

考虑并行干扰抵消的通信网络 终端敏感信息混沌加密

任彦龙, 魏楚元, 胡晓霞, 李 欣

(北京建筑大学 数字化与智算中心, 北京 100044)

摘要: 针对传统通信网络终端敏感信息的加密方法通常无法兼顾信号的高敏感性和复杂环境下的鲁棒性, 从而使加密后的信息容易被破解或篡改的问题, 提出一种基于并行干扰抵消技术和演化超网络模型的混沌加密解决方案. 首先, 通过最小均方误差构建权值矢量矩阵, 实现各用户干扰信号的估计和排序, 并从中减除干扰, 以提升目标信号的质量; 其次, 引入演化超网络模型, 利用超边关联规则确定信息样本的敏感性, 构建决策分类模型, 实现对敏感数据的挖掘; 最后, 利用 Lyapunov 指数衡量混沌序列的敏感性, 结合前馈流密码机制及置乱处理, 生成高安全性敏感信息密钥流, 以确保加密过程中的高敏感性和复杂环境下的鲁棒性, 从而提高加密信息的安全性和抗破解能力. 实验结果表明, 该方法能提高加密方法的抗干扰能力, 在提高信息传输效率的同时保证信息安全.

关键词: 通信网络安全; 敏感信息; 并行干扰抵消; 混沌运动; 混沌映射; Lyapunov 指数

中图分类号: TP393 **文献标志码:** A **文章编号:** 1671-5489(2026)03-0657-08

Chaos Encryption of Sensitive Information in Communication Network Terminals Considering Parallel Interference Cancellation

REN Yanlong, WEI Chuyuan, HU Xiaoxia, LI Xin

(Center of Digitalization and Intelligent Computing,
Beijing University of Civil Engineering and Architecture, Beijing 100044, China)

Abstract: Aiming at the problem that traditional encryption methods for sensitive information in communication network terminals often failed to balance the high sensitivity of signals and robustness in complex environments, making encrypted information vulnerable to cracking or tampering, we proposed a chaotic encryption solution based on parallel interference cancellation technology and evolutionary hypernetwork model. Firstly, by constructing a weight vector matrix with minimum mean square error, the estimation and ranking of interference signals from each user could be achieved, and interference could be subtracted from them to improve the quality of the target signal. Secondly, an evolutionary hypernetwork model was introduced to determine the sensitivity of information samples by using hyperedge association rules, construct a decision classification model, and achieve mining of sensitive data. Finally, by using Lyapunov exponent to measure the sensitivity of chaotic sequences, combined with feedforward stream cipher mechanism and scrambling processing, a high

收稿日期: 2025-02-13.

第一作者简介: 任彦龙(1991—), 男, 汉族, 硕士, 实验师, 从事网络安全和大数据分析的研究, E-mail: renyanlong@bucea.edu.cn.

基金项目: 北京市数字教育研究课题重点项目(批准号: BDEC2022619014)和校设科研基金自然科学基金项目一般项目(批准号: ZF16073).

security sensitive information key stream was generated to ensure high sensitivity and robustness in complex environments during the encryption process, thereby improving the security and anti cracking ability of encrypted information. The experimental results show that the proposed method can improve the anti-interference ability of encryption methods, and enhance the transmission efficiency of information while ensuring information security.

Keywords: communication network security; sensitive information; parallel interference cancellation; chaotic motion; chaotic mapping; Lyapunov exponent

通信网络终端作为信息传递的端点,承载着海量的数据交换工作,目前已成为现代社会不可或缺的一部分^[1].但在享受便捷高效的通讯服务时,也面临信息安全的挑战^[2].敏感信息(如个人身份资料、金融交易记录、商业机密等)在传输过程中一旦被泄露或篡改,即可能会导致严重后果^[3].因此,如何确保这些敏感信息的安全性已成为通信网络设计和运营中必须优先考虑的问题之一.加密技术是保护数据安全的重要方法^[4],对通信网络终端进行有效的加密措施可显著提升数据传输的安全等级,为用户隐私和企业利益建立坚固的防线.

胡栋鹏等^[5]提出了一种融合区块链技术的加密方案.在数据加密过程中,加密模块先由密钥管理中心提供的公钥加密原始数据,形成加密后的密文,而授权用户则可利用私钥从云端服务器解密这些数据包,恢复原始的明文数据;然后采用支持多关键字检索功能的公钥加密机制,确保即使在加密状态下也能实现精确的内容搜索;最后,基于格理论的密文策略属性基加密方法,保护数据索引的安全性,以实现更细粒度的加密.该方法仅依靠区块链技术并不能完全解决数据在传输过程中的高敏感性和鲁棒性问题,无法提供足够的防护.周娟等^[6]创建了一个查询表,对敏感信息进行标记;通过逆向查找初始数据中的关键字位置,分析这些关键字的位置属性、状态和出现频率,据此动态生成对应的加密密钥;引入时间戳记录数据包在网络中传输的时间点,反映网络的实时动态特性;构建一个表示异质信息网络的无向图模型,使用混淆矩阵掩盖数据的真实结构;根据节点在不同时间点的行为轨迹,生成一个加密序列,实现加密.查询表的创建和维护依赖于敏感信息的准确标记,如果标记不准确或存在遗漏,则可能导致加密密钥生成错误,从而影响加密的安全性.Liu^[7]根据信息的具体存储格式,将原始数据分解为最基本的二进制构成,通过特定规则对这些二进制位进行交换处理,引入首次的混淆和扩散,从而完成第一阶段加密;利用三维空间内的混沌置乱技术,对已经过初步加密的信息施加更深层次的扰乱,使经过一级加密的数据块在该环境中按混沌轨迹动态地重新排列,从而实现了二级加密的目标,确保信息的高度保密性和安全性.尽管二进制位交换可增加信息的混乱程度,但这种简单交换规则可能易被攻击者通过统计分析方法破解.Liu等^[8]结合压缩感知理论和数论中的剩余定理,通过引入非线性加密机制,减少计算资源有限的终端设备在处理数据时所需的计算量和能量消耗;融入超混沌系统,应用数学变换、位异或操作以及数据随机置乱技术,对已经过初步压缩加密的数据进行再次加密.随机置乱的效果受多种因素影响,无法兼顾信号的高敏感性和复杂环境下的鲁棒性,从而使加密后的信息易被破解或篡改,导致加密后的数据存在安全隐患.

为解决上述问题,本文提出考虑并行干扰抵消的通信网络终端敏感信息混沌加密方法.通过并行干扰抵消技术,对多个重叠信号进行分离和处理,进而提高通信信号质量;利用混沌系统的不可预测性和动态特性增强数据保护机制,提供更高安全性的加密方法.

1 考虑并行干扰抵消的敏感信息处理

1.1 并行干扰抵消

在通信网络终端敏感信息加密过程中,面临的主要挑战是如何在保持高敏感性的同时,确保信息在复杂环境下的鲁棒性,避免被外部攻击者破解或篡改.传统加密方法通常难以同时满足这两个要求.并行干扰抵消是一种信号处理技术,用于减少这种多用户干扰^[9-10].其基本原理是先对多个干扰用户的信号进行估计和抵消,然后从接收信号中减去估计的干扰信号,改善接收信号的性能,从而提

高目标信号的质量. 因此, 通过最小均方误差构建权值矢量矩阵, 实现各用户干扰信号的估计和排序, 并从中减除干扰, 以提升目标信号的质量. 这种方法不仅能有效减少外部干扰, 提高信号的鲁棒性和清晰度, 还能增强加密信息的安全性, 确保在复杂环境下信息的完整性和可靠性.

在通信网络终端中, 假设存在 A 个用户通过频率选择性衰落信道并传输信息. 每个用户的接收信号经历 B 条独立的多径传播路径, 并采用扩频技术以获得扩频增益 C , 接收端配置 D 个天线阵元捕捉信号^[11]. 在码元间隔中, 设第 u 个接收天线捕获到的离散基带信号为

$$z_u = \mathbf{S}\mathbf{G}_u \mathbf{E}y + \mathbf{e}_u, \quad (1)$$

其中: $\mathbf{S}$ 表示 $A \times AB$ 的扩频码矩阵, $\mathbf{S} = (s_{11}, \dots, s_{1B}, s_{A1}, \dots, s_{AB})$, s_{AB} 为第 a 个用户通过第 b 条可分辨多径传播时使用的扩频序列; $\mathbf{G}_u$ 表示 $ABD \times A$ 的扩频码矩阵; E 表示码元幅值; y 表示通信网络数据码元; $\mathbf{e}_u$ 表示高斯噪声向量.

接收到信号后, 基于最小均方误差准则构建权值矢量矩阵^[12]:

$$\mathbf{F} = (\mathbf{Z}^H \mathbf{Z} + \sigma^2 \mathbf{z}_u)^{-1} \mathbf{Z}^H, \quad (2)$$

其中 $\mathbf{Z}$ 表示接收信号矩阵, $\mathbf{Z}^H$ 表示权值矢量矩阵的共轭转置, σ^2 表示高斯方差值. 对权值矢量矩阵中的矢量进行排序:

$$f(\mathbf{F}) = \arg \min_{z_u \in \mathbf{Z}} \|\mathbf{F}\|^2, \quad (3)$$

其中 $\|\cdot\|$ 表示范数计算. 基于式(3)的排列顺序, 抵消网络信息数据的干扰, 生成发送信号 v 的软判决:

$$r = \mathbf{F}\mathbf{z}_u. \quad (4)$$

再对软判决后的发送信号进行硬判决, 获得信号 v 的估计值:

$$\hat{v} = Q(r), \quad (5)$$

其中 $Q(\cdot)$ 表示硬判决.

在通信网络终端中, 采用并行干扰估计与逐级抵消技术处理干扰. 在抵消特定天线信号时, 并行估算所有天线的干扰, 并利用之前步骤中已判决的数据逐步减少当前信号中的干扰成分. 表明在算法的每一步迭代中, 都会使用上一步(($i-1$)步)所获得的判决结果以减轻接收信号中的干扰. 为进一步优化该过程, 在每个迭代步骤中, 根据对先前估计值的置信程度, 引入抵消因子 β . 该因子用于按比例抵消干扰, 降低由于早期误判而导致的错误传播风险, 在保持性能的同时有效管理干扰.

先获得信号 v 的第 i 步软判决结果:

$$r(i) = \beta_i \times \text{diag}\left(\frac{1}{\mathbf{I}}\right) \times [\mathbf{z}_u - \mathbf{I}(i)] + (1 - \beta_i) \times r(i-1), \quad (6)$$

$$\mathbf{I}(i) = \mathbf{I} \times \hat{v}(i-1), \quad (7)$$

其中 $\mathbf{I}$ 表示干扰矩阵, $\mathbf{I}(i)$ 表示第 i 步的信号干扰. 再对估计信号进行硬判决, 得到进一步抵消干扰后的信号数据:

$$\hat{v}(i) = Q(r(i)). \quad (8)$$

1.2 敏感信息挖掘

经过并行干扰抵消后, 仍存在信息样本敏感性识别不准确及加密密钥流生成不稳定的问题, 可能导致加密后的信息仍易受攻击. 为进一步提升加密信息的安全性和鲁棒性, 需引入演化超网络模型^[13], 利用超边关联规则准确识别信息样本的敏感性, 并构建决策分类模型, 实现对敏感数据的精准挖掘. 该步骤旨在增强系统在复杂环境下的防护能力, 确保加密信息在传输过程中的完整性和安全性.

演化超网络即将通信网络终端信息变化模拟成超网络的动态过程, 并将此动态视角整合进敏感信息挖掘框架内. 在该方法中, 将经过并行干扰抵消处理的信息数据点视为超网络中的节点^[14], 构建一个以超网络为基础的决策分类模型 W . 通过通信网络终端的信息输入输出对, 建立训练集 K , 并对其进行演化, 得

$$K = (\hat{v}_j, y_j)_{j=1}^N, \quad (9)$$

其中： N 和 c 分别为训练集的数据总数量和维度， y_j 为第 j 个通信网络终端信息样本 $\hat{v}$ 的类别，这里分为敏感性和非敏感性。

在超网络结构中，每条超边都关联一个决策分类规则，而与这条超边相连接的节点则代表用于信息分类的决策属性^[15]。在实际应用中，超网络被用来表示输入信息样本 $\hat{X}$ 及其所属类别 Y 之间的联合概率分布 $P(\hat{X}, Y)$ 。把超网络应用于通信网络终端信息分类时，该过程可被视为计算输入信息样本属于敏感或非敏感信息类型的条件概率。目标是确定哪个类别对输入信息样本有最大条件概率^[16]，并将该类别作为通信网络终端信息样本的最终结果 $\hat{y}$ 。上述过程可表示为

$$\hat{y} = \operatorname{argmax}_{Y \in \{0,1\}} P(\hat{X}, Y) \left(\frac{Y}{\hat{X}} \right), \tag{10}$$

$$P(\hat{X}, Y) \approx \frac{1}{|M|} \sum_{j=1}^{|M|} g_j^h, \tag{11}$$

其中 $|M|$ 为超网络超边的总数量， g_j^h 为第 j 个超边。如果超边和信息样本直接有匹配，则 $g_j^h = 1$ ，表明该信息样本为敏感信息；否则 $g_j^h = 0$ 。

通过上述步骤，演化超网络模型能准确识别信息样本的敏感性，并实现对敏感数据的精准挖掘，从而提升加密信息的整体安全性和鲁棒性。

2 基于混沌理论的通信网络终端敏感信息加密

2.1 Lyapunov 指数衡量混沌序列的敏感性

经敏感数据挖掘后，存在混沌序列对初始条件高度敏感的问题，这可能导致加密信息在传输过程中易受外部攻击。为进一步提升加密信息的安全性和鲁棒性，需利用 Lyapunov 指数衡量混沌序列的敏感性^[17]。通过量化初始邻近点在迭代过程中的分离程度，可更准确地评估系统的稳定性和不稳定性，从而有效增强加密信息在复杂环境下的防护能力，确保其在传输过程中的完整性和安全性。

为深入分析混沌序列中的吸引子特性，需确定混沌轨道的平均统计特征。在常规条件下，混沌运动表现出对初始条件的高度敏感性，这表明即使是非常接近的起始位置和速度，随着时间的增加，所生成的轨迹也会逐渐发散。利用 Lyapunov 指数刻画此现象^[18]。对于一维动力系统混沌序列 $x_{m+1} = J(x_m)$ ，初始两个邻近点在迭代过程中的行为受函数导数 $\left| \frac{dJ}{dx} \right|$ 的影响。如果 $\left| \frac{dJ}{dx} \right| > 1$ ，则说明这两个点在混沌序列中将趋于分离；相反，如果 $\left| \frac{dJ}{dx} \right| < 1$ ，则迭代会使这两点逐渐靠近。在混沌序列加密迭代过程中， $\left| \frac{dJ}{dx} \right|$ 的值会动态变化，导致迭代过程在分离和聚合之间不断切换，可表示为

$$\lambda = \lim_{m \rightarrow \infty} \frac{1}{m} \sum_{m=1}^m \hat{y} \ln \left| \frac{dJ(x)}{dx} \right|_{x_m}, \tag{12}$$

其中： m 为迭代次数； λ 为经过多次迭代后每次迭代导致的状态分离程度指数，即平均指数分离率。当 $\lambda < 0$ 时，说明两个点会趋向于彼此靠近并可能合并为一点，这种情况对应于系统中的稳定不动点和周期性行为；当 $\lambda > 0$ 时，说明两个点将逐渐分离，反映轨道的局部不稳定性。通过这种分析，可更全面地理解混沌序列的特性，从而提高加密信息的安全性和鲁棒性。

2.2 敏感信息混沌加密

经过 Lyapunov 指数衡量混沌序列的敏感性后，虽能有效评估系统的稳定性和不稳定性，但仍需进一步提升密钥流生成的稳定性和加密系统的鲁棒性，以确保在复杂环境下的高安全性。因此，结合前馈流密码机制及置乱处理^[19-20]，生成高安全性敏感信息密钥流。但仍需不断优化这些关键技术，以应对未来潜在的安全威胁。该方法不仅提升了密钥流的生成质量，还增强了加密信息的整体防护能力，但仍有改进空间，为通信网络终端的敏感信息安全提供更可靠的技术保障^[21]。

在该加密方案中，初次加密过程直接采用混沌前馈型密码技术。该技术依赖于系统对初始条件的高度敏感性，并通过反复迭代演进以满足加密强度的需求。加密过程中采用分段线性混沌映射^[22]，映

射结果为

$$x(k+1)=J(x(k))=\begin{cases}\lambda x(k)/q, & 0\leqslant x(k)<q, \\ \lambda(x(k)-q)/(0.5-q), & q\leqslant x(k)<0.5, \\ J(1-\lambda x(k)), & 0.5\leqslant x(k)<1, \end{cases}\quad (13)$$

其中 $J(x(k))$ 表示计算出的 Lyapunov 指数序列, $x(k)$ 表示混沌加密的密钥流, q 表示不变分布系数. 首先, 使用加密驱动信号 $p(k)$ 作为混沌映射的输入信息. 其次, 由式(13)生成的混沌序列中选取 o 序列, 并将其转换为连续的 o' 位输出信号. 该输出信号之后被用于将数据映射到区间 L 内, 从而形成新的驱动信号 $p'(k)$. 这个新的驱动信号会推动混沌序列的迭代过程. 选择特定的二进制位作为密钥流的一部分, 这些抽取的二进制位构成的密钥流则用于加密过程.

- 为增强加密密码的复杂性和信息的安全性, 对混沌密码进行置乱处理, 步骤如下:
- 1) 加密驱动信号加密敏感信息, 生成初始密钥 $x(0)$, 将密钥表示为一个正方形矩阵. 设矩阵中的任意一点坐标为 (s, t) , 把该点变换到新的位置 (s', t') . 该过程改变了原始矩阵中元素的位置, 形成一个新的信息布局.
 - 2) 由于坐标变换可能有一定的周期性, 即经过一定次数的变换后可能会重复原有的序列模式. 为避免这种情况, 当变换使用次数过多时, 根据相应的迭代过程调整迭代周期 T 和信息之间的依赖关系, 以确保不会过早出现重复模式.
 - 3) 根据给定的密码阶数, 在 l 维空间中执行变换. 采用多次变换方法进行多次操作, 直至达到满意的加密效果为止.

通过上述方法, 不仅解决了密钥流生成不稳定和安全性不足的问题, 还显著提高了加密信息的安全性和抗破解能力, 确保了加密过程中的高敏感性和复杂环境下的鲁棒性.

3 实验分析

3.1 实验环境

为验证本文方法在实际应用中的效果, 分别使用本文方法、区块链技术和时间戳方法对通信网络终端敏感信息进行加密, 实验环境如图 1 所示.



图 1 实验环境

Fig. 1 Experimental environment

实验搭建包括通信网络终端设备、路由器和接收端设备. 终端与路由器之间以及路由器与接收端之间的连接带宽为 12 Mbps. 通信系统的往返延迟为 12 ms, 信道带宽为 4 kHz, 理论上可支持的最大数据传输速率达 40 Mbps. 实验的其他参数如下: 抵消因子为 1.8, 初始信噪比为 25 dB, 天线数量为 8, 采样频率为 2 kHz, 量化位数为 8, 训练集数据量为 17 000, 迭代周期为 10, 迭代次数为 110.

3.2 实验分析

3.2.1 抗干扰能力

在实际通信环境的并行干扰抵消性能测试中, 干扰的强度和特性不断变化, 抵消因子是用于衡量对于干扰信号进行抵消程度的参数. 实验分别使用不同的抵消因子 $\beta=0.05, 0.1, 0.5, 0.7$, 得到不同抵消因子下的误码率与信噪比之间的关系, 结果如图 2 所示. 由图 2 可见, 当 $\beta=0.05$ 时, 随着信噪比的

增加, 误码率能维持在较低水平, 说明此时的通信网络性能最好, 因此, 后续将维持在抵消因子为 0.05 的情况下进行实验.

令本文方法中抵消因子为 0.05, 对比区块链技术和时间戳方法, 分析 3 种方法在同一通信网络终端的误码率变化情况, 结果如图 3 所示. 由图 3 可见, 随着信噪比的增加, 本文方法误码率的下降幅度更大, 表明该方法有更强的抗干扰能力. 这是由于并行干扰抵消技术能先从复杂的干扰环境中提取出敏感信息, 从而更好地保持了信息的完整性和保密性, 减少了外部干扰对加密信息的影响. 进一步分析表明, 该方法通过精确识别和分离敏感信息, 显著降低了外部噪声和干扰对加密系统的破坏, 从而在提高加密信息的安全性和抗破解能力方面表现出色.

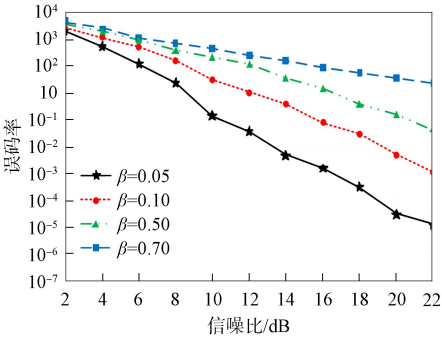


图 2 不同抵消因子下信号误码率与信噪比的关系
Fig. 2 Relationship between signal error rate and signal-to-noise ratio under different cancellation factors

3.2.2 加密性能

在对通信网络终端信息进行加密时, 如果明文位数足够多, 则密文的模式就会变得更复杂和难以预测. 分别使用上述 3 种方法对敏感信息进行加密, 得到明文位数随着迭代次数增加的结果如图 4 所示. 由图 4 可见, 本文方法加密后的明文位数更多, 说明信息被暴力破解的难度更大, 从而进一步证明了本文方法的加密性能更优. 这是由于并行干扰抵消技术为混沌加密提供了一个相对干净的传输环境, 减少了外部干扰对加密信息的影响. 该技术能有效分离并抑制噪声, 确保敏感信息在传输过程中保持较高的完整性和保密性. 通过精确识别和过滤干扰, 本文方法显著降低了外部干扰对加密系统的破坏, 提高了加密信息的安全性和抗破解能力. 这种环境不仅减少了信息被破坏的风险, 还增强了系统的鲁棒性, 使暴力破解变得更困难.

3.2.3 信息传输性能

信息传输性能分析能直接反映加密后的信息是否能以足够的速率进行传输, 上述 3 种方法的通信网络信息传输时滞性能如图 5 所示. 由图 5 可见, 本文方法在 7 s 时即能进入时滞稳定状态, 而区块链技术和时间戳方法分别在 10 s 和 14 s 达到稳定, 表明本文方法在加密过程中有更好的信息传输性能.

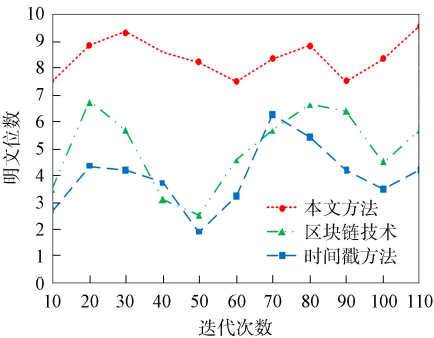


图 4 不同方法的加密效果
Fig. 4 Encryption effects of different methods

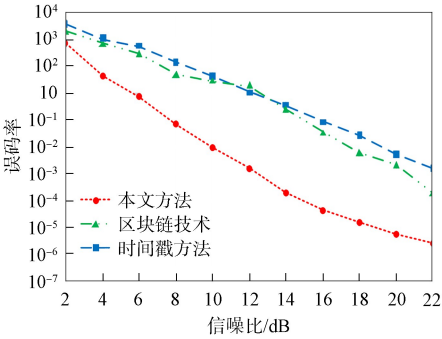


图 3 不同方法的抗干扰能力
Fig. 3 Anti-interference ability of different methods

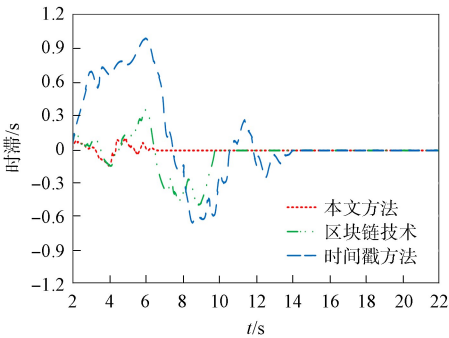


图 5 不同方法的信息传输时滞结果
Fig. 5 Results of information transmission delay by different methods

这是由于并行干扰抵消和混沌加密的结合可优化资源利用, 从而节省了传输资源, 使信息能以更高效的方式传输. 这种方法通过并行干扰抵消技术有效减少了外部干扰, 确保了信息在传输过程中的完整性和保密性. 同时, 混沌加密机制提供了更高的随机性和不可预测性, 进一步增强了加密信息的安全性. 这两种技术的结合不仅提升了信息传输的效率, 还显著提高了系统的抗破解能力, 使信息在传输过程中更安全可靠.

综上所述, 在通信网络中, 终端敏感信息很容易成为攻击者的目标, 为维护用户的个人隐私信息安全, 提供更高级别的保护措施, 本文提出了一种考虑并行干扰抵消的通信网络终端敏感信息混沌加密方法. 首先, 利用并行干扰抵消和最小均方误差准则, 对干扰信号进行量化和消除; 其次, 通过演化超网络模型, 将通信数据作为动态节点处理, 建立用于敏感信息识别的决策分类框架, 提高敏感信息识别的准确性; 最后, 基于混沌理论, 采用 Lyapunov 指数测量混沌序列的敏感度, 通过分段线性映射生成密钥流, 确保数据传输的保密性和安全性. 实验结果表明, 本文方法在数据传输速率上有明显提升, 能实时消除通信过程中可能被攻击者利用的干扰信号, 且在 7 s 时即可进入时滞稳定状态, 显著提高了数据传输速率和信息传输性能, 从而为通信网络终端的敏感信息提供了坚实的安全保障.

参 考 文 献

[1] WEI L. Cognitive Wireless Communication Network Information Sharing Method Based on Blockchain Technology [J]. International Journal of Internet Protocol Technology, 2023, 16(2): 99-109.

[2] LI Y Y, SHA J D. Network Covert Channel Data Security Detection Method Based on Threshold Re-encryption [J]. International Journal of Information and Communication Technology, 2023, 23(2): 188-200.

[3] LIU J L, QIN J, WANG W C, et al. Key-Aggregate Based Access Control Encryption for Flexible Cloud Data Sharing [J]. Computer Standards and Interfaces, 2024, 88: 103800-1-103800-15.

[4] KENYA T, MAMORU O, EIJI O. Demonstration of Chaos-Based Radio Encryption Modulation Scheme through Wired Transmission Experiments [J]. IEICE Transactions on Communications, 2023, 106(2): a1-a10.

[5] 胡栋鹏, 汤紫雄, 曾坚毅. 基于区块链技术的光通信网络数据加密方法设计 [J]. 激光杂志, 2023, 44(10): 128-132. (HU D P, TANG Z X, ZENG J Y. Design of Data Encryption Method for Optical Communication Network Based on Blockchain Technology [J]. Laser Journal, 2023, 44(10): 128-132.)

[6] 周娟, 张驰, 殷晓虎, 等. 基于时间戳的异质信息网络数据动态加密传输 [J]. 电子器件, 2024, 47(3): 649-655. (ZHOU J, ZHANG C, YIN X H, et al. Dynamic Encrypted Transmission of Heterogeneous Information Network Data Based on Timestamp [J]. Chinese Journal of Electron Devices, 2024, 47(3): 649-655.)

[7] LIU S. Image Encryption Method with Chaotic Transformation Fusion Bit Operation [J]. Journal of Nonlinear and Convex Analysis, 2024, 25(6): 1481-1490.

[8] LIU J L, ZHANG Y, GONG B. A Data Compression and Encryption Method for Green Edge Computing [J]. Cluster Computing, 2023, 26(5): 3341-3359.

[9] 乌琦, 司中威, 戴金晟, 等. 基于多用户串行干扰抵消的贝叶斯盲检测算法 [J]. 北京邮电大学学报, 2024, 47(1): 1-6. (WU Q, SI Z W, DAI J S, et al. Bayesian Blind Detection Algorithm Based on Multi-user Serial Interference Cancellation [J]. Journal of Beijing University of Posts and Telecommunications, 2024, 47(1): 1-6.)

[10] 孙琳, 李海森, 李羿萱. 双向干扰抑制的多用户滤波多音水声通信研究 [J]. 华中科技大学学报(自然科学版), 2023, 51(9): 40-47. (SUN L, LI H S, LI Y X. Bidirectional Interference Suppression for Multiuser Filtered Multitone Acoustic Communications [J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2023, 51(9): 40-47.)

[11] 徐晓瑶, 黄晓国, 张琦, 等. 基于数字化设计仿真的射频干扰抵消 SiP 设计 [J]. 现代电子技术, 2023, 46(14): 141-146. (XU X Y, HUANG X G, ZHANG Q, et al. Design of RF Interference Cancellation SiP Based on Digital Design and Simulation [J]. Modern Electronics Technique, 2023, 46(14): 141-146.)

[12] 张国梅, 张欣, 尹佳文, 等. 基于深度残差神经网络的 GNSS 接收机干扰抑制方案 [J]. 数据采集与处理, 2023, 38(2): 293-303. (ZHANG G M, ZHANG X, YIN J W, et al. An Interference Suppression Scheme Based on

Deep Residual Neural Networks for GNSS Receivers [J]. Journal of Data Acquisition and Processing, 2023, 38(2): 293-303.)

[13] 臧国全, 张盼盼, 柴文科, 等. 个人通信数据的敏感性识别与隐私计量研究 [J]. 图书情报知识, 2024, 41(2): 110-120. (ZANG G Q, ZHANG P P, CHAI W K, et al. Sensitivity Identification and Privacy Measurement of Personal Communication Data [J]. Documentation, Information & Knowledge, 2024, 41(2): 110-120.)

[14] 金秋, 林馥, 裴斐. 基于层次聚类的敏感信息安全过滤模型研究 [J]. 计算机仿真, 2023, 40(10): 296-299. (JIN Q, LIN F, PEI F. Research on Security Filtering Model of Sensitive Information Based on Hierarchical Clustering [J]. Computer Simulation, 2023, 40(10): 296-299.)

[15] MURALITHARAN J, ARUMUGAM C. Privacy BERT-LSTM: A Novel NLP Algorithm for Sensitive Information Detection in Textual Documents [J]. Neural Computing & Applications, 2024, 36(25): 15439-15454.

[16] ANGSHUMAN J. Sensitive Information Leakage Analysis of Database Code by Abstract Interpretation [J]. International Journal of Security and Networks, 2023, 18(2): 91-105.

[17] 孟庆微, 王西康, 齐子森, 等. 基于余幂-激活离散超混沌加密的多参数加权分数傅里叶变换安全通信方法 [J]. 电子与信息学报, 2023, 45(5): 1688-1696. (MENG Q W, WANG X K, QI Z S, et al. Multiple Parameters Weighted-Type FRactional Fourier Transform Secure Communication Method Based on Cosine Power-Activation Discrete Hyperchaotic Encryption [J]. Journal of Electronics & Information Technology, 2023, 45(5): 1688-1696.)

[18] HUANG Z, ZHANG F F, KOU L, et al. A Real-Time Image Encryption Algorithm for a Distributed Energy System Based on the 13-D Complex Chaotic Sequence [J]. IEEE Multimedia, 2023, 30(4): 71-81.

[19] 王伟杰, 姜美美, 王淑梅, 等. 基于量子长短期记忆网络的量子图像混沌加密方案 [J]. 物理学报, 2023, 72(12): 21-32. (WANG W J, JIANG M M, WANG S M, et al. Quantum Image Chaos Encryption Scheme Based on Quantum Long-Short Term Memory Network [J]. Acta Physica Sinica, 2023, 72(12): 21-32.)

[20] ROGHAYEH D, HOSSEIN K. Chaotic Based Color Image Encryption Using a Hybrid Method of Reversible Cellular Automata and DNA Sequences [J]. Multimedia Tools and Applications, 2024, 83(6): 17429-17450.

[21] 王东伟, 黄德启, 张阳婷, 等. 基于多智能体通信的城市交通信号控制研究 [J]. 东北师大学报(自然科学版), 2025, 57(4): 57-63. (WANG D W, HUANG D Q, ZHANG Y T, et al. Research on Urban Traffic Signal Control Based on Multi-agent Communication [J]. Journal of Northeast Normal University (Natural Science Edition), 2025, 57(4): 57-63.)

[22] 范晶晶, 刘壮, 陈超, 等. 基于动态密钥的车载以太网安全通信方法 [J]. 江苏大学学报(自然科学版), 2024, 45(3): 302-308. (FAN J J, LIU Z, CHEN C, et al. Secure Communication Method for Automotive Ethernet Based on Dynamic Key [J]. Journal of Jiangsu University (Natural Science Edition), 2024, 45(3): 302-308.)

(责任编辑: 韩 啸)