文章编号:1671-4598(2024)09-0163-07 DOI:10.16526/j.cnki.11-4762/tp.2024.09.023 中图分类号:TP393 文献标识码:A

基于窄带物联网的铁路通信网络安全加密控制系统设计

邵瑞强[1,2]
(1. 国能朔黄铁路发展有限责任公司，山西 原平 034100；2. 北京交通大学，北京 100044)

摘要：铁路通信网络在数据传输过程中容易受到网络攻击，降低网络的安全性；为了解决这个问题，设计了基于窄带物联网的铁路通信网络安全加密控制系统；以STM32F103为窄带物联网的控制终端芯片，用于采集、处理和分析数据，通过控制终端与人机接口，使用USART实现计算机的下载及调试，设计接口数据传输电路，采用拨码开关电路完成输入端电流信号和电压信号的切换，并通过调整电阻尺寸来校正输出电压，实现数据的高效传输；应用窄带物联网加密技术，确保每个子机构都具备唯一的属性密钥，结合AES加密算法将数据加密成密文，通过逆变换、解密处理，获取噪声相位，避免乱序密文影响子密文排序，实现通信网络安全加密控制；由系统测试结果可知：所设计系统信道误码率最大值未超过30%，网络吞吐量最大值为260 bit/s，具有高效加密控制能力。

关键词：窄带物联网；铁路通信网络；安全加密控制；AES加密

Design of Railway Communication Network Security Encryption Control System Based on Narrowband IoT

SHAO Ruiqiang[1,2]
(1. Shuohuang Railway Development Limited Liability Company, Yuanping 034100, China;
2. Beijing Jiaotong University, Beijing 100044, China)

Abstract: Railway communication network is prone to network attacks during data transmission, which reduces the security of the network. To address this issue, a railway communication network security encryption control system based on the narrowband Internet of Things was designed. Using STM32F103 as a narrowband IoT control terminal chip, it is used to collect, process, and analyze the data. Through the control terminal and human-machine interface, USART is used to download and debug the computer, and design the interface data transmission circuit. The input current signal and voltage signal are switched by using a dial switch circuit, and the output voltage is corrected by adjusting the resistance to achieve efficient data transmission. The narrowband IoT encryption technology is applied to ensure that each sub organization has a unique attribute key. Combined with AES encryption algorithm, the data is encrypted into the ciphertext. Through inverse transformation and decryption processing, noise phase is obtained to avoid disordered ciphertext affecting the sorting of sub ciphertext, and achieve the communication network security encryption control. Testing results show that the maximum channel error rate of the designed system does not exceed 30%, and the maximum network throughput is 260 bit/s, which has efficient encryption control capability.

Keywords: narrowband IoT; railway communication network; security encryption control; AES encryption

0 引言

为了提高网络通信水平，需要在保证电信安全的前提下，参考计算机网络安全防护技术，着重加强运营支持系统，强调网络和数据安全，从而逐渐地构建起了铁路通信网络的技术标准体系。铁路通信网络是一个由承载网络、业务网络和支撑网络组成的专用网络，其中包含大量的列车运行信息、乘客个人信息、信号灯控制等敏感信息，伴随着通信系统的不断发展，通信系统的建设和运营变得越来越复杂，铁路通信网络可能面临网络攻击，如黑客入侵、恶意软件传播、拒绝服务攻击等，这些攻击可能导致列车功能异常、交通事故，甚至威胁旅客安全，这就要求通信系统具有一定可视化、可管性、可控性和可测量性。随着各种服务的广泛使用，对通信网络的负荷要求越来越高，其安全保护范围也越来越大。当前，在铁路通信网的运行和管理过程中，还没有一套系统、规范的安全策略，为此，需要研究一种铁路通信网络安全加密控制系统，以保障铁路通信网络的安全运行。

文献[1]设计了一种基于卷积神经网络的安全控制系统，该系统以WSN为研究对象，通过建立WSN的卷积神经网络建模，参照KDDCup99数据，对WSN的安全性进

收稿日期:2023-08-31； **修回日期**:2023-10-16。
作者简介:邵瑞强(1981-),男,大学本科,工程师。
引用格式:邵瑞强.基于窄带物联网的铁路通信网络安全加密控制系统设计[J].计算机测量与控制,2024,32(9):163-169.

行评价。文献［2］设计了基于区块链匿名属性的加密系统，该方案采用了一种隐蔽方法，即由两个参与方合作产生完备的属性密钥，然后再对该密钥进行相应的属性比较。然后，利用区块链生成和存储的属性证书，对随机指示方式下的密文和明文两种不同类型的密码进行安全评估。文献［3］设计了基于国产密码 SM2 的加密系统，通过将已有的 SM2 公钥加密方法与 Broadcast 加密方法有机融合，采用 Diffie-Hellman 密钥互易与多项式密钥共享的思路，以最大限度地保持原来的 SM2 公钥加密方法，对其进行简单扩充，以达到多用户环境下信息安全 Broadcast 的自治与可控。

但目前的网络安全加密控制技术只能实现环路级别的信息采集和控制，不能实时准确地监控轨道交通信息，也就无法实现信息的智能化监控和精细化管理。而窄带物联网是一种低功耗、宽覆盖、高连接密度的无线通信技术，可以在复杂的环境中实现可靠的通信，专门用于支持物联网设备的快速、可靠的互联。为此，设计了基于窄带物联网的铁路通信网络安全加密控制系统。

1 基于窄带物联网的加密控制系统总体结构设计

窄带物联网是 5G 标准中的一项，它是为大型物联网而开发的一项低能耗的广域网技术，而在铁路通信过程中，基于安全加密的身份验证是一个十分关键的体系。按照现有方法，可以通过使用者的生物特征和身份证件，实现对铁路通信网络安全加密的用户身份验证。这种验证方式属于窄带物联网验证方式，在现有的基于地面的分布式系统中，由于用户的通信数据都是以单一的方式分散于整个网络，使得该系统的可靠性面临较大的挑战[4]。黑客能够通过对整个安全体系的使用者可信性进行攻击来获取使用者的通信数据，这对于使用者的身份认证带来极大的安全性危险，黑客也能够通过伪造某些假的身份数据来对使用者的通信网络环境进行实时监视[5]。基于窄带物联网的加密控制系统总体结构如图 1 所示。

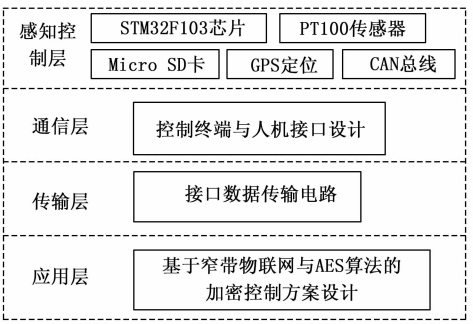

图 1 基于窄带物联网的加密控制系统总体结构

图 1 中，感知控制层主要负责对铁路通信网络信息进行采集和处理，通信层通过设计控制终端与人机接口实现通信，传输层通过设计接口数据传输电路，实现了应用端和设备端之间的连接，应用层基于窄带物联网与 AES 算法实现加密控制系统的开发与设计[6]。将每个模块和后台数据库的连接起来，从数据库中访问数据，从而可以在移动电话端对通信状态和周围环境参数进行实时查询[7]。如果发现有异常情况，就会自动地向用户发送报警信息，并作出相应提示，同时还可以远程控制加密动作。

在窄带物联网的加密控制技术基础上，用户可以随时利用加密证书来查询加密过程和内容。基于窄带物联网，利用数据查询的方式，将公共密钥保存到数据库中，与加密算法相结合，就能实现加密证书的注册、更新、加密等一系列工作的顺利进行，从而确保在窄带物联网中的数据不可修改性[8-10]。加密算法可以完全封闭地对历史数据存储空间管理，在不对整个网络内容下载情况下，可以实现对整个网络加密查询和校验[11]。由于在窄带物联网中，数据查询的记录是向所有用户开放的，所以数据查询不能很好地用于公有互联网中，由此保证了铁路通信网络的安全。

2 加密控制系统硬件结构设计

由于信道高度的差异和覆盖范围的差异，可能会影响到铁路通信的安全性。为此，设计了基于窄带物联网的安全加密控制系统硬件结构。

2.1 窄带物联网控制终端设计

窄带物联网的体系架构包括一个窄带物联网终端和一个基站分组核心网络，在充分考虑到窄带物联网终端的硬件结构基础上，该系统采用了物联网专用的网络接口协议，实现了与物联网网络的数据传输[12]。考虑到联机管理平台和工业系统的功能相对较强，同时考虑到代管和安全等因素，所以使用 HTTP/HTTPs 作为联机管理平台和工业系统的接口。

以 STM32F103 为窄带物联的终端机，根据相应的 AT 命令，完成终端机数据的采集、处理和分析，并与无线传感器网络中的无线传感器网络模块进行通信。窄带物联网模块通过 JTAG 调试方式，可实现全局带宽，并可为其提供大量的外围接口及网络协议栈[13]。该终端能将各种数据量如开关量、数字量、模拟量等与 GPS 信号相结合，并通过 SPI、ADC 等方式连接。窄带物联网控制终端结构如图 2 所示。

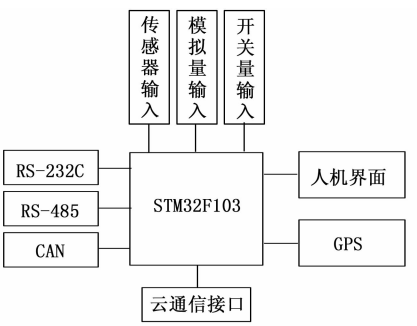

图 2 窄带物联网控制终端结构

在数据传输方面，采用了 RS-232C、RS-485、CAN 等总线通信模式，以太网通信可以与互联网相连，也可以与 4G 移动路由器相连，达到云端上载的目的。信号控制输出包括了 4 个 4～20 mA 的模拟量和 16 个开关量，使用了大容量的 SD 卡来储存数据，并保存系统相关参数，通过将相应文件

系统迁移到 SD 卡上[14]，便于执行 SD 卡的读取和写入。

窄带物联网控制终端，主要包含以下几个部分。

1）STM32F103 终端微控制芯片：

STM32F103 是一款 32 位、中、低级别 ARM 单片机，由意法公司生产，核心为 Cortex-M3，是一款 32 位 ARM 单片机。它是连接数据采集部分和数据传输部分的一座桥梁，其工作内容有：对部分采集的数据进行运算和处理，对显示模块的运行，对数据的存储，与服务器远程通信，对 GPS 信号处理，实现定位和授时，输出报警信息，与上位机进行数据交换[15]，实现系统参数标定。

2）信号采集：

系统的采集输入信号包括 8 路 PT100 温度传感器、16 路开关量、8 路 4～20 mA 模拟量，可以对控制电路在实际操作过程中所遇到的基本参数信息进行模拟，使用多路参数并行采集方式，可以提升采集速率。

3）数据存储模块：

通过对大容量 Micro SD 卡中所储存的信息进行处理，实现了当系统出现故障时，它是被即时还原的。SD 卡小巧、易于操作、数据不容易丢失[16-17]，在系统出现问题时可以保证数据的完整。

4）GPS 定位授时：

在发生故障时，能及时准确地得到故障点的定位信息，为故障点的报警和报警提供技术支援[18]。利用 GPS 模组进行定位及授时，服务器可以迅速地获得系统位置和时间信息，从而可以对系统运行状况及时调整。

5）CAN 总线：

对于信号量较多的控制现场，单个的监控线路无法实现对这么多信道的实时监控，所以就必须采取多台设备的连接，即一主多从，从设备将经过 CAN 总线的数据传送给主设备，并对其集中管理[19]。CAN 总线是一种高度可靠的设备，它是一种可以把安装在它上面的全部控制信道连接起来的线路，形成局部网络，增强设备直接控制能力，有效提高了系统控制电路的综合判定和响应速度。

2.2　控制终端与人机接口设计

控制终端与人机接口主要包括了按钮、OLED LCD 显示屏、多功能串口接口 3 个部分，这些部分可以实现对软件编程、设备状态信息进行实时显示。该接口具有低功耗和宽工作电压特点，并与主机以 IIC 模式进行通信。设计的控制终端与人机接口，如图 3 所示。

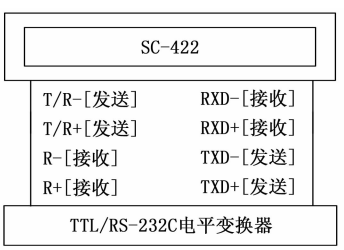

图 3　控制终端与人机接口

STM32F4 包括 4 个通用同步/异步串行通信接口 USART 及 2 个通用异步串行通信接口，一般的串行通信接口为 TTL/RS-232C 的电平变换器，而只有 USART 可用来进行程序的下载，所以使用 USART 来实现计算机的下载及调试[20]。RS-232C 通信模块主要起到了系统参数标定、数据显示和 IAP 数据下载的作用。

1）系统参数标定：

系统启动前，先对温度、模拟量的输入、输出进行校准，将 STM32F103 终端微控制对应的管脚设定为最低，在系统上电后，通过编写计算机校准软件和编写通讯协议，来完成参数校准，并将其存储在芯片中。对上述参数进行标定后，将系统关机，将管脚硬件调高，重新通电后，进入正常工作模式。

2）数据显示：

当该系统在工作状态下，将会把每一个模块的初始化的数据都会被输出出来，同时，该数据还会与 RS-232C 接口计算机直接通信，以方便操作者实时观测，并能实时地显示出系统参数。在系统调试时，采用 RS-232C 通信协议，将整个系统工作情况直接传送给计算机，便于软件调试。

3）IAP 数据下载：

本系统运行时，将各模块初始化值全部输出，并将这些值与 RS-232C 接口 PC 通信，便于操作人员观察，并可对系统各项参数实时显示。在系统测试过程中，利用 RS-232C 通信方式，将测试结果与上位机进行了实时通信，方便了对软件的测试。

2.3　接口数据传输模块设计

接口数据传输模块由两个部分组成，一是数据收集部分，二是控制信号的输出部分。数据收集部分使用主控芯片自带的模/数转换器，能够将指定的 4～20 mA 电流信号或 0～10 V 电压信号转换为对应的 0～3.3 V 电压信号，以便主控芯片进行处理。共有 4 路信息数据传输电路，采用拨码开关电路来实现输入端电流信号和电压信号的切换，通过调节电阻大小来校正输出电压。其中接口数据传输电路的工作原理如图 4 所示。

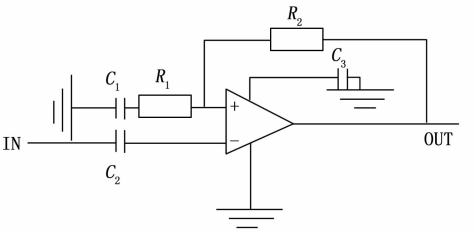

图 4　接口数据传输电路原理图

因为主芯片本身带有数字模拟转换器，所以该控制信号的输出，只需把 0～3.3 V 的电压信号转换为 4～20 mA 的电流信号即可。接口数据传输模块通过使用执行器开度控制模块，基于自锁按钮的驱动电路，实现了对驱动电路的一次切换，并对输出信号进行了修正。通过硬件系统的设计，满足加密控制系统的运行要求，同时为软件功能的实现提供技术支持。

3 基于窄带物联网的加密控制方案设计

窄带物联网软件系统中的加密控制方案的设计过程如下：首先将一个安全参数 α 和一个一般性的属性集合 u 输入到一个窄带物联网，使用这些安全参数来产生一个具有大素数的群组，并将这些群组的生成元和一个大素数作为一个整体的共同参数 G_a。定义了一种双线性图，选取 2 个具有较高的碰撞抵抗力的哈希函数 Hash，用一种随机的语言把一个整体的标识表达式映射到一个群体中。该过程可表示为：$\mathrm{Setup}(\alpha,u)\rightarrow G_a$。

然后通过属性授权机构管理每个子机构的属性，任意选择 2 个指数，作为每个子机构的私钥，可表示为：$\mathrm{Setup}(G_a)\rightarrow S_a$。当使用者存取该系统时，会从一个属性子组织获得一个私有密钥，各子组织将使用该私有密钥来识别各使用者的独特身份，从而产生的各特性密钥为：

$$S_b = g \cdot G_a I^{\beta} \tag{1}$$

式中，g 表示群的生成元；I 表示身份标识符；β 表示选择的指数。

将属性密钥发送给用户后在窄带物联网控制终端上执行属性密钥分配这一阶段，需先在离线阶段上处理一些复杂计算，并将结果存储在终端设备上。

由于铁路通信网络数据属于外派数据，需要结合 AES 加密算法将数据加密成密文后，再传送给另一终端。AES 加密是一种基于 S-盒的加密方法，它通过行移位和列移位把明文以字节的方式传输到译码单元，从而实现了一种新型的对称加密。采用了一种基于关键运算的方法，实现了对信息正确度的自动修复，并为掩模运算提供了一个随机控制序列。该算法使用了可调的线性遮罩来实现系统线性化，并且通过遮罩补偿来对其进行校正，以防止系统输入信号泄露。

在 AES 算法中，S 盒的字节排列运算主要以 S 盒为主导，AES 的 S 盒属于一种乘法反变换结构，它是一种唯一的非线性转换形式，它可以用 S 盒乘法反变换来实现，得出的结果如下：

$$W(S_b) = f[I(S_b)] \tag{2}$$

式中，I 表示逆运算，f 表示仿射计算。

S 盒算法是将一个面积较大的单元划分为若干面积较小的单元，通过对这些单元进行平方和乘法等一系列的变换，使之在面积较大的单元上完成一次乘法逆运算。结合公式(2)，将乘法逆运算进行逆变换处理，得到的处理结果如下：

$$W^{-1}(S_b) = f^{-1}[I^{-1}(S_b)] \tag{3}$$

将（2）与（3）相结合，获得 S 盒乘法逆变换结果，由此实现 AES 算法中的 S 盒变换。

将变换结果作为密码文，得到的子密文可表示为：

$$R_i = W^{-1}(S_b)(S_a \cdot w_i + \gamma_i) + (S_b \cdot w_i + \tau_i) \tag{4}$$

式中，w_i 表示第 i 个待加密数据；γ_i、τ_i 分别表示每个子机构和每个属性对应的噪声数据。

设定铁路通信节点坐标为 $A(x_a,y_a)$，其中 x_a，y_a 分别代表通信链路在网络结构中的信道高度和距离，充分考虑交互通信问题，对窄带物联网结构中的任意节点定义相关坐标，由此计算通信节点与通信链路在同一窄带物联网内的通信节点距离 y_b，计算公式为：

$$y_b = \begin{Bmatrix} y_b \pm jx_a y_a \\ y_b \pm 1 \\ \notin [0,j] \end{Bmatrix} \tag{5}$$

式中，j 表示节点数量。

在通信节点距离 y_b 下，将第 i 个子密文 R_i 映射为乱序密文形式，即 $R_i \xrightarrow{y_b} R'_i$，基于此，得到的有效密文为：

$$R''_i = R_i - y_b R'_i \tag{6}$$

通过距离映射有效密文和乱序密文关系，保证子密文间映射具有一定独立性。

在加、解密的过程中，噪声会逐渐增加，当噪声超过允许值时，会导致全同态信息与实际信息产生偏差。为了避免乱序密文影响子密文排序，需要对密文进行并行加密处理，可表示为：

$$K(R''_i) = \cos(\varphi + \gamma_t + \tau_t) \tag{7}$$

式中，φ 表示调制相位；γ_t、τ_t 分别表示子机构和属性噪声相位。

通过识别再加密的标识符，读出公钥和私钥，将其写入到一个并行加密过程中，然后按顺序进行多项式的分解。经过多次分解，密码文本被不断地修改。为了获得完备的密码算法，首先根据多个敏感属性的特点，对输入信息进行分组，保证无偏移量出现。采用重加密方式，对随机混沌序列进行重新组合，从而获得了网络多敏感属性数据并行重加密结果。将密文加密处理后打包为密文包形式，再通过认证用户操作实现网络的安全加密控制。

4 系统测试

4.1 测试场景描述

在窄带物联网条件下，在铁路通信网络的安全加密控制系统应用中所选取的场景进行了描述，高铁移动通信场景主要包含了高架桥、路堑、城区、隧道、郊区、车站等多种场景，而高架桥和路堑两个场景是最具有高铁特点的复杂电波传播情景，也是高铁移动通信系统应用的一个典型场景。现场测量场景如图 5 所示。

选取一组既包括高架桥梁又包括壕沟的高铁线路，以提高通道测量效率。在壕沟情景中，根据壕沟两侧的壕沟高度，将壕沟划分为高壕沟和低壕沟。整个通道测量的长度大约是 500 米，从高堑线开始，通过高架线到低堑线。其中，山地高裂隙场（长度为 110 m 左右）为地下洞室，洞室外侧与山地洞室相连，为山地地区普遍采用无线通信环境。这座高架大桥的长度大约为 250 m，两边都是比大桥表面更高的小山。低堑景设在高架桥的尾部，长 150 m 左右，两边都是小山。路堑、高架桥和隧道的建设，其目的就是突破地势的制约，构筑稳定的地基，保证高速铁路的行车安全。

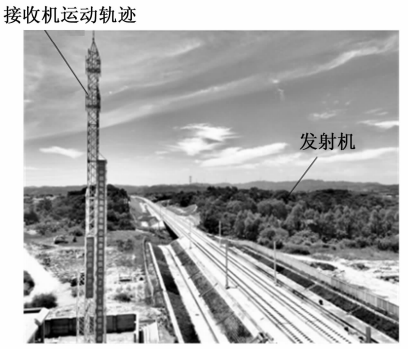

图 5　测试场景示意图

4.2　网络入侵情况设定

铁路通信的安全性为铁路安全运行提供了保障，在进行通道测试时，发射器安装在 30 m 左右的高台上。以高速铁路为研究对象，通过对高速铁路上 10 m 长的静止信道测量，获得高速铁路上的信道 PDP，揭示高速铁路上多径分布特征。基于此，设置了 4 种网络入侵形式。

1）拒绝服务攻击：

由于对服务端发出了许多的要求，使得服务端不能对这些要求作出正确的反应，因此造成了整个系统的停机或不能工作。攻击者通常是利用多台计算机进行网络攻击，造成服务器负载过大，从而造成网络瘫痪。

2）网络钓鱼：

“网络钓鱼”指的是冒充正规站点或邮箱，骗取用户信息。黑客向受害者发出虚假的电邮和文字信息，让受害者点击链接，输入相关信息。这些攻击手段可以窃取使用者的账号和交易信息，从而达到非法活动目的。

3）恶意软件：

所谓“恶意软件”，就是指被用来对计算机进行攻击、破坏、盗取机密数据、进行违法犯罪行为等的一种恶意程序。此类软件往往以文件、软件、电子邮件和链接的形式存在，只要用户一下载和安装，就能迅速地侵入用户的电脑，监控用户的行为，窃取用户的个人数据，甚至操控用户的电脑。

4）网络入侵：

所谓的网络入侵，就是通过破解网络系统密码，或者利用软件弱点等手段，获得目标计算机的权限，从而获得敏感信息。攻击手段有：暴力破解、脚本攻击、SQL 注入等，上述攻击内容为相对高级的攻击方式，对黑客技术要求也很高。

4.3　测试装置

在系统测试过程中，将所研制的末端装置与电机驱动装置相连接，测试装置原理框图如图 6 所示。

终端设备将对开度进行控制的模拟量信号输出到电气执行器，并对其进行反馈。通过在 A、B 两个地区进行的多次测试，能够获取相关测试数据，以此为依据进行测试结果分析。

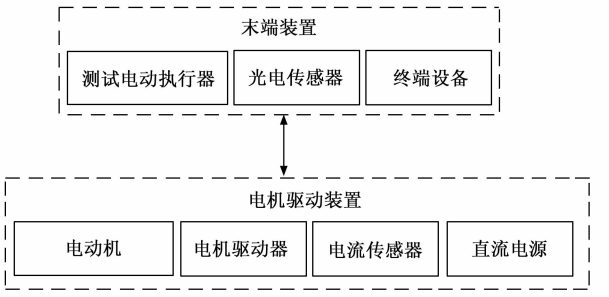

图 6　测试装置原理框图

4.4　测试结果与分析

4.4.1　加密效果分析

将信道误码率、网络吞吐量作为测试指标，对比分析基于卷积神经网络的控制系统、基于区块链匿名属性的加密控制系统和基于窄带物联网加密控制系统的加密效果，对比结果如图 7 所示。

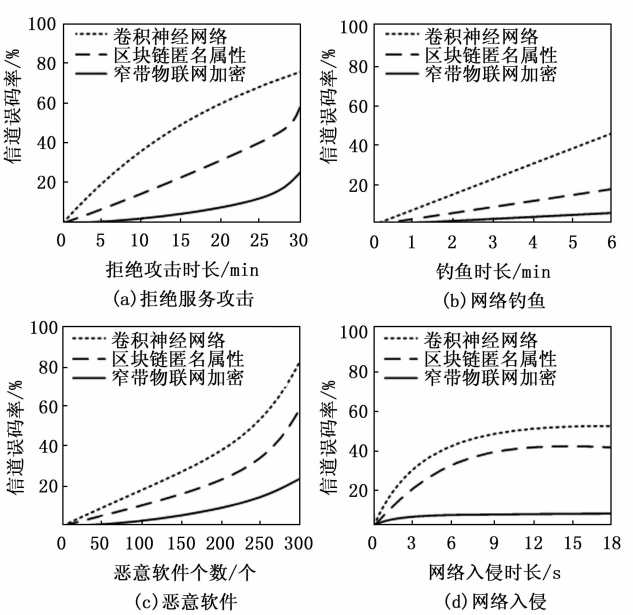

图 7　不同系统的信道误码率对比分析

由图 7（a）可知，在不同拒绝攻击时长下，使用基于卷积神经网络的控制系统比其余两种系统信道误码率要高，在时长为 5 min 时，就达到了 20％的信道误码率，随着时长增加，最大信道误码率为 76％；使用基于区块链匿名属性的加密系统在时长为 5 min 时，信道误码率仅为 8％，但是随着时长增加，在 28 min 时出现了信道误码率快速增加的区域，且在 30 min 时信道误码率达到最大为 60％；而使用基于窄带物联网加密控制系统相比于其他两种系统，信道误码率要更低，只有在时长为 25～30 min 时，出现了快速增长趋势，但最终未超过 30％。

由图 7（b）可知，在不同网络钓鱼时长下，使用 3 种系统的信道误码率较低，其中，使用基于卷积神经网络的控制系统最高信道误码率为 46％，使用基于区块链匿名属性的加密系统最高信道误码率为 19％，使用基于窄带物联

网加密控制系统最高信道误码率为 6%，这 3 种系统的信道误码率均低于 50%，说明均能够有效抵抗钓鱼诱惑，但其中使用设计系统的加密控制效果最好。

由图 7（c）可知，恶意软件攻击会对这 3 种系统均造成一定负面影响，其中对基于卷积神经网络的控制系统影响最大，对基于窄带物联网加密控制系统影响最小，其对应的信道误码率最大值为 24%。

由图 7（d）可知，使用基于卷积神经网络的控制系统在网络入侵时长 0～15 s 内，信道误码率达到最大值为 50%，在 15～18 s 内，信道误码率保持不变；使用基于区块链匿名属性的加密系统在网络入侵时长 0～12 s 内，信道误码率达到最大值为 40%，在 12～18 s 内，信道误码率保持不变；使用基于窄带物联网加密控制系统在网络入侵时长 0～6 s 内，信道误码率达到最大值为 5%，在 6～18 s 内，信道误码率保持不变。

4.4.2 系统可靠性分析

使用不同系统对比分析网络吞吐量，对比结果如图 8 所示。

由图 8（a）可知，使用基于区块链匿名属性的加密系统在不同攻击时长下的网络吞吐量小于其余两种系统，该系统对应的网络吞吐量最大值为 220 bit/s；使用基于卷积神经网络的控制系统在拒绝攻击时长为 3 s 时，网络吞吐量达到最大，对应的数值为 241 bit/s；使用基于窄带物联网加密控制系统在不同攻击时长下的网络吞吐量最大，其中在拒绝攻击时长为 4 s 时，网络吞吐量达到最大，对应的数值为 260 bit/s。

由图 8（b）可知，使用基于区块链匿名属性的加密系统在不同钓鱼时长下的网络吞吐量最小，其中在钓鱼时长为 10 s 时网络吞吐量达到最大，对应的数值为 122 bit/s；使用基于卷积神经网络的控制系统在钓鱼时长为 4 s 时网络吞吐量达到最大，对应的数值为 145 bit/s；使用基于窄带物联网加密控制系统在钓鱼时长为 3 s 时网络吞吐量达到最大，对应的数值为 215 bit/s。

由图 8（c）可知，3 种系统随着恶意软件攻击时长的增加，网络吞吐量下降趋势也随之降低。使用基于卷积神经网络的控制系统、基于区块链匿名属性的加密系统的网络吞吐量最大值分别为 200 bit/s 和 140 bit/s，使用基于窄带物联网加密控制系统网络吞吐量最大值为 260 bit/s。

由图 8（d）可知，3 种系统在网络入侵时长为 5 s 时，网络吞吐量均达到最大值。在网络入侵时长为 30～50 s 时，网络吞吐量在一定数值范围内保持不变，随着时间增加，网络吞吐量均降低，但使用所设计系统网络吞吐量依然最大，证明设计系统能够在高负载网络环境下稳定运行，具有一定的可靠性。

5 结束语

通信网络的发展，给人们生活和生产带来了极大的便利，同时也极大地提高了社会经济效益。然而，随着外界环境不断改变，通信网络也面临着来自外界的威胁，若核心技术受到攻击限制，那么由外界恶意攻击造成的节点传输风险、病毒风险等都会造成网络不稳定现象，从而产生被动防御的现象。针对目前铁路通信网络中存在的问题，设计了基于窄带物联网的铁路通信网络安全加密控制系统。结合窄带物联网的加密控制技术来增强通信网络的安全性，解决现有密码体制存在的不完善问题。通过测试结果可知，所设计系统信道误码率较低，网络吞吐量较高，可以为通信网络的安全运行提供理论依据和技术支持。

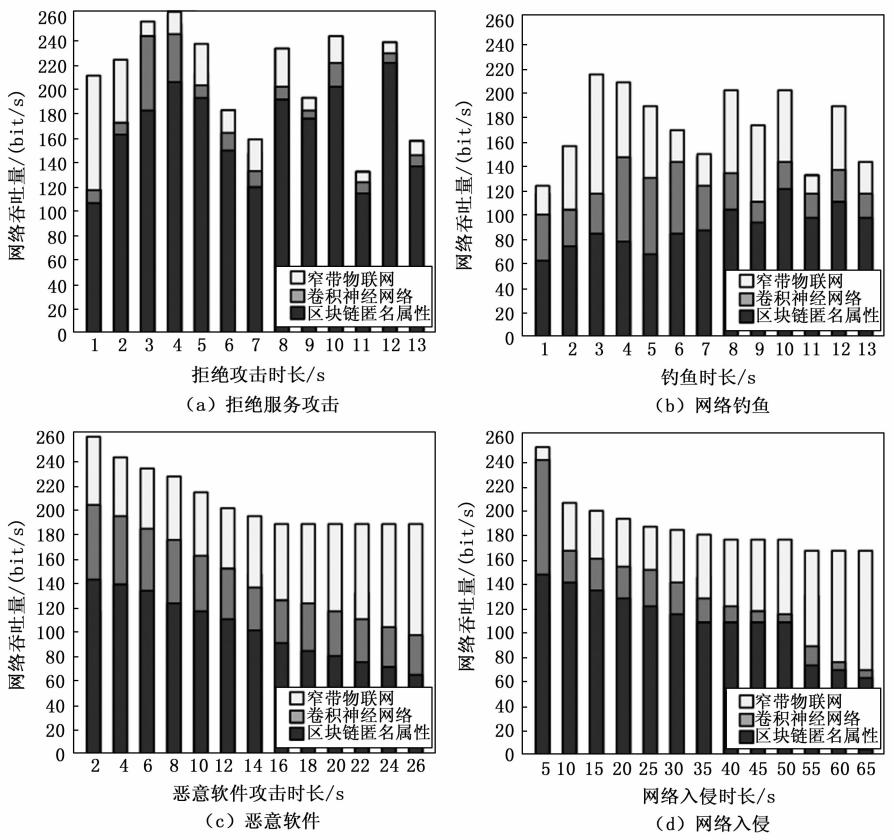

图 8 不同系统的网络吞吐量对比分析

参考文献：

[1] 颜 蔚. 基于卷积神经网络的无线网络安全风险评估及控制 [J]. 沈阳工业大学学报，2022，44 (5)：565－569.

[2] 庄朝源，郭 瑞，杨 耿. 区块链中可验证外包解密的匿名属性加密方案 [J]. 计算机工程与应用，2022，58 (19)：124－134.

[3] 陈泌文，向 涛，何德彪，等. 基于国产密码 SM2 的实用公钥广播加密方案 [J]. 中国科学：信息科学，2022，52 (12)：2321－2335.

[4] 徐善智，张晓荣，乔凌霄，等. 基于窄带物联网的电动执行器监控系统设计 [J]. 仪表技术与传感器，2022，469 (2)：75 - 78.

[5] 吴少乾，李西明. 对抗网络上的可认证加密安全通信 [J]. 计算机科学，2021，48 (5)：328 - 333.

[6] 苏昀暄，涂　正，王绪安，等. 一种基于 CKKS 同态加密与神经网络的安全人脸识别方案 [J]. 兰州理工大学学报，2023，49 (2)：103 - 109.

[7] 阳　浩，黄湛华，何　亮，等. 基于无序滚动码双重加密算法的智能锁通信安全协议设计 [J]. 科技通报，2022，38 (10)：24 - 28.

[8] 刘佳佳，吴　昊，李盼盼. 铁路 5G 移动通信系统边缘计算安全研究 [J]. 计算机工程与应用，2021，57 (12)：1 - 10.

[9] 鞠冠章. 基于人工智能的内网信息安全访问控制系统设计 [J]. 现代电子技术，2023，46 (9)：83 - 86.

[10] 杨立锐，郭心悦. 基于物理层加密的 OFDM 可见光通信系统安全传输方案 [J]. 光通信技术，2023，47 (1)：17 - 24.

[11] 马艳娥，李瑞金. 基于 DFT-S-OFDM 的网络信息安全加密传输仿真 [J]. 计算机仿真，2022，39 (1)：358 - 361.

[12] 屠袁飞，杨庚，张成真. 一种面向云端辅助工业控制系统的安全机制 [J]. 自动化学报，2021，47 (2)：432 - 441.

[13] 唐　猛，李海华，谢灵运，等. 多中继物理层网络编码系统加密设计及安全性能研究 [J]. 云南大学学报（自然科学版），2021，43 (4)：652 - 662.

[14] 陈学先，李宏发，李霄铭，等. 基于同态加密的能源大数据安全系统 [J]. 福建师范大学学报（自然科学版），2023，39 (2)：9 - 25.

[15] 贾晓霞，邢进生. 基于微控制单元的彩色图像加密无线通信方案 [J]. 南京师大学报（自然科学版），2022，45 (2)：98 - 105.

[16] 王聪丽，平西建，张　涛. 基于 Lorenz 混沌系统的红外图像 ROI 加密算法 [J]. 应用科学学报，2022，40 (2)：246 - 252.

[17] 靳旭文，李国东，刘　雯. 基于 3D-CS 混沌系统的双 DNA 编码图像加密算法 [J]. 包装工程，2021，42 (3)：259 - 269.

[18] 李　莉，杨鸿飞，董秀则. 基于身份多条件代理重加密的文件分级访问控制方案 [J]. 计算机应用，2021，41 (11)：3251 - 3256.

[19] 任颖超，燕雪峰. 基于属性加密的 DDS 访问控制方案 [J]. 数据采集与处理，2023，38 (2)：314 - 323.

[20] 池水明，陈　勤，党正芹. 一种基于策略控制的可撤销属性基代理加密方案 [J]. 计算机工程与科学，2013，35 (9)：94 - 98.

(上接第 162 页)

[5] 孔　杰，田学民，尚林源. 基于 EMD 和闭环测试的回路振荡诊断方法 [J]. 控制工程，2019，26 (5)：879 - 885.

[6] 朱　博，杜泽龙，梁鸿鹏，等. 基于云端服务资源的室内外连续监控机器人系统架构设计 [J]. 计算机应用，2022，42 (S1)：333 - 341.

[7] 马金龙，于宗光，赵桂林，等. 用于反熔丝 FPGA 的片上闭环电荷泵电路 [J]. 固体电子学研究与进展，2022，42 (4)：309 - 316.

[8] 倪启南，杨　明，李云嵩，等. 全闭环伺服驱动系统位置控制通信延时补偿技术 [J]. 电工技术学报，2022，37 (10)：2513 - 2522.

[9] 曹英健，仲　悦，张　华. 基于高速数字信号处理器的面向多对象数字伺服控制平台研制 [J]. 导弹与航天运载技术，2021，380 (3)：78 - 82.

[10] 徐洪涛，李延民. 基于 AMESim 和反步控制器的阀控电液伺服系统滑模控制分析 [J]. 液压与气动，2021，354 (2)：123 - 128.

[11] 张建宇，高天宇，于潇雁，等. 基于自适应时延估计的空间机械臂连续非奇异终端滑模控制 [J]. 机械工程学报，2021，57 (11)：177 - 183.

[12] 崔凯凯，韩　维，张　勇，等. 基于低通非奇异终端滑模引导的舰载机抗侧风着舰控制技术 [J]. 控制与决策，2022，37 (9)：2255 - 2264.

[13] 丁明宽，石志勇，韩兰懿，等. 基于 EMD-DFA-小波阈值的 MEMS 陀螺信号去噪方法 [J]. 火炮发射与控制学报，2021，42 (2)：50 - 56.

[14] 吕　峥，庄　炜，吴　越，等. 基于改进 EMD 方法的 FBG 传感网络光谱基线校正研究 [J]. 仪器仪表学报，2022，43 (1)：190 - 197.

[15] 方培俊，蔡英凤，陈　龙，等. 基于 ED-LSTM 的智能汽车神经网络横向动力学建模与控制 [J]. 力学学报，2022，54 (7)：1896 - 1908.

[16] 王贵英，张千宏. 基于广义除法下非线性模糊差分方程的动力学行为研究 [J]. 西南大学学报（自然科学版），2022，44 (8)：116 - 126.

[17] 蔺童童，杨明智，张　雷，等. 高速磁浮列车流线型头部拱形结构对列车与隧道耦合气动特性的影响 [J]. 铁道科学与工程学报，2022，19 (9)：2515 - 2523.

[18] 常思源，肖　尧，李广利，等. 翼反角对高压捕获翼构型亚声速气动特性影响分析研究 [J]. 力学学报，2022，54 (10)：2760 - 2772.

[19] 朱　峰，杨　啸，蒋倩倩，等. 磁浮列车电弧辐射特性及对航向信标影响分析 [J]. 系统工程与电子技术，2022，44 (7)：2096 - 2103.

[20] 崔金龙，李元奎，索基源，等. 基于改进 A～＊算法的船舶航向航速协同优化方法 [J]. 大连海事大学学报，2022，48 (4)：29 - 37.

[21] 马逢群，谭捍东，孔文新. 基于有限内存拟牛顿法的电阻率法三维主轴各向异性反演研究 [J]. 地球物理学进展，2022，37 (2)：637 - 647.

[22] 屈志坚，洪应迪，王子潇. 配电网调度监测数据的多线程集群共享内存折叠压缩方法 [J]. 中国电机工程学报，2021，41 (3)：921 - 932.

[23] 丁理杰，刘姗梅，史华勃. 水电高占比电网中水轮机模型对频率振荡特性影响及其适应性分析 [J]. 电力系统保护与控制，2021，49 (12)：174 - 180.

[24] 鲍　悦，陈俊宇，施天玥，等. 基于先验误差模型的机载高分宽幅 DBF-SAR 自聚焦算法 [J]. 航空学报，2021，42 (6)：515 - 529.