

一种混沌密钥加密改善铁路安全通信的新方法

蒋逢灵^{1,2} 刘沅明¹ 刘贤群¹

JIANG Fengling LIU Yuanming LIU Xianqun

摘要

铁路信号安全通信是铁路运输最为重要的安全保障,关系到旅客的生命财产安全。现有的铁路安全通信是依靠中国列控系统 CTCS-3 在铁路安全通信协议 RSSP-II 下保障铁路的安全通信,但会受到已经明文和选择性明文等攻击,对铁路通信安全造成潜在的威胁。基于 Lyapunov 稳定性理论,通过设计设置有限时间的控制函数,从理论上证实了分数阶超混沌系统在有限时间里能够实现同步控制,并结合 RSSP-II 协议将铁路安全通信的数据信息调制到混沌信号中以混合信号进行加密传输,最后再利用相应的同步信号对混合信号进行解密,实现了铁路通信的安全传送。数值仿真结果表明了所提方案的正确性与可行性,展现出所提方案的工程领域应用潜力。

关键词

分数阶超混沌系统;混沌密钥;RSSP-II;安全通信;铁路通信

doi: 10.3969/j.issn.1672-9528.2024.08.031

0 引言

国家非常重视铁路事业的发展,铁路是国家重要交通基础设施和重大民生工程。根据中国铁路总公司发布的《中长期铁路网规划》内容,我国高铁已经形成了“四纵四横”,正在朝“八纵八横”的铁路网建设事业发展。高铁的运行速度为了满足人们的出行需求不断提高,运行速度已经达到 350 km/h,为了人们的生命财产安全,相关铁路的安全通信问题越来越引起人们的重视^[1-2]。参考欧洲列控系统 ETCS 的技术标准^[3],我国的列车控制系统经过技术引进和自主创新阶段的发展,设计了保障列车安全运行的 CTCS-3 (Chinese train control system of level 3),是目前保障铁路信号安全通信的关键,通过铁路安全通信协议 RSSP-II (railway signal safety protocol-II)^[4]保障无线闭塞中心列车与地面设备间的安全数据传输。随着工业网络技术的发展,新的攻击手段不断发生,即便处于封闭状态的 CTCS 列控系统也难以保证绝对安全,在铁路通信数据传输中还会面临重复、重排序、插入、延迟、删除、损坏和伪装等威胁^[5],使列控系统面临极大的信息安全挑战。

混沌具有非周期、随机性、类噪声等特性^[6],分数阶超混沌系统比低维混沌系统具有更加复杂的混沌序列,与密码学具有天然的联系和相似性,非常适用于安全通信^[7]、图像

加密^[8]、密钥分发^[9]等领域中。混沌系统对初值极度敏感,即便两个非常相近的状态,系统输入初始值微小的变化都有可能引起输出的巨大差异,甚至在演变的过程中分化成两个完全不同的状态。这给混沌系统的控制造成了很大的困难,但是人们从未停止对混沌系统的同步控制。科学家 Edward 等人提出了混沌系统的小参数扰动控制方法,也就是通常所说的 OGY 法^[10]。Pecora 等人基于 PC 同步方法实现了混沌系统的同步控制,提出了重要的混沌同步控制的理论^[11],激发了学者们对混沌系统同步控制研究的热情,其他学者相继提出广义同步、自适应同步、滑膜同步控制等方法^[12-14]。尽管研究同步的方法已逐步成熟,但是这些方法都是在时间趋于无穷大时才能保证混沌系统渐渐趋于稳定,收敛速度太慢。这种同步方法只能应用于一些时效性不高、比较粗犷的工程领域。针对这种情况,人们提出了有限时间同步控制的概念,它能够在有限的时间内实现混沌系统的同步控制,具有更好的鲁棒性。

鉴于此,为了进一步改善混沌加密铁路安全通信,提高铁路安全通信时间戳的响应时间的可控性,基于 Lyapunov 稳定性理论构造出有限时间控制函数,通过设置合适的参数实现了主从系统的有限时间同步。在不改变原有 RSSP-II 铁路通信协议安全保护设备的基础上,利用混沌掩盖技术在信号发送端将铁路安全通信的数据信息通过加密函数调制到混沌信号中以混合信号的方式进行传输,对传输信息进行混沌加密。最后,在接收端利用混沌同步信号,通过解密函数将通信数据信息解密。

1. 湖南铁路科技职业技术学院 湖南株洲 412006

2. 湖南省高铁运行安全保障工程技术研究中心 湖南株洲 412006

[基金项目]湖南省自然科学基金资助项目(2022JJ60009)

1 分数阶微积分及其逼近

目前提出了很多分数阶微分定义版本, 比如 Riemann-Liouville 定义等, 都非常具有代表性。这里采用著名的 Caputo^[15] 定义:

$$D_*^\alpha x(t) = J^{n-\alpha} x^{(n)}(t), \alpha > 0 \quad (1)$$

式中: n 为 $n \geq \alpha$ 的第一个整数, $J^{n-\alpha}$ 是阶数为 $n-\alpha$ 阶的 Riemann-Liouville 积分算子。

$$J^\beta y(t) = \frac{1}{\Gamma(\beta)} \int_0^t \frac{y(\tau)}{(t-\tau)^{1-\beta}} d\tau \quad (2)$$

式中: β 为积分算子的阶数 ($0 < \beta \leq 1$), $\Gamma(\beta)$ 是 Gamma 函数。

假设分数阶混沌系统为:

$$D_t^q x(t) = Ax(t) + f(x(t)) \quad (3)$$

将式 (3) 作为驱动系统, 那么其响应系统为:

$$D_t^q y(t) = Ay(t) + g(y(t)) + U(t) \quad (4)$$

式中: q 为分数阶系统的阶数, A 为分数阶混沌系统的线性部分的 $n \times n$ 系数矩阵, $x(t)$ 和 $y(t)$ 为系统状态变量, $f(x(t))$ 和 $g(y(t))$ 为非线性函数, $U(t)$ 为驱动系统中的控制器。

定义误差系统为:

$$e(t) = y(t) - x(t) \quad (5)$$

那么, 通过设置合适的控制函数 $U(t)$, 在分数阶混沌系统初始值取一定值的情况下, 只要满足误差系统使得 $\lim_{t \rightarrow \infty} \|e(t)\| = \|y(t) - x(t)\| = 0$, 那么系统 (4) 与系统 (3) 将在有限的时间内容实现同步。

引理 1^[16]:

$$D^q x^u = \frac{\Gamma(u+1)}{\Gamma(u+1-q)} x^{u-q} D^q x \quad (6)$$

引理 2^[17]: 假设函数 $f(t) \in C_a^\alpha([a, b])$, $D_a^\alpha f(t) \in C_a^\beta([a, b])$, 其中 $\alpha, \beta > 0$ 且 $m-1 < \beta < m$, $n-1 < \alpha < n$, 则有:

$$D_a^\beta (D_a^\alpha f(t)) = D_a^{\alpha+\beta} f(t) \quad (7)$$

引理 3^[18]: 当任意实数满足 $a, b > 0$ 且 $0 < c < 1$ 时, 可得:

$$(a+b)^c \leq a^c + b^c \quad (8)$$

引理 4^[19]: 假设有函数 $x(t) \in \mathbf{R}$ 连续可导, 则对于任意时间常数 $t \geq t_0$, 则有:

$$\frac{1}{2} D^q (x^T(t)x(t)) \leq x^T(t) D^q (x(t)) \quad (9)$$

式中: $0 < q < 1$ 。

定理 1^[20]: 考虑导分数阶系统:

$$D_t^q x(t) = f(x, t) \quad (10)$$

假设满足:

$$x^T D_t^q x \leq -\rho (x^T x)^\lambda \quad (11)$$

那么系统 (10) 是有限时间稳定的, 且在有限时间

$t \leq \left[V(0)^{q-\lambda} \frac{\Gamma(1-\lambda)\Gamma(1+q)}{\Gamma(1+q-\lambda)2\rho} \right]^{\frac{1}{q}}$ 内系统会趋于同步。其中 $0 < q < 1$,

ρ, λ 都是任意的正常数, 并且满足 $0 < \lambda < \frac{q+q^2}{2}$ 。

2 分数阶系统有限时间稳定性定理证明

证明, 根据引理 4 和定理 1, 可得:

$$\frac{1}{2} D^q x^T x \leq \rho (x^T x)^\lambda \quad (12)$$

这里, 令 $V = x^T x$, 那么 $(x^T x)^\lambda = V^\lambda$, 整理后可得:

$$D^q V \leq -2\rho V^\lambda \quad (13)$$

假设 $V > 0$, 等式两边求解, 则得:

$$V^{-\lambda} D^q V \leq -2\rho \quad (14)$$

根据引理 1, 可以得出:

$$D^q V^{q-\lambda} = \frac{\Gamma(1+q-\lambda)}{\Gamma(1-\lambda)} V^{-\lambda} D^q V \quad (15)$$

由式 (13)、式 (14) 和式 (15), 可得:

$$V^{-\lambda} D^q V = \frac{\Gamma(1-\lambda)}{\Gamma(1+q-\lambda)} D^q V^{q-\lambda} \leq -2\rho \quad (16)$$

将式 (16) 简化后得:

$$D^q V^{q-\lambda} \leq -2\rho \frac{\Gamma(1+q-\lambda)}{\Gamma(1-\lambda)} \quad (17)$$

对式 (17) 两边在 $0 \rightarrow t$ 求积分后可得:

$$V(t)^{q-\lambda} - V(0)^{q-\lambda} \leq -2\rho \frac{\Gamma(1+q-\lambda)}{\Gamma(1-\lambda)\Gamma(1+q)} t^q \quad (18)$$

因此, 当 $t \leq \left[V(0)^{q-\lambda} \frac{\Gamma(1-\lambda)\Gamma(1+q)}{\Gamma(1+q-\lambda)2\rho} \right]^{\frac{1}{q}}$ 时, 系统在有限时

间内是趋于稳定的。

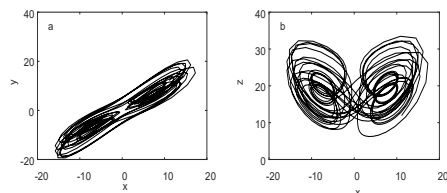
定理 1 证毕。

3 分数阶 Chen 超混沌系统的描述

分数阶 Chen 超混沌系统模型为研究对象, 其驱动系统表示为:

$$\begin{cases} D^q x_1 = a(y_1 - x_1) + w_1 \\ D^q y_1 = bx_1 - x_1 z_1 + cy_1 \\ D^q z_1 = x_1 y_1 - dz_1 \\ D^q w_1 = y_1 z_1 + rw_1 \end{cases} \quad (19)$$

式中: α 为阶数 ($0 < \alpha < 1$)。在 Matlab 中对系统进 $c=28$ 行仿真, 取 $\alpha=0.96$, 参数 $a=35, b=3$, 设置系统初始值 $x_1(0)=10, y_1(0)=10, z_1(0)=10, w_1(0)=10$, 得到分数阶 Chen 系统相空间的混沌吸引子如图 1 所示。其中图 (a)、图 (d) 分别为系统 x - y 、 x - z 、 y - z 、 y - w 的相空间混沌吸引子, 由图 1 可知分数阶 Chen 超系统确实存在混沌现象。



(a) x - y

(b) x - z

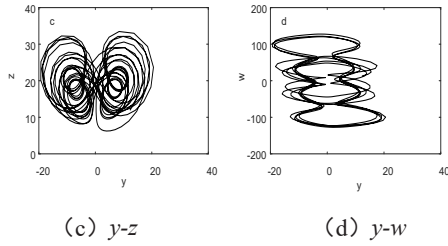


图 1 系统 (19) 的超混沌吸引子

根据式 (3) 和 (4) 的描述, 则式 (19) 为驱动系统, 那么相应的响应系统为:

$$\begin{cases} D^q x_2 = a(y_2 - x_2) + w_2 + u_1 \\ D^q y_2 = bx_2 - x_2 z_2 + cy_2 + u_2 \\ D^q z_2 = x_2 y_2 - dz_2 + u_3 \\ D^q w_2 = y_2 z_2 + rw_2 + u_4 \end{cases} \quad (20)$$

式中: $u=[u_1, u_2, u_3, u_4]^T$ 是控制函数。定义误差为 $e_1=x_2-x_1$, $e_2=y_2-y_1$, $e_3=z_2-z_1$, $e_4=w_2-w_1$, 则由式 (20) 减去式 (19), 得同步误差系统为:

$$\begin{cases} D^q e_1 = a(e_2 - e_1) + e_4 + u_1 \\ D^q e_2 = (b - z)e_1 + ce_2 + x'e_3 + u_2 \\ D^q e_3 = -de_3 + xe_2 + (y + e_2)e_1 + u_3 \\ D^q e_4 = re_4 + ze_2 - y'e_3 + u_4 \end{cases} \quad (21)$$

构造控制函数为:

$$\begin{cases} u_1 = -ae_1 - \rho e_1^\omega \\ u_2 = -b(e_1 + e_2) + z_1 e_1 - ce_2 - x_2 e_3 - \rho e_2^\omega \\ u_3 = -x_2 e_2 - (y_2 + e_2)e_1 - \rho e_3^\omega \\ u_4 = -2re_4 - z_2 e_2 + e_3 - \rho e_4^\omega \end{cases} \quad (22)$$

将式 (22) 代入式 (21), 得到同步误差动态方程为:

$$\begin{cases} D^q e_1 = -ae_1 - \rho e_1^\omega \\ D^q e_2 = -be_2 - \rho e_2^\omega \\ D^q e_3 = -de_3 - \rho e_3^\omega \\ D^q e_4 = -re_4 - \rho e_4^\omega \end{cases} \quad (23)$$

因此, 从分析分数阶超混沌系统之间的同步问题, 就可以转换为分析误差系统, 其是否满足向零点收敛, 即误差系统在无限的时间内趋于 0。根据定理 1 的条件, 从任意值出发, 系统 (21) 都将会在有限时间 t 内趋向于 0, 那么分数阶超混沌系统 (19) 和 (20) 即实现有限时间同步。

证明:

选取 Lyapunov 函数:

$$V(t) = \frac{1}{2} e^T(t) e(t) \quad (24)$$

根据引理 4 可得:

$$D^q V(t) \leq e^T D^q e \quad (25)$$

再根据上式可得:

$$\begin{aligned} e^T D_t^q e &= [e_1 e_2 e_3 e_4]^T D_t^q [e_1 e_2 e_3 e_4] \\ &= e_1(-ae_1 - \rho e_1^\omega) + e_2(-be_2 - \rho e_2^\omega) \\ &\quad + e_3(-de_3 - \rho e_3^\omega) + e_4(-re_4 - \rho e_4^\omega) \\ &= -ae_1^2 - \rho e_1 e_1^\omega - be_2^2 - \rho e_2 e_2^\omega \\ &\quad - de_3^2 - \rho e_3 e_3^\omega - re_4^2 - \rho e_4 e_4^\omega \\ &\leq -\rho e_1 e_1^\omega - \rho e_2 e_2^\omega - \rho e_3 e_3^\omega - \rho e_4 e_4^\omega \\ &= -\rho(e_1^2)^{\frac{1+\omega}{2}} - \rho(e_2^2)^{\frac{1+\omega}{2}} - \rho(e_3^2)^{\frac{1+\omega}{2}} - \rho(e_4^2)^{\frac{1+\omega}{2}} \end{aligned} \quad (26)$$

由引理 3 得:

$$\begin{aligned} &-\rho(e_1^2)^{\frac{1+\omega}{2}} - \rho(e_2^2)^{\frac{1+\omega}{2}} - \rho(e_3^2)^{\frac{1+\omega}{2}} - \rho(e_4^2)^{\frac{1+\omega}{2}} \\ &\leq -\rho(e_1^2 + e_2^2 + e_3^2 + e_4^2)^{\frac{1+\omega}{2}} \end{aligned} \quad (27)$$

故有:

$$\begin{aligned} e^T D_t^q e &= [e_1 e_2 e_3 e_4]^T D_t^q [e_1 e_2 e_3 e_4] \\ &\leq -\rho(e_1^2 + e_2^2 + e_3^2 + e_4^2)^{\frac{1+\omega}{2}} \\ &= -\rho([e_1 e_2 e_3 e_4]^T [e_1 e_2 e_3 e_4])^{\frac{1+\omega}{2}} \\ &= -\rho(e^T e)^{\frac{1+\omega}{2}} \end{aligned} \quad (28)$$

将参数表达式代入定理的有限时间公式中, 可以得到:

$$t \leq \left[(e^T e)^{q-\frac{1+\omega}{2}} \frac{\Gamma(1-\frac{1+\omega}{2})\Gamma(1+q)}{\Gamma(1+q-\frac{1+\omega}{2})2\rho} \right]^{\frac{1}{q}} \quad (29)$$

式中: $\lambda=(1+\omega)/2$ 。可以看出, 通过证明, 式 (29) 符合定理 1 中所约束的要求, 并且代入有限时间公式中, 也是符合有限内容趋于同步的时间条件。因此, 误差系统 (21), 通过构造合适的控制器函数 (22), 在有限的时间 t 内是收敛的, 并且是稳定的, 即验证了系统在有限的时间内是能实现同步的。

在 Matlab 中对分数阶超混沌系统进行模拟仿真, 以此来验证系统 (19) 和系统 (20) 在有限时间内系统实现同步。取系统参数 $a=35$, $b=7$, $c=12$, $d=3$ 和 $r=0.5$, $\rho=2$, $\omega=0.5$, $\alpha=0.96$; 驱动系统 (7) 的初始值为 $x_1(0)=10$, $y_1(0)=10$, $z_1(0)=10$, $w_1(0)=10$; 响应系统 (8) 的初始值为 $x_2(0)=-10$, $y_2(0)=-10$, $z_2(0)=-10$, $w_2(0)=-10$ 。误差系统的仿真结果如图 2 所示。从图 2 中可知通过构造控制函数式 (22), 证实了在有限的时间内误差 $e_1(t)$, $e_2(t)$, $e_3(t)$ 和 $e_4(t)$ 均收敛于 0 并且是稳定的, 即系统 (8) 与系统 (7) 在有限时间内实现了同步, 其各个状态变量随时间的同步曲线如图 3 ~ 图 6 所示。

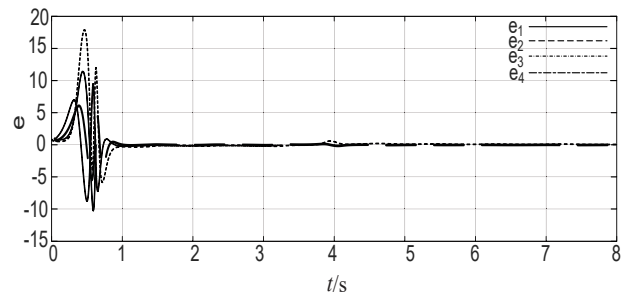


图 2 误差曲线

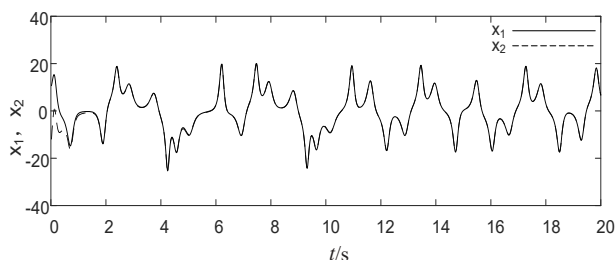


图 3 x_1, x_2 同步曲线

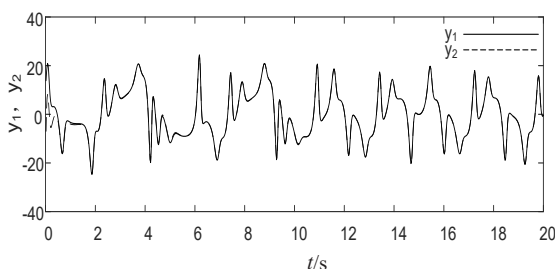


图 4 y_1, y_2 同步曲线

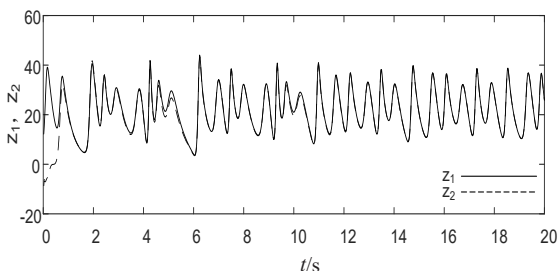


图 5 z_1, z_2 同步曲线

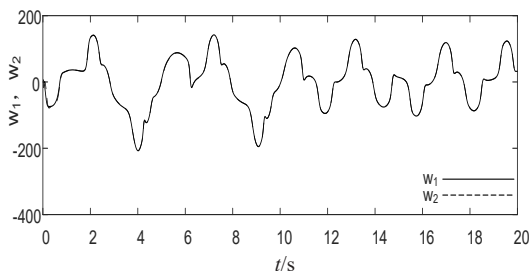


图 6 w_1, w_2 同步曲线

4 铁路安全通信的混沌加密方法

4.1 铁路通信的混沌加密方案

铁路安全通信主要是利用 RSSP- II 协议中的安全功能模块进行安全保护,保障铁路设备之间的通信。安全功能模块中的消息鉴定层(MASL)是整个通信安全保护的核心功能如图 7 所示。子系统 A 和子系统 B 要实现通信,就要先进行密钥认证,经过双方认证成功才能进行信息交换,这样就可以有效保护信息的安全传送。但是这种方案是基于密码学原理,在密钥交换、密钥传送以及密码本身等方面都可能存在潜在风险。

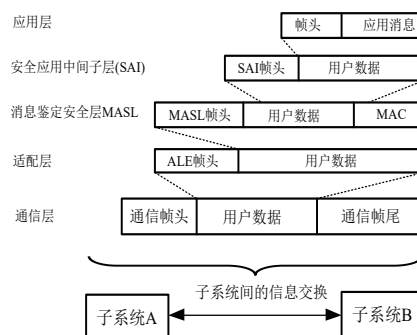


图 7 RSSP- II 协议中定义的消息结构

结合混沌掩盖技术,在不改变 RSSP- II 协议基础上,从数据保护的角度对传送信号进行混沌加密,利用混沌信号的特性对传输信号进行保密传送,如图 8 所示。在子系统 A 中通过加密函数把传送信号加密到混沌信号中以混合信号传送,在子系统 B 再通过相应的混沌同步信号对传送信号进行解密,最后恢复出有用信号,达到安全保密传送的目的。

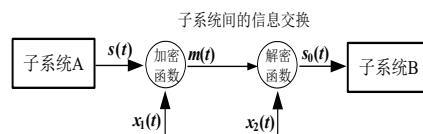


图 8 混沌加密示意图

4.2 数值仿真

为了验证所提方案的可行性,对方案进行模拟仿真。传送信号选择幅度为 2,周期为 1 s 的正弦波信号作为 $s(t)$ 信号进行模拟仿真,如图 9 所示。经过混沌加密后以混合信号 $m(t)$ 进行传输如图 10 所示。这种经过混沌加密后的信号与原信号几乎完全不一样,安全性得到了极大的提高。最后通过解密函数对原信号进行混沌解密,得到解密的信号 $s_0(t)$,大约经过 2.2 s 与原信号 $s(t)$ 完全同步,如图 11 所示。

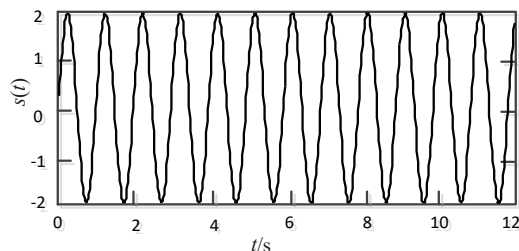


图 9 随机信号图

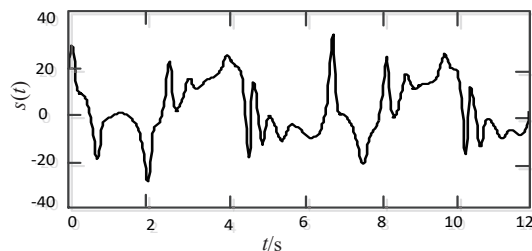


图 10 混沌密钥加密信号

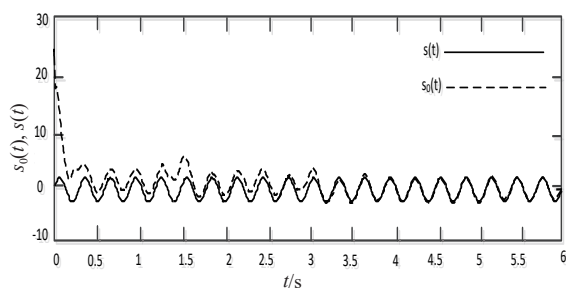


图 11 原信号与解密信号对比图

5 结语

我国铁路是利用 RSSP- II 铁路安全通信协议保障铁路的通信安全,但是数据在传输过程中会遇到不同程度的攻击者,威胁到铁路通信的安全可靠性,势必需要找到一种新的加密方法改善铁路的安全通信。混沌信号具有高度的类随机、非周期、对初值极度敏感等特性,特别是分数阶超混沌系统具有比低位系统更为宽广的密钥空间,相对其他加密方式具有更高的安全性。因此,结合 RSSP- II 铁路安全通信协议,在不改变原有安全通信协议框架结构的前提下,尝试在安全保护模块中对数据信息进行混沌加密保护,希望以此来确保数据信息的安全传送。最后,通过数据仿真分析,大于经过 2.2 s 恢复了传送数据信息。数值仿真结果验证了理论分析的一致性。铁路安全通信关系到乘客的生命财产安全,随着高铁速度的进一步提速,铁路安全通信需要寻找一种更加高级、更加安全可靠的加密方式。下一步研究工作将结合量子通信中量子的不可克隆性和不可分割性的特点,在通信过程中提高安全性,研究量子混沌密钥加密改善铁路安全通信的新算法。

参考文献:

- [1] 郭伟,闫连山,王小敏,等.RSSP- II 铁路信号安全通信协议的安全性分析[J].铁道学报,2016,38(8):50-56.
- [2] 张元玲,徐中伟,万勇兵,等.铁路信号安全通信协议中的 MAC 改进算法[J].计算机工程,2012,38(3):246-248.
- [3] 陈黎洁,单振宇,唐涛.列车运行控制系统中安全通信协议的形式化分析[J].铁道学报,2012,34(7):70-76.
- [4] 周宏伟,张涛,苗长俊.RSSP- I 与 RSSP- II 铁路安全通信协议对比分析[J].铁道通信信号,2013,49(1):76-78.
- [5] 左林,刘贞,王一民.SM4 分组密码算法在 RSSP- II 铁路信号安全通信协议中的应用[J].铁路通信信号工程技术,2020,17(8):24-27.
- [6] 方锦清.驾驭混沌与发展高新技术[M].北京:原子能出版社,2002.
- [7] 蒋逢灵,刘贤群,邓景新,等.分数阶混沌系统同步及其在保密通信中的应用[J].长江信息通信,2023,36(11):58-62.
- [8] 牛士铭,薛茹,丁聪.基于改进型 3D_Henon 混沌映射的彩色图像加密方法[J].计算机工程与科学,2024,46(4):657-666.
- [9] 鄢懿,张灿,郭振永.基于混沌密钥控制的联合信源信道与安全算术码编译码算法[J].电子与信息学报,2016,38(10):2553-2559.
- [10] EDWARD O, CELSO G, JAMES A. Controlling chaos[J]. Physical review letters,1990,64(11):1196-1199.
- [11] PECORA L M, CARROLL T L. Synchronization in chaotic system[J]. Physical review letters,1990,64(8):821-824.
- [12] MODIRI A, MOBAYEN S. Adaptive terminal sliding mode control scheme for synchronization of fractional-order uncertain chaotic systems[J]. ISA transactions,2020,105:33-50.
- [13] REMERO M, MANOSO C. Fractional generalized predictive control strategy with fractional constraints handling[J]. IEEE access,2022,10:128779-128789.
- [14] TRIKHA P, JAHANZAIB LS, NASREEN, et al. Dynamical analysis and triple compound combination antisynchronization of novel fractional chaotic system[J]. Journal of vibration and control, 2022,28(9-10):1057-1073.
- [15] ATANGANA A. On the new fractional derivative and application to nonlinear Fisher's reaction-diffusion equation[J]. Applied mathematics and computation, 2016, 15(273): 948-956.
- [16] LI C, DENG W. Remarks on fractional derivatives[J]. Applied mathematics and computation,2006,187(2):777-784.
- [17] 胡建兵,肖建,赵灵冬.阶次不等的分数阶混沌系统同步[J].物理学报,2011,60(11):181-184.
- [18] BECKENBACH E F, BELLMAN R. Inequalities[M]. Berlin: Springer Science&Business Media, 2012.
- [19] OUANNAS A, ODIBAT Z, HAYAT T. Fractional analysis of coexistence of some types of chaos synchronization[J]. Chaos solitons & fractals, 2017,105:215-223.
- [20] 郑广超,刘崇新,王琰.一种具有隐藏吸引子的分数阶混沌系统的动力学分析及有限时间同步[J].物理学报,2018,67(5):43-50.

【作者简介】

蒋逢灵(1982—),男,湖南道县人,硕士,副教授,研究方向:混沌理论及应用。

(收稿日期:2024-05-20)