文章编号:1671-4598(2024)02-0162-06 DOI:10.16526/j.cnki.11-4762/tp.2024.02.024 中图分类号:U238.7 文献标识码:A

车载式铁路轨道巡检数据无线传输加密系统设计

苏有斌，邱 祯，刘奇峰
（国能朔黄铁路发展有限责任公司，山西 原平 034100）

摘要：车载式铁路轨道巡检数据在运行中传输中，随着传输数据量的增大，局域网络布局不合理的弊端体现，导致数据传输能力与安全性下降；设计一种车载式铁路轨道巡检数据无线传输加密系统。由车载设备、DMS、无线通信模块、数据接收天线以及数据接收装置搭建数据无线传输加密系统框架，采用多个无线 AP 构建成局域网络，与车载无线传输网络实时链接并进行铁路轨道巡检数据传输；在系统框架的支持下，分别对系统硬件与软件进行设计；系统硬件主要分为业务逻辑、数据解析和无线通信3个层次；系统软件主要是利用 AES 对巡检数据进行加密，并获得对应的数字签名，对已加密的数据进行无线网络传输；经系统应用试验证明，当传输时间为 5.0 s 的情况下，该系统的数据无线传输速度为 423 Mbps；当加密次数为 5 的情况下，该系统的数据加密覆盖率为 94%；该系统的丢包率最大值为 6.9%，最小值为 3.6%，说明该系统具备良好的车载式铁路轨道巡检数据传输能力，且数据加密性能良好，传输速度快。

关键词：车载式；铁路轨道；巡检数据；数据传输无线传输；传输加密；局域网络

Design of Wireless Transmission Encryption System for Vehicle Mounted Railway Track Inspection Data

SU Youbin, QIU Zhen, LIU Qifeng
(CHN Energy Shuohuang Railway Development Co., Ltd., Yuanping 034100, China)

Abstract: During the transmission of vehicle-mounted railway track inspection data in operation, with the increase of transmission data, there is the shortage of unreasonable layout in local area network, resulting in the decline of data transmission capacity and security. A wireless transmission and encryption system for vehicle-mounted railway track inspection data is designed. The data wireless transmission encryption system framework is composed of the on-board equipment, DMS, wireless communication module, data receiving antenna and data receiving device. Multiple wireless access points (Aps) are used to build a local area network, which is linked to the on-board wireless transmission network in real time and carries out the data transmission for the railway track inspection. With the support of the system framework, the system hardware and software are designed respectively. The system hardware is mainly divided into three levels of the business logic, data analysis and wireless communication. The system software mainly uses the advanced encryption standard (AES) to encrypt the patrol data, obtain the corresponding digital signature, and transmit the encrypted data through the wireless network. The system application test proves that when the transmission time is 5.0 s, the wireless data transmission speed of this system is 423 Mbps; When the number of encryption times is 5, the data encryption coverage rate of this system is 94%; The maximum packet loss rate of the system is 6.9%, with the minimum value of 3.6%, indicating that the system has a good data transmission capability for on-board railway track inspection, good data encryption performance, and fast transmission speed.

Keywords: vehicle-mounted; railway track; patrol data; data transmission wireless transmission; transmission encryption; local area network

0 引言

随着数字化时代的到来，铁路运输行业的信息化建设已经成为不可忽视的趋势。铁路轨道作为列车运行的基本硬件，轨道状态及轨道旁设备的实时状态分析是轨道维护体系中的重要环节。由于轨道巡检项目多且工况较为复杂，受到多个环境因素的干扰，使得需要对列车车载设备完成相关的巡检工作，并对数据进行实时传输与分析。车载式铁路轨道巡检技术是目前铁路运输行业中应用广泛的一种技术手段。它通过采用激光测距、高分辨率照相、车载多传感器等技术手段对铁路轨道的各项指标进行实时监测和分析，以发现潜在的问题和缺陷，提高铁路运输的安全性和可靠性。现阶段，作为铁路运输行业中的一个重要环节，

收稿日期:2023-02-27； **修回日期**:2023-04-04。
基金项目:国能朔黄铁路公司科技创新项目(SHYP-22-05)。
作者简介:苏有斌(1976-),男,硕士,高级工程师。
引用格式:苏有斌,邱 祯,刘奇峰.车载式铁路轨道巡检数据无线传输加密系统设计[J].计算机测量与控制,2024,32(2):162-167,188.

车载式铁路轨道巡检对于数据安全和保密性的要求也越来越高。对铁路轨道巡检数据进行加密处理，可以有效地防止数据泄露、信息被窃取等风险，同时也可以确保数据的完整性和可靠性。然而，在车载式铁路轨道巡检数据的采集和传输过程中，数据面临着被非法访问、篡改、破坏等风险。为了保护铁路轨道巡检数据的机密性和完整性，对数据进行加密处理已经成为一种必要的手段。但是由于车载式铁路轨道巡检数据方式比较单一，且并未对数据做任何的加密处理，导致数据安全性大幅度降低。

针对数据的安全无线传输，王皓然等人[1]在硬件设计中，优化嵌入式控制器以及信息存储电路。在软件设计中，采用四维 Chen 离散处理技术以及混沌动力学理论数据加密方案，并采用无线传输的方式实现数据安全传输；刘佳等人[2]基于大数据分析建立无线传输系统。通过调试车载设备信号，结合物联网技术完成数据安全传输，提高传输性能和应用需求；但这两种系统未能全面考虑局域网络布局对数据传输速度的影响，具有一定的局限性。

车载式铁路轨道巡检数据传输局域网络布局不合理，导致数据传输能力与安全性下降，所以设计车载式铁路轨道巡检数据无线传输加密系统，旨在为铁路运输行业中数据安全保护提供理论和实践指导，确保铁路轨道巡检数据的安全可靠性，为铁路运输的发展做出贡献。

1　铁路轨道巡检数据无线传输加密系统结构及原理

由车载设备、DMS、无线通信模块、数据接收天线以及数据接收装置搭建数据无线传输加密系统框架，采用多个无线 AP 构建成局域网络，与车载无线传输网络实时链接并进行铁路轨道巡检数据传输。车载式铁路轨道巡检数据的无线传输加密系统结构原理如图 1 所示。

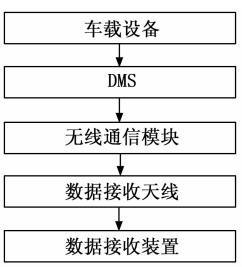

图 1　车载式铁路轨道巡检数据无线传输加密系统结构原理图

1）车载设备：将车载设备安装至铁路车载设备的安装位置和数量根据具体的车辆型号和车辆用途而定。一般来说，铁路车载设备安装位置包括车头、车厢和车尾 3 个部位，而装置数量则取决于车载设备的种类、功能和车辆的尺寸和载重等级。车载设备可以为驾驶员和车辆提供各种服务，例如导航、音频、视频、通讯、安全驾驶、车辆诊断等。车载设备的工作原理是通过各种传感器收集各种铁路车辆数据，例如速度、方向、位置、车辆状态等，并通过嵌入式计算机进行处理和存储，并通过显示器和通讯系统向驾驶员提供相应的信息和服务。同时，车载设备可以通过通讯系统与其他设备进行数据交换和信息共享。

2）DMS：车载式巡检数据的无线传输装置与安装在铁路轨道巡检设备上的动态实时监测系统建立连接，监测系统中主要包含信息采集装置 DMS，DMS 负责对铁路轨道巡检数据进行采集，在数据采集过程中，可以实现数据的分析、处理和保存，当数据接收装置对接到地面网络信号之后，可自动完成与服务器的实时连接，将铁路轨道巡检数据压缩后，利用无线传输网络与接收天线之间完成数据加密与数据接收[3-4]。

3）无线通信模块：该模块是一种将铁路轨道巡检数据的数字信号转换成无线信号并进行传输的设备。无线通信模块的原理基于无线电波传输的技术原理，主要包括 3 个方面的内容：调制解调、射频信号放大和无线传输。首先，调制解调是无线通信模块实现铁路轨道巡检数据的数字信号到无线信号转换的重要基础，将数字信号通过调制解调电路进行调制，可以将其转换成符合无线电波传输的模拟信号；射频信号放大是将调制后的模拟信号加以放大，以提高信号传输的距离和质量；无线传输是指将放大后的无线信号通过天线进行铁路轨道巡检数据信号的无线传输。

4）数据接收天线：该天线是一种用来接收无线电频谱中的电磁波以提取载有数据的天线。其基本原理是利用天线的辐射和受辐射的特性，将通过空气传播的电磁波转化为电流信号的形式，然后再经过前端电路进行放大、滤波等处理，最后通过解调器将数据提取出来。在数据接收天线中，天线的长度一般要与所接收的信号波长相匹配，并且其线圈截面积也要足够大以保证较好的接收灵敏度。当电磁波被接收天线辐射到时，相应的电场和磁场变化将导致天线内部产生电流，这个电流信号包含了所接收铁路轨道巡检数据信号的各种信息。通过前端电路进行放大和滤波，可以将所接收的信号转换成合适的电压或电流信号，并进行进一步的信号处理。在这个过程中，如果接收的信号中包含多个频率的分量信号，需要进行频率选择性的滤波，以防止混叠现象发生。最后，解调器可以在信号处理的最后一步将所提取的信息恢复成数字或者模拟的形式，使得铁路轨道巡检数据信号可以被其他设备所使用。

5）数据接收装置：该装置是一种用来接收无线电频谱中的电磁波以提取有效铁路轨道巡检数据的装置。其主要工作原理分为以下几个步骤：

步骤 1：接收天线接收电磁波信号，并将其转化为电流或电压信号。接收天线的选取需要根据接收信号的频率和波形进行匹配，以便提高接收的效率和精度。

步骤 2：将电流或电压信号进行前置放大和滤波处理。前置放大器可以将接收到的小信号进行放大，以便后续处理的电路能够对信号进行更加精确地处理。此外，对于不同频率的信号需要选择不同的滤波器，以保证有效地提取目标信号，同时滤波器也可以用来防止干扰信号影响目标信号的提取。

步骤 3：信号解调。将前置处理后的信号进行解调，而

解调的方式具体取决于信号的类型和信息的编码方式。相干解调和非相干解调是两种不同的解调方式，相干解调适用于连续波的信号，而非相干解调适用于脉冲、调制和复杂信号的解调。

步骤 4：数字信号处理。对于数字信号的处理，可以使用数字信号处理器（DSP）或者特定的集成电路进行数据分析、处理、计算和存储。数字信号处理是实现高速、高精度信号分析和处理的必备技术手段。

步骤 5：数据输出。最后，数据接收装置将所处理的铁路轨道巡检数据输出到显示器、计算机或者其他信息处理设备上，以便进行进一步的分析、处理和展示。

2 系统硬件

铁路轨道巡检数据无线传输加密系统硬件是实现数据无线传输的前提，因此硬件设计主要是将无线通信传输作为相关目标的，硬件主要分为业务逻辑、数据解析和无线通信 3 个层次，具体如图 2 所示。

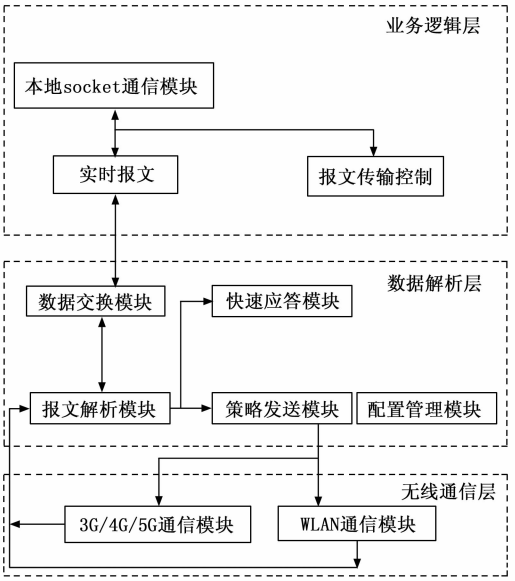

图 2 系统硬件架构

2.1 业务逻辑层

业务逻辑层主要包含铁路轨道巡检数据报文传输控制和本地 socket 通信模块两个主要模块。

报文传输控制模块中主要控制着铁路轨道综合巡检装置，并利用 FTP 协议完成与地面服务器之间的文件传输，满足数据无线加密传输的基础业务逻辑[5-6]。本地 socket 通信模块通过与地面服务器之间的连通实时传输巡检数据，并建立网络数据传输的基础业务逻辑。列车向服务器发出的巡检报文中包含常态巡检以及故障信息等，服务器向列车发送的报文中包含铁路轨道的故障点指示以及行驶命令等，以此实现实时报文传输[7]。

2.2 数据解析层

该层主要包含报文解析模块、数据交换模块、快速应答模块以及策略发送和配置管理等模块。其中在报文解析模块中，每个报文对应一个原宿设备编码，根据这个编码能够获悉报文的具体发送方式，并得到报文实际目的地的 IP 地址，在此基础上根据报文的发送应答等级，决定具体的执行策略，对报文实施加解密处理[8]。数据交换模块主要承担着巡检数据无线加密传输系统硬件中的业务逻辑层和解析层之间的数据传递工作。快速应答模块负责响应多种数据传输指令，保证数据传输工作的顺利开展。策略发送模块主要根据报文的发送属性，决定无线加密传输通信层的发送方式和周期。配置管理模块对于地面服务器的维护起到非常重要的作用，负责统配 IP 地址和网络物理接口名称等一系列工作。

2.3 无线通信层

无线加密传输中的通信层主要由 WLAN 和 3G/4G/5G 模块组成，WLAN 模块中包含 UDP 协议并以此作为报文收发接口，利用 CMD 协议[9]对上述的通信需要完成对应的协商认证和链接通道建立，在 TCP 协议的基础上实现铁路轨道巡检数据的下载和断点续传，3G/4G/5G 模块中主要包含无线传输接口，支持多种无线传输方式。

系统硬件前端装置主要由列车信号主机 110 V 电源提供能量，同时自身具备电池供电系统，各个板卡部分需要的电源能量同样由前端装置的主电源提供，低于 5 V 的电源则自身的稳定电压线路提供[10]。车载式铁路轨道巡检装置站在作业时，需要采集轨道状态信号，对完成对应的数据分析，并将报文数据有效地提供给前端装置主板，设计时考虑到主处理器的运算压力问题，尽可能地降低系统的编程难度，提高系统对巡检数据传输的实时性，通过独立的数据处理器完成巡检感应信号的解析工作，以此获取实时报文。铁路轨道巡检感应信号处理架构如图 3 所示。

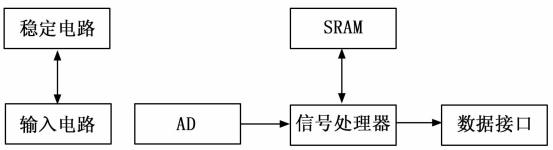

图 3 铁路轨道巡检感应信号处理架构

在铁路轨道巡检感应信号处理架构中，需要保证电压和电路状态相对稳定。利用单片低压差稳压器完成核心的电压处理，为作业模块提供相对应的稳定电源。针对铁路轨道巡检的输入信号，选择小于 3 V 的交流电压来辅助完成数据解析。在铁路轨道巡检感应电路中安置隔离芯片 ISO124，可有效地对传输信号进行隔离并放大处理，数据采样电路中加装 AD 模式的数据转换器，与外围电路联合构成定时中断状态下的数据采样模块，在并行接口的辅助下，实现巡检数据的实时采集[11]。信号处理器选用 TMS320F28355 型号，主要负责解析程序中的巡检数据，与静态存储芯片共同构建系统的外扩存储环境，可以对轨道巡检数据进行实时运算和处理，可以保证巡检数据的串行接口与前端装置之间的数据交互。

车载式铁路轨道巡检数据感应信号解析程序如图 4 所示。

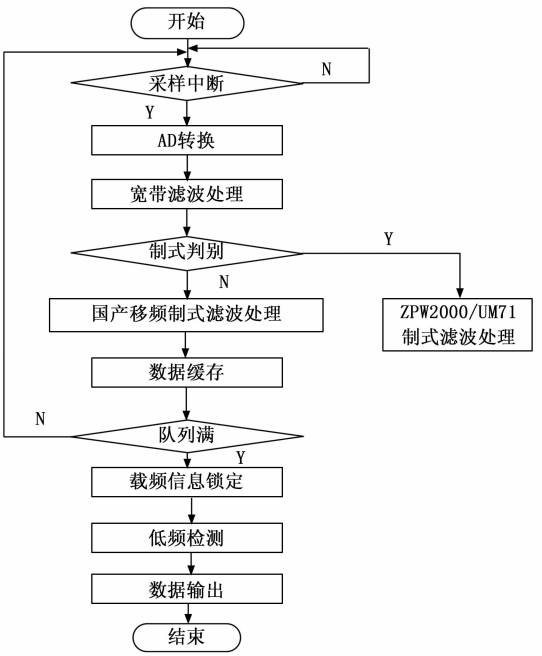

图 4　轨道巡检数据感应信号解析流程

在感应信号解析需要通过运算模块联合对应的子处理器共同完成，利用模数转换装置将采样数据进行 A/D 转换和带宽滤波处理，将其中的主信号、干扰信号以及邻区段等制式进行判别，并对不同制式进行再次滤波处理，有效地提高巡检数据信号的抗干扰性，并增强车载铁路巡检数据信号的分辨率，并将数据缓存到系统的数据库中。当缓存队列已满的情况下，锁定载频信息并对信号低频部分进行检测，以此实现对于轨道巡检数据感应信号解析[12]。

3　系统软件加密算法的设计

AES（Advanced Encryption Standard）是一种目前被广泛应用的对称加密算法[13-14]，加密和解密使用相同的密钥，加密时将明文按分组长度划分为若干块，通过加密运算生成密文，解密时同样将密文划分为若干块，通过解密运算生成明文[15-16]。AES 算法的核心是代替了原来的置换、替换和线性变换等运算方法，使用了更具有代表性的 SubBytes、ShiftRows、MixColumns 等基本变换，即 S 盒变换、行移位变换、列混淆变换。通过这些变换的组合以及轮密钥加法，AES 实现了高强度、高效率的加密和解密运算[17]，具有以下优点：

1）安全性高：AES 采用对称加密方式，密钥长度可达到 256 位，加密时使用的密钥只有授权用户拥有，加密后的密文很难被解密，因此安全性非常高。

2）高效性：AES 加密和解密速度快，计算量小，可适用于软硬件实现，非常适合于加密处理大数据块和流数据。

3）灵活性好：AES 算法可以根据需求动态地调整密钥长度，适合多种应用场景。

4）兼容性强：AES 算法被广泛应用于不同的操作系统、编程语言和应用软件中，因此具有较好的兼容性。

5）支持硬件加速：AES 算法可以在支持硬件加速的设备上进行加解密处理，比如由 Intel 提供的 AES 指令集，使加解密速度更快。

综上所述，AES 算法因安全性高、高效性、灵活性、兼容性强以及支持硬件加速等优点而被广泛应用于数据加密领域[18-19]。

为了满足系统对轨道巡检数据的快速有效加密要求，使用 AES 对所传送的巡检数据进行加密，AES 采用一次一密的方式[20]，使每次的密钥都不同，在无线网络上传送前，传送端先使用随机的生成器生成密钥对铁路轨道巡检数据报文进行加密，随后通过 ECC 对 AES 算法进行密钥处理，简化密钥处理过程，获得对应的数字签名，并对加密完成的数据进行无线网络传输。

混合密钥处理过程分 3 个部分：

1）获取 ECC 加密公钥和私钥。选择加 AES 密算法所需要的曲线参数，在二进制算法中利用到 6 个对应参数，分别为 $T=(p,a,b,G,n,h)$，其中 p,a,b 主要负责确定椭圆曲线走势，G 表示椭圆基础点，n 表示 G 的阶，h 表示椭圆上包含点数 m 与 n 相除后得到的整数位，p,a,b,G 属于公开部分。

此时在椭圆曲线 E 上随机选择一个点 p，p 所对应的阶为 n 且同样属于公开部分，在 $[1,n-1]$ 中选择出一个整数 K_s，通过计算 $K_P=K_sP$ 可以确定公钥 K_P 和私钥 K_s。

2）巡检数据的加解密处理。在加密 AES 密钥的过程中，传输方需要对待传输的轨道巡检数据进行明文编码，将其编码到椭圆曲线 $E(a,b)$ 上的对应点 $M=(m_x,m_y)$ 上，由此随机生成一个整数编码条件 $r(r<n)$，分别计算 $C_1=M+rK$；$C_2=rG$，将计算得出的 C_1,C_2 实时传输给巡检数据接收方。

数据接收方接到加密数据后，在解密 AES 密钥的过程中，下述公式对巡检数 M 实施解码处理，具体的公式如下：

$$C_1-kC_2=M+rK-K(rG)=m+rK-r(kG)=M \tag{1}$$

得出的 M 实施解码动作后，获得数据解码密钥。

3）数字签名。在初步确定安全 Hash 函数的条件下，公开处理椭圆曲线参数集公钥 K_P。当列车向管理站发送巡检数据 M 并进行签名时，首先需要选择并确定一个随机数 K，且满足 $1<K<n-1$ 条件；随后计算：

$$KG=(X_1,Y_1),r=X_1 \bmod n \tag{2}$$

若得出的结果为 $r=0$，则转向 1；紧接着继续计算：

$$K^{-1} \bmod n,e=SHA(M) \tag{3}$$

最后计算签名属性：

$$S=K^{-1}(e+K_sr)(\bmod n) \tag{4}$$

若计算得到的 $S=0$，此时则可以转回第一步并输出最终签名 (r,S)。

当管理站接收到列车发送的巡检数据明文 M 和签名

(r,S) 后，首先需要验证 r、S 是属于 $(1,n-1)$ 之间的整数；随后分别计算 $E=SHA(M)$，$W=S^{-1}(\mathrm{mod}n)$ 和 $U_1=EW(\mathrm{mod}n)$，$U_2=rW(\mathrm{mod}n)$；将计算 $X=U_1G+U_2K_p=(X_1,Y_1)$ 得到的结果进行评估，若 $X=0$，则拒绝接收到的签名，并计算对应的 $V=X_1\mathrm{mod}n$，若结果 $r=V$ 则可以接收签名。

在此基础上选择巡检数据的传输模板，将数据按照相关要求进行整合并完成排序，为保证铁路轨道巡检数据在无线加密传输的过程中，明文和密文之间遵循序列完备原则并保持差异性，巡检数据的加密传输需要在两个串口并行状态下完成，具体的巡检数据加密传输模板如图 5 所示。

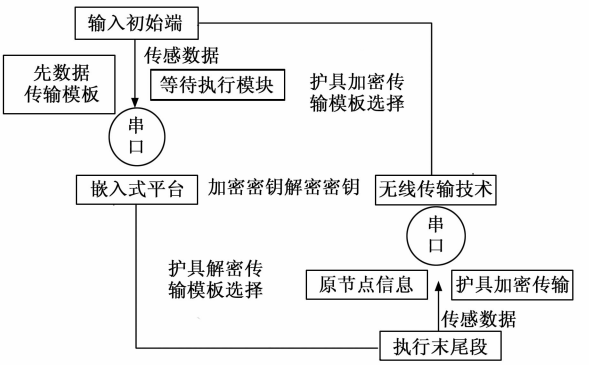

图 5 巡检数据加密传输模板

4 系统应用试验

受到列车前端装置的影响，列车不具备专用天线的安装条件，为了能更好地验证无线传输加密系统通道的稳定性，试验选择在山区和隧道较多的路段进行。首先将应用试验分为 5 个单程，每个单程 80 km，并分别编号为 T1～T5，在不同编号的单程上进行轨道巡检数据无线加密传输应用试验，T1、T3 段车程的巡检数据从机次位发出，T2 段车程的巡检数据从列车尾部发出，上述 3 次的数据传输均通过车载 GPS 天线完成，并且与巡检设备连接完好，T4 和 T5 段车程应用试验的巡检数据分别从机次位和列车尾部发出，传输通过列内置天线完成，巡检设备与测试接口连接均正常。

系统应用试验测评中，列车的电务检测模块要保持开启状态，能够实时接收测试结果，评估无线信号的强度，与此同时打开数据分析机统计巡检数据的丢失情况，巡检数据无线加密传输的测试统计数据结果如表 1 所示。

由表 1 可以看出，在 T1、T3、T4 这 3 段，铁路轨道巡检数据传输过程中的丢包数量均维持在 3 个以内，平均丢包率小于 2.23%，信号强度保持在 44～62 dB 之间，这可以说明从列车的机次位发出巡检数据，无论使用车载 GPS 或是内置天线，都能够很好地满足巡检数据的传输需要；在 T2、T5 这两段中，巡检数据都是从列车尾部发送，尤其在 T5 车程的试验中，巡检数据的最大连续丢包个数是 5 个，而在 T2 车程的试验中，最大的连续丢包数量高达 14 个，且平均丢包率也偏高，信号的整体接收强度相对来说较低，因此可以判定巡检数据若想从列车尾部发送，那么只有内置天线才能满足无线加密传输的需求。

表 1 系统应用试验测试数据结果统计

序号	1	2	3	4	5
车次	T1	T2	T3	T4	T5
距离/km	80	80	80	80	80
轨道电路区段量/个			115		115
数据包总量/个	14 706	15 333	17 664	17 542	14 002
有效数据包量/个	14 669	11 945	17 415	17 155	13 035
平均丢包率/%	0.26	22.11	1.41	2.23	6.88
最大连续丢包数/个	1	14	2	3	5
平均信号强度/dB	61	81	62	44	72
备注	模拟数据	模拟数据	实际数据	模拟数据	实际数据

为了深度验证所研究的车载式铁路轨道巡检数据无线传输加密系统性能，对无线传输进行了速度检测，并通过与文献［1］系统和文献［2］系统两种不同方法进行比对，得出相关的实验结论，巡检数据无线传输速度比对结果如图 6 所示。

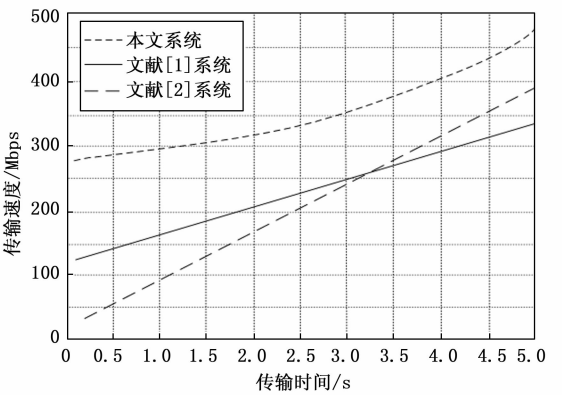

图 6 巡检数据无线传输速度比对

分析图 6 中的数据可知，随着传输时间的不断增加，3 种系统的车载式铁路轨道巡检数据无线传输速度均呈现不断递增趋势，而本文方法的无线传输曲线始终高于文献［1］系统和文献［2］两种系统。其中，当传输时间为 0.5 s 的情况下，文献［1］系统的车载式铁路轨道巡检数据无线传输速度为 58 Mbps，文献［2］系统的车载式铁路轨道巡检数据无线传输速度为 140 Mbps，本文系统的车载式铁路轨道巡检数据无线传输速度为 278 Mbps；当传输时间为 3.0 s 的情况下，文献［1］系统的车载式铁路轨道巡检数据无线传输速度为 240 Mbps，文献［2］系统的车载式铁路轨道巡检数据无线传输速度为 249 Mbps，本文系统的车载式铁路轨道巡检数据无线传输速度为 352 Mbps；当传输时间为 5.0 s 的情况下，文献［1］系统的车载式铁路轨道巡

检数据无线传输速度为 340 Mbps，文献［2］系统的车载式铁路轨道巡检数据无线传输速度为 382 Mbps，本文系统的车载式铁路轨道巡检数据无线传输速度为 423 Mbps。以此证明在相同传输时间条件下，通过与文献［1］系统和文献［2］系统进行对比可知，本文系统在相同时间下巡检数据无线传输速度更快，速度优于其他两种系统。

保证铁路轨道巡检信息的安全性，是设计车载式无线传输加密系统的主要目的，这里针对数据加密安全性能进行测试，不同方法的数据加密覆盖率测试对比结果如图 7 所示。

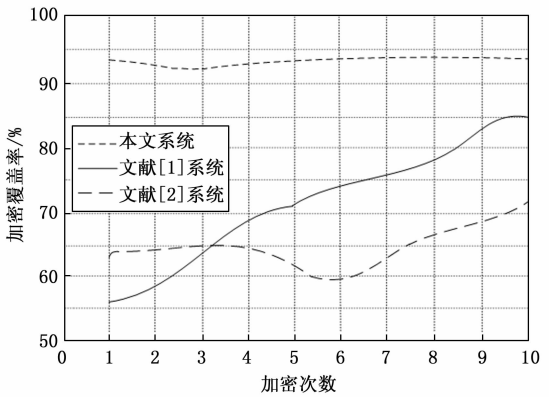

图 7　不同方法的数据加密覆盖率测试结果

从图 7 中可以看出，随着加密次数的不断增加，3 种系统的车载式铁路轨道巡检数据加密覆盖率均呈现波动变化趋势。当加密次数为 1 的情况下，文献［1］系统的车载式铁路轨道巡检数据加密覆盖率为 56%，文献［2］系统的车载式铁路轨道巡检数据加密覆盖率为 63%，本文系统的车载式铁路轨道巡检数据加密覆盖率为 93%；当加密次数为 5 的情况下，文献［1］系统的车载式铁路轨道巡检数据加密覆盖率为 72%，文献［2］系统的车载式铁路轨道巡检数据加密覆盖率为 63%，本文系统的车载式铁路轨道巡检数据加密覆盖率为 93%；当加密次数为 5 的情况下，文献［1］系统的车载式铁路轨道巡检数据加密覆盖率为 85%，文献［2］系统的车载式铁路轨道巡检数据加密覆盖率为 73%，本文系统的车载式铁路轨道巡检数据加密覆盖率为 94%；综合来看，所研究的无线传输加密系统的加密覆盖率存在一些波动，但整体来看，与文献［1］系统和文献［2］系统相比，所研究方法在加密覆盖率始终保持在较高的水平，说明该系统的加密效果好，可有效地加强巡检数据的安全性，提高铁路列车行驶的安全系数。

在上述实验的基础上，为了验证不同系统的车载式铁路轨道巡检数据无线传输加密性能，对比了不同系统在无线传输加密过程中的丢包率，对比结果如表 2 所示。

分析表 2 中的数据可知，文献［1］系统的车载式铁路轨道巡检数据无线传输加密过程中的丢包率最大值为 36.8%，文献［2］系统的车载式铁路轨道巡检数据无线传输加密过程中的丢包率最大值为 25.7%，本文系统的车载式铁路轨道巡检数据无线传输加密过程中的丢包率最大值为 6.9%，分别比文献［1］系统与文献［2］系统低 31.7%、18.8%。文献［1］系统的车载式铁路轨道巡检数据无线传输加密过程中的丢包率最小值为 23.6%，文献［2］系统的车载式铁路轨道巡检数据无线传输加密过程中的丢包率最小值为 16.9%，本文系统的车载式铁路轨道巡检数据无线传输加密过程中的丢包率最小值为 3.6%，分别比文献［1］系统与文献［2］系统低 20%、13.3%。综合来看，本文方法的丢包率最低，该方法在传输数据时，丢包率低，保证了数据能够准确地到达目的地，从而保证了数据的完整性和准确性。不仅如此，还能够有效减少重复传输和数据校验的过程，节省了时间和带宽资源。

表 2　不同系统的丢包率对比结果　　%

传输时间	文献[1]系统	文献[2]系统	本文系统
0.5	36.8	23.2	5.3
1.0	38.9	25.7	4.7
1.5	26.4	24.8	5.6
2.0	26.8	23.6	4.7
2.5	26.5	18.6	3.6
3.0	24.7	17.9	5.8
3.5	25.6	16.9	6.9
4.0	26.7	18.9	5.7
4.5	24.1	17.6	5.4
5.0	23.6	15.6	6.3

5　结束语

设计了车载式铁路轨道巡检数据无线传输加密系统，系统硬件主要分为业务逻辑、数据解析和无线通信 3 个层次。系统软件主要是利用 AES 对巡检数据进行加密，并获得对应的数字签名，对已加密的数据进行无线网络传输。该系统无须对列车电务设备进行大规模改装，能够有效完成轨道巡检和数据安全传送，最大程度上保证数据安全性与传输效率，经试验证明所研究系统具备广泛应用的条件，传输速度快，加密效果好，可以广泛应用在数据无线传输加密领域。通过对车载式铁路轨道巡检数据无线传输加密系统的研究和应用，我们可以有效地保障铁路轨道的安全和正常运营，提高铁路交通运输的精度和可靠性。相信在未来，这一技术将继续得到进一步的完善和普及，为人们的出行带来更加便捷、安全和舒适的体验。

参考文献：

[1] 王皓然，周泽元，班秋成. 混沌加密的电网数据安全传输系统设计［J］. 单片机与嵌入式系统应用，2022，22（4）：16-19.

[2] 刘　佳，张福景，杜晓明. 无接触网有轨电车车地无线传输系统研究［J］. 城市轨道交通研究，2020，23（5）：140-143.

[3] 仝　军，田洪生，吴翠红. 考虑节点能量特征的无线传感数据加密传输方法［J］. 传感技术学报，2022，35（9）：1277-1281.

（下转第 188 页）