

# 基于 5G 技术的高校智慧图书馆通信数据加密方法<sup>①</sup>

林团娇

(福州工商学院, 福建福州, 350017)

**摘要** [目的] 由于传统数据加密方法加密不稳定, 安全性差, 为此本文提出基于5G技术的高校智慧图书馆通信数据加密方法。[方法] 该方法首先设定多种加密等级和文字编码, 调整编码生成序列, 对数据预处理并进行加密节点的布设。然后将接收到的加密信息安全储存在基于5G技术的多节点通信网络数据模型中; 最后调整接口之间的频差, 计算丢失补偿值, 由此完成通信网络数据加密传输。[结果] 实验结果表明, 运用本文方法雪崩效应系数均在临界值以下, 加密稳定性和安全性强。[结论] 本文设计方法在大量用户在线情况下, 能够安全、稳定地实现数据加密。

**关键词** 5G; 智慧图书馆; 数据加密

## Communication Data Encryption Method for University Smart Library Based on 5G Technology

Lin Tuanjiao

(Fuzhou Technology and Business University, Fuzhou, Fujian, 350017, China)

**Abstract** [Purpose] Because the traditional data encryption method is unstable and the security is poor, this paper proposes a communication data encryption method of university smart library based on 5G technology. [Methods] Firstly, this method sets a variety of encryption levels and text codes, adjusts the code generation sequence, preprocesses the data and arranges encryption nodes. Then the received encrypted information is safely stored in the multi-node communication network data model based on 5G technology; Finally, adjust the frequency difference between interfaces and calculate the loss compensation value, thus completing the

①本文系 2021 年度福建省中青年教育科研项目基金项目“基于 5G 技术下的高校智慧图书馆建设研究”(项目编号: JAT211025)的研究成果之一。

encrypted transmission of communication network data. [ **Results** ] The experimental results show that the avalanche coefficient of this method is below the critical value, and the encryption stability and security are strong. [ **Conclusions** ] The method designed in this paper can realize data encryption safely and stably when a large number of users are online.

**Keywords** 5G; Smart Library; Data Encryption

## 1 引言

随着现代化社会的快速发展,开放式网络环境中存在较多安全隐患。为了保障通信信息在传输过程中的安全性与实时性,本文提出了通信数据加密方法对数据进行加密<sup>[1]</sup>。对于高校智慧图书馆系统来说,该系统在单独组建的局域网中,具有独立的网络线路,需要实施加密处理,采用公钥和私钥联合使用的方式来保护用户信息。通过数据加密,服务器可以更快地为用户提供接口支持,并减少外来威胁侵入网络、诈骗或窃听等攻击行为,防止黑客入侵对用户数据进行非法操作。此外,实施有效的加密算法可以增加系统的可靠性。

在现阶段的网络通信中,使用数据加密技术可以避免传输层加密节点处受到攻击。在不同节点的数据通信模型中进行加密时,需要将通信信息以明文形式传输,从而避免数据节点遭受外部攻击<sup>[2]</sup>。在信息传输过程中,如果服务器发生故障,则需要及时对通信数据进行加密,以防止信息丢失的情况发生。加密技术可以通过身份验证等方法,精准识别身份信息,提高加密技术的有效应用,保障计算机网络安全。

由于设计及配置缺陷导致大量网络安全漏洞的存在,加上海量数据使得安全性降低,易受攻击者和病毒的影响,从而产生安全性问题,影响用户操作,并导致通信数据的受损和丢失,使得预期结果无法实现<sup>[3]</sup>。因此,在当前阶段,本文以高校智慧图书馆通信数据加密方法为研

究对象,运用 5G 技术并结合实际情况进行实验与分析。

## 2 高校智慧图书馆通信数据加密

### 2.1 高校智慧图书馆通信数据加密预处理

为了提升高校智慧图书馆系统中的加密效果并确保通信数据安全性,文章对数据预处理。根据数据的类型和应用区域不同,设定多种加密等级,并形成对应的文字编码<sup>[4]</sup>。首先将多层级的通道脑电信号按照加密预处理的顺序进行分割,分割成块后再进行变形重组;然后将其与执行处理平台进行关联,形成灰度混淆帧结构。在考虑相关性的应用效果下,调整编码生成序列以及对应的长度;同时在不确定的网络环境之下,对数据进行限制和加密,完成预处理。在完成对网络通信数据线性加密预处理后,文章需要进行单项重组加密结构的多项设定。单项重组加密结构可以根据通信数据的加密层级设置动态目标,并计算出重组单值,具体计算公式为:

$$H = s - \frac{1}{a} \quad (1)$$

公式中: $H$ 为重组单值; $s$ 为信息熵; $a$ 为重置系数。根据计算的重组单值,可以划定信息熵的架构,并确定加密协议的信息等级,不同的加密等级对应的加密目标也是动态的,它们可以根据通信数据量的变化做出相应的更改和调整<sup>[5]</sup>。为了满足网络通信数据的传输途径以及覆盖区域,需要设定基础性的加密节点,这些节点作为基础核心节点,具有较强的

主控性, 它们是加密层级的核心。采用改进 MD5 算法, 计算加密核心节点的细粒度, 其计算公式为:

$$s = \frac{t-1}{2} - u \quad (2)$$

公式中:  $S$  为加密核心节点的细粒度;  $t$  为重组距离;  $u$  为应变加密极限值。将动态的加密目标设定在内部的加密结构中, 并布设辅助加密节点周围的核心加密节点, 以形成相应的加密覆盖范围。通过增加或减少细粒度, 在合理的范围内对每个动态的加密目标进行调整, 从而完成加密节点的布设。

## 2.2 建立 5G 技术的多节点通信网络数据模型

在高校智慧图书馆通信数据加密预处理结果的基础上, 建立多节点通信网络数据模型, 使用 D2D 通信连接 5G 网络。在 D2D 通信模式下, 对系统用户的控制认证, 用户就可以进行直接通信, 提升通信速率。将  $s$  设置为私钥, 公共信息设定为  $J$ ,  $G = \{x_i, y_i, z_i, k_i\}$  为安全信息  $c$  的签名。通信数据根据签名  $G$  来检测安全信息  $c$  是否可信, 为了验证签名  $G$  是否成立需要对其进行检验<sup>[6]</sup>。如果成立, 则说明  $c$  可信。如果不成立则说明签名  $G$  将受到攻击, 并传输错误通信数据。当收到错误信息后, 得到攻击者的身份信息; 然后随机选择一些已知用户参数的通信数据并计算。在高校智慧图书馆系统发送请求后, 系统会生成一系列的匿名证书和私钥。为了向云端上传信息, 系统会建立新的标签。当系统收到一段含有标签的信息时, 云端会保存该信息。使用对称加密的密钥对信息进行加密, 并将加密后的信息发送到高校智慧图书馆系统中<sup>[7]</sup>。系统将加密信息传输到用户注册通信数据, 这样只需明确通信数据的真实身份, 而不考虑匿名证书。为了防止通信数

据的匿名证书被模仿网络攻击, 将接收到的信息存储在一个防篡改模型中, 提供安全储存加密信息和敏感数据的安全储存, 并保护加密运行。

## 2.3 多节点通信数据加密传输

在 VPI 组网中, 由于不同节点的接收精度不同, 信号接收与发送的通信数据会产生相应的频差, 导致多节点通信网络中的数据丢失<sup>[8]</sup>。为了解决这个问题, 在数据处理过程中, 文章利用相对运动时间内一致信号的相位误差值来计算接收信号的频差, 以实现不同接口信号的同步。在多节点通信数据加密传输中, 利用收发两端接口对数据信号进行一致性处理。

在 VPI 组网环境下, 高校智慧图书馆系统可以获取不同接口之间通信数据产生的信号频差值。在接收到多余信号的同时, 系统可以对传输过程中的信号值进行补偿, 以避免数据信息的丢失或破坏, 并提高传输过程中的安全性和实时性。数据传输时, 不同接口间的各个节点运行状态保持一致, 设  $k$  为多节点通信数据间的丢失补偿值, 在信号同步的环境中, 其补偿值的计算公式表示为:

$$k = \frac{k_a}{r} \times S \times \cos\theta \quad (3)$$

公式中:  $k_a$  为中心节点的信号接收频率;  $r$  为数据信号在多个节点内传输的一致性时长;  $\theta$  为信号节点的移动变化角<sup>[9]</sup>。计算多节点通信数据的补偿值, 得到在加密传输过程中, 所产生的丢失数据情况并进行补偿。在高校智慧图书馆通信信号传输一致时, 完成多节点通信网络数据的加密。

## 3 实验测试与分析

### 3.1 搭建实验环境

实验搭建网络环境过程中, 将主机和采集装置连接到集线器中, 获取主机上生成的通信

数据集并记录到 SQL 中。其中，设备参数配置如表 1 所示：

表 1 参数配置

项目	配置信息
CPU型号	Intel酷睿i6
运行内存	128G
机身内存	128G
操作系统	Windows11

通过对数据集的分析，得出在网络系统中通信信息情况，并整理信息，归纳分析记录在数据库中。工作人员通过整合数据信息来进行通信数据的加密传输实验，在实验过程中使用两台操作主机采集获得的通信数据。由公私钥对生成后的信息进行签名，然后验证通信网络对称加密传输信息，将得到的信息发送到主站系统中。同时虚拟机环境需要配置 Ubuntu8

的 Openssl 开源软件算法库及其他测量设备。

### 3.2 测试与分析

为了测试高校智慧图书馆应用本文方法后数据加密方法的应用性和有效性，进行测试实验。以某高校智慧图书馆为例，提取高校智慧图书馆系统中用户最近一月使用系统的相关数据为实验对象，得到相关用户数据。实验所运用的用户通信数据如表 2 所示。

表 2 用户通信数据

用户	用户端IP	借读书数量/本
1	192.168.2.3	5
2	192.168.2.4	10
3	192.168.2.5	9
4	192.168.2.6	7
5	192.168.2.7	4

在智慧图书馆系统中，为了方便管理员对用户需求进行服务并及时处理借阅与归还图书事务，有部分用户数据以半公开方式显示在系统终端上。为此，通过检测高校智慧图书馆用户端 IP 地址的方法来进行用户通信数据窃取。在借阅图书后，将通信数据加密方法集成到智慧图书馆系统终端中，并利用雪崩效应法进行测试。该测试将用户端所有通信数据统计合成一个数据集，并在理想状态下观察加密后的数据集在终端中是否出现异常波动。若出现异常

波动，表示用户端存储的所有数据可能存在崩塌的风险，并且风险发生的概率较大。为了获得更准确的测试数据，我们使用雪崩效应的效应系数值来衡量其效果。同时，对使用系统的用户身份信息进行加密处理，以确保数据安全。其中效应系数计算公式为：

$$D=\frac{2^n-1}{1+2^r} \quad (4)$$

公式中： $D$  为雪崩效应系数； $n$  为用户端通信数据的大小； $r$  为数据的排布表达式。本

文设置三个小组,实验组应用本文方法,对用户端通信数据进行加密处理,对照组 1 和对照组 2 将应用传统方法进行加密处理。实验将收集并处理这些数据,以应用系统通信作为加密方法的起始标识。在应用人数达到 5000 人时,实验将测试系统中用户通信数据加密方法的应用效果。同时,实验设定一个雪崩效应的临界

值为 0。当用户端通信数据的雪崩效应系数超过该临界值时,实验将认为系统中用户个人通信数据的安全性较低,并存在一定程度上的威胁风险,甚至可能发生通信数据被盗取的情况。持续进行测试,直到系统应用人数超过 50000 人为止。同时,实验将根据在线人数的变化计算其效应系数,并将结果呈现如图 1 所示:

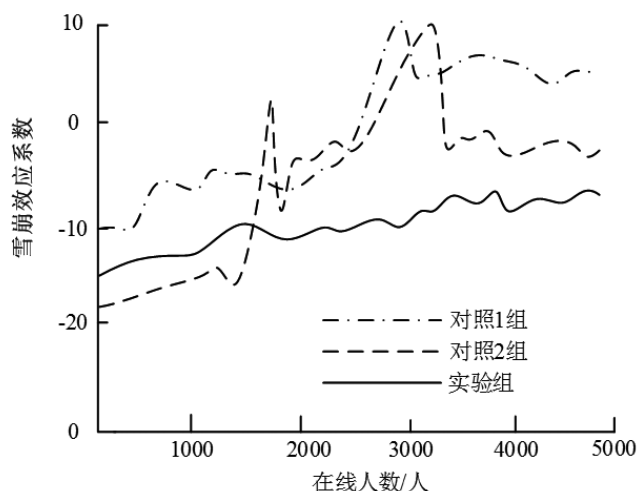


图 1 对比结果

根据图 1 可知,对照组的雪崩效应系数在不同的在线人数下均超过了临界值,说明对照组在对用户端通信数据进行加密处理后,出现了雪崩效应,特别是对照组 2 在 2000 人和 3200 人在线时,由于人数过多,终端对于用户通信数据的处理存在漏洞,加密过程不稳定,导致安全性较差。相比之下,实验组的雪崩效应系数都在临界值以下,并且随着在线人数的增加,保持相对稳定的增加趋势,表明本文方法能够在不同程度上较好地对用户的通信数据进行加密。尤其在大批量用户同时在线的情况下,能够确保用户通信数据的安全性,提升智慧图书馆的应用性和用户数据的安全性,实现了加密方法的有效应用。

## 4 结语

本文从高校智慧图书馆问题入手,提出了基于 5G 技术的高校智慧图书馆通信数据加密方法。该方法对传输数据进行实时挖掘和识别,增加了通信过程中数据的有效性,优化了加密方法。但该方法中还存在一些不足,例如在构建传输环境过程中存在不确定因素问题、数据存储中的双向传输问题,以及密钥的安全性问题等。今后应更加完善计算,通过有效生成随机数,寻找最优加密方法,得到传输数据策略,减少数据冗余,挖掘更多的通信数据加密的可能性。通过分析并处理通信数据的加密方法,保障传输中的安全性与实时性。改善与应用 5G 技术,实现高校智慧图书馆通信数据加密方法的深入研究。



## 参考文献

- [1] 李强. 新一代人工智能+5G技术环境下的智慧图书馆新生态[J]. 图书馆理论与实践, 2021(3): 52-57.
- [2] 刘海宁, 张少卿, 鄂思宇. 基于5G技术的航空机载系统无线通信应用[J]. 航空学报, 2022, 43(12): 459-467.
- [3] 贾飞侠. 5G通信技术助力智慧校园建设的应用研究[J]. 电视技术, 2022, 46(11): 225-228.
- [4] 王敏. 基于5G网络技术的智能收割通信系统优化[J]. 农机化研究, 2023, 45(3): 232-236.
- [5] 孙阳盛, 涂崎, 赵中华, 等. 基于5G及IEC61850的韧性配网故障信息智能传输技术研究[J]. 电力系统保护与控制, 2022, 50(21): 108-117.
- [6] 杜蕾, 左昊明, 李亚设. 基于Citespace的国内智慧图书馆近十年发文热点及前沿剖析[J]. 图书馆理论与实践, 2021(6): 42-49.
- [7] 龚利, 赵延杰, 朱明辉. 一种基于北斗和5G技术融合的复杂环境下机车定位方法[J]. 北京交通大学学报, 2021, 45(2): 44-51+70.
- [8] 王云弟, 王文韬, 谢阳群, 等. 融合5G的高校图书馆智慧学习服务体系构建[J]. 图书馆理论与实践, 2021(2): 85-90.
- [9] 张晖, 余蕊, 张宁池, 等. 基于5G通信的智能配电网改造经济性综合评估方式[J]. 科学技术与工程, 2021, 21(25): 10746-10754.