0.15
验证区块数量 I_1	150
待选区块数量 I_s	100
密钥区块信息变化量 Δf	1 500
运维数据信号在不同区块之间的传输时间 t_i	0.5 s

通过采用上述参数对本文算法进行配置,并进行模拟传输分析。待实验完成后,对三种传输方案下的运维数据传输结果进行记录,从而实现实验传输效果的有效对比分析。

2.3 传输效果对比

本文方法通过对信噪比进行调整,从而模拟实际传输过程中的干扰成分,由此可以得到本文方法在不同信噪比条件下的数据丢包率结果如下图所示。

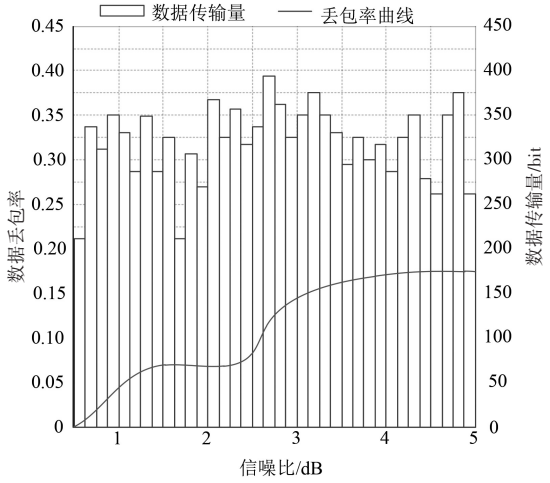

图 2 不同信噪比下数据丢包率结果

Fig. 2 Data packet loss rate results under different signal-to-noise ratios

通过上述实验结果可以看出,随着信噪比的不断增高,数据丢包率越来越高。但从数据丢包率的整体波动范围来看,本文传输机制下,运维数据的传输效果较好,数据丢包率不超过 20%。

此外,为提高实验结果的对比性,将文献[3]所提基于数据加密和身份控制的安全传输方法文献[4]所提基于 SSL 和国密算法的安全传输方法作为对比方法,与本文方法共同进行实验。本次实验以运维信息数据泄露规模作为对比指标,对不同数据安全传输方法的安全传输性能进行衡量,该值可以通过将数据接收端以及发送端得到的数据量进行作差求得,具体实验结果如下表所示。

表 3 运维信息数据泄露规模

Tab. 3 Scale of operation and maintenance information data leakage

实验次数	泄露规模/bit×10³		
	本文方法	文献[3]方法	文献[4]方法
1	2.5	5.8	6.5
2	2.3	5.4	6.2
3	2.4	5.2	6.8
4	2.8	6.1	6.4
5	1.5	5.8	7.1
6	1.6	5.4	7.0
7	1.8	5.7	7.5
8	1.4	6.3	7.8
9	1.2	6.0	7.4
10	2.3	5.4	7.5
11	2.7	4.8	7.2
12	2.6	2.9	7.1
13	2.5	6.1	6.8
14	1.2	6.4	6.5
15	2.0	5.4	6.6
16	2.1	5.2	4.5
17	2.1	5.0	5.4

通过上述实验结果可以看出,在针对不同规模的数据进行模拟传输时,不同方法的实际安全效果也有所不同。通过数值上的对比可以明显看出,本文提出的基于区块链技术的地下管线运维数据安全传输方法在实际传输效果方面明显优于两种文献传输方法,数据泄露规模更小。

3 结论

本文所提出的基于区块链技术的地下管线运维数据安全传输方法的研究,不仅是对现有数据传输安全性的一次重要提升,更是对未来智慧城市建设中关键基础设施安全保障的积极探索。通过本方法的研究与实施,能够有效解决地下管线运维数据在传输过程中面临的安全隐患,确保数据的完整性、真实性和不可篡改性,从而为城市基础设施的安全稳定运行提供有力支撑。

参考文献

[1]殷莉, 陈益均. Present 算法下机房数字化信息安全传输仿真[J]. 计算机仿真, 2023, 40(12):300-303, 347.

[2]BARAKAT M T, ALQADI Z A. Highly secure method for secret data transmission [J]. International Journal of Scientific Engineering and Science, 2022(6):49-55.

[3]孔庆阳, 何乐生, 金浩男, 等. 体测设备物联网数据安全传输机制的设计与实现[J]. 计算机应用, 2022, 42(S2):180-185.

[4]代乾坤. 基于 SSL 和国密算法的安全传输系统设计[J]. 计算机应用与软件, 2023, 40(2):326-330.

(下转第 165 页)