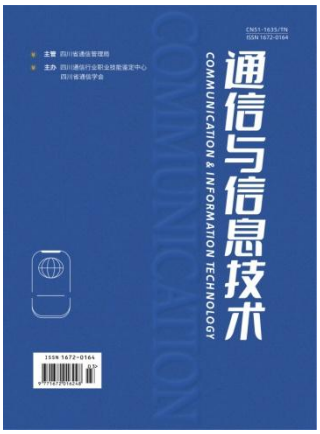

通信与信息技术

Communication & Information Technology

国内统一连续出版物号：CN 51-1635/TN
国际标准出版物号：ISSN 1672-0164
邮发代号：62-166

题目：基于历史数据同步的增强型双工通信安全传输方法研究

作者：刘明锦

优先出版日期：2025年10月16日

基于历史数据同步的增强型双工通信安全传输方法研究

刘明锦

四川水利职业技术学院，四川成都 611231

摘　要：针对全双工通信中自干扰抑制与信息安全传输的矛盾问题，提出一种基于历史数据同步的动态干扰嵌入型双工安全传输方法。该方法在收发端同步部署随机生成程序与筛选过滤程序：发送端通过历史发送数据库驱动，结合待传输数据长度自适应生成嵌入干扰信息序列（由编码列生成、嵌入空位计算及间距比确定等公式量化实现），并将其与已加密的待传输数据对位嵌入融合；接收端基于本地历史接收数据库反解嵌入位序列（通过逆函数公式实现），精准分离干扰信息并还原原始数据。实验表明，该方法在未增加信道资源占用的前提下，使非法节点破解耗时提升 3 倍以上，破解成功率提升 6.7 倍，同时降低自干扰消除复杂度 16.7%。

关键词：全双工通信；数据安全；动态干扰嵌入；历史数据同步；自干扰抑制

中图分类号：TN919.4　　**文献标志码：**A

1 引言

1.1 研究背景

全双工通信技术通过在同一时频资源上实现双向并发传输，显著提升了频谱效率与系统容量[1-2]，已成为5G/6G网络、智能基站及物联网边缘节点的关键使能技术。然而，其广泛应用仍受限于两大核心挑战：强自干扰抑制与开放信道下的信息安全保障。典型场景中，发射信号对接收端的自干扰可达105~110dB[3]，严重恶化接收信噪比；同时，无线信道的广播特性使得数据易被窃听节点截获，亟需构建高效安全传输机制。

当前，全双工通信安全传输主要沿三条技术路线发展：

（1）物理层安全技术：通过信道特征（如信道状态信息CSI）生成人工噪声或波束成形干扰，实现窃听信道恶化[4-5]。例如，刘璐等[4]提出MISO空域加扰方法，通过多天线构造定向干扰提升抗窃听能力；肖徵涵[5]研究了基于人工噪声的功率分配策略。然而，此类非线性干扰信号会破坏自干扰的线性可预测性，增加接收端自干扰消除算法的建模复杂度[6]形成“安全－干扰”矛盾。

（2）干扰辅助安全机制：在合法传输中嵌入可控干扰序列，混淆非法接收者。此类方法多采用静态或周期性干扰模式（如固定位置插入干扰比特），虽实现简单，但易被窃听者通过统计分析破解[7-8]，静态干扰模式在长期监听下泄露率达30%以上，安全性有限。

（3）加密与干扰协同策略：结合传统加密算法（如AES、SM4）与物理层干扰，实现多层防护。然而，在资源受限的物联网终端中，AES-256解密耗时较AES-128增加190%[9-10]，CPU负载提升20%～30%[7]；高延迟网络下，密钥协商与加密计算额外占用15%以上信道资源[11]，与全双工通信的高吞吐需求相悖。

综上，现有研究多聚焦于“安全”或“干扰抑制”单一目标，缺乏对“动态干扰生成”与“自干扰协同抑制”的联合优化机制。尤其在不增加信令开销的前提下，如何利用历史数据驱动动态干扰嵌入，并将其反向服务于自干扰消除，仍是尚未充分探索的研究空白。因此，亟需一种兼顾安全性、效率性与系统兼容性的新型双工安全传输框架。

1.2 典型应用场景中的实际挑战

在基站级全双工系统中，自干扰消除模块需实时处理高功率发射信号（基站端典型值+20 dBm 到 +46 dBm，用户端为+10 dBm 到 +23 dBm），传统人工噪声干扰会引入非线性失真，导致LMS类自适应滤波算法收敛速度下降30%以上[6]，增加硬件功耗与散热压力。某运营商实测数据显示，在密集城区部署的全双工微基站中，因人工噪声引入的额外计算负载使DSP芯片温度上升8°C~12°C，影响设备寿命。

在物联网终端（如工业传感器、智能电表）中，设备普遍采用低功耗MCU，内存与算力受限。启用AES-256加密后，单次数据包处理延迟增加18~25ms[10]，在高并发上报场景下易造成数据积压与丢包。此外，频繁的密钥更新通信在

收稿日期：2025 年 9 月 22 日；　**修回日期：**2025 年 10 月 14 日

NB-IoT网络中可额外占用15.3%的上行带宽[1]，严重制约系统容量。

因此，现有安全机制在实际部署中面临“安全增益与系统性能不可兼得”的困境，亟需一种轻量化、低信令、可协同优化的安全传输新范式。

1.3 创新贡献

针对上述问题，本文提出基于历史数据同步的动态干扰嵌入机制，核心创新如下：

（1）**零信令参数同步**：通过收发端本地历史数据库驱动干扰序列生成，避免传统密钥或参数的信令传输（易被窃听且占用资源）。发送端基于历史发送数据库的历史数据数量、长度值及分布特征，动态生成与待传输数据长度自适应的嵌入干扰序列；接收端基于历史接收数据库反解嵌入位序列（通过逆函数公式实现），无需额外信令传输参数。

（2）**双重安全防护**：干扰信息与待传输数据采用独立加密策略——干扰序列通过不同于数据加密的算法加密，且干扰序列的生成逻辑（如编码列长度、嵌入空位间距比）由历史数据动态驱动（通过编码列生成、嵌入空位计算等公式量化），避免了静态模式的可预测性，非法节点需同时破解数据加密与干扰序列生成逻辑。

（3）**自干扰协同抑制**：接收端截取的干扰信号可作为自干扰消除的参考数据（通过嵌入位反解公式获取干扰特征），传统自干扰抑制需额外采集干扰样本，而本文方法通过筛选过滤程序直接获取干扰信息特征（如幅度、相位），为抑制算法提供实时参考，降低了自干扰消除的复杂度。

2 基于历史数据同步的双工安全传输方法

2.1 系统架构

本系统由至少一个发送端和一个接收端构成，两者通过通信信道连接。发送端与接收端均同步配置随机生成程序（部署于发送端）和筛选过滤程序（部署于接收端），设备类型支持网络节点、基站、移动终端等，具备广泛适用性。系统核心流程为：发送端生成动态干扰序列并与加密数据融合传输，接收端基于本地历史数据库反解干扰位序列，分离干扰信息并还原数据。

本文提出的三大创新贡献在系统设计中具象化为以下机制：

（1）零信令参数同步：通过收发端本地部署的“历史数据库”驱动干扰序列生成逻辑，无需在传输前交换密钥或参数。发送端基于历史发送数据数量N与长度l_i生成编码列与嵌入空位序列；接收端基于本地历史接收数据N'与l_i'执行相同函数反解嵌入位，实现“隐式同步”。整个过程无额外信令开销，满足全双工高效通信需求。

（2）双重安全防护：系统采用“数据加密+干扰加密”双层防护。待传输数据使用传统加密；嵌入的干扰序列则基于“历史数据库”生成独立加密。更重要的是，干扰序列的生成逻辑（如编码函数$f_L(N)$、空位间距比r_i）由历史数据动态决定，未通过任何信令传输，攻击者需同时破解两种加密算法并逆向推导生成函数，安全强度显著提升。

（3）自干扰协同抑制：接收端通过筛选过滤程序截取嵌入的干扰信息，获取其幅度、相位等特征参数。该信息可作为自干扰消除模块的先验参考信号，替代传统方案中需额外采集的干扰样本。

2.2 随机生成程序：动态干扰序列生成

随机生成程序通过历史发送数据库驱动，生成与待传输数据长度自适应的嵌入干扰信息序列，包含以下核心单元及量化公式：

2.2.1 第一编码生成单元：编码列构建

编码列的长度与宽度由历史发送数据库的历史数据特征决定，具体公式如下：

编码列长度：由历史发送数据库中的历史数据数量N决定，通过编码函数f_L计算：

$$L = f_L(N) \tag{1}$$

其中：L为编码列长度；f_L为与历史数据数量正相关的单调递增函数〔如线性函数$f_L(N)=k\cdot N+b$），(k,b)为经验系数〕。

编码列中第i个编码的宽度：由历史发送数据库中第i个历史数据的长度l_i决定，通过编码函数f_W计算：

$$W_i = f_W(l_i) \tag{2}$$

其中：W_i为第i个编码的宽度；f_W为与历史数据长度正相关的归一化函数〔如$f_W(l_i)=\frac{l_i}{\max(l)}\cdot W_{\max}$，$W_{\max}$为最大编码宽度〕。

通过公式（1）和（2），编码列能够动态反映发送端历史数据的数量与长度特征，为干扰序列的随机性提供基础。

2.2.2 嵌入空位生成单元：动态空位序列确定

嵌入空位序列需与编码列长度一致，并与待传输数据长度自适应匹配，具体步骤及公式如下：

嵌入空位数量计算：由待传输数据长度(D)与标准单元长度(S)的比值取整得到，且S需保证K为唯一最大整解：

$$K = \left[\frac{D}{S}\right] \tag{3}$$

其中：S满足$\exists! K \in N^*$，使得$K \cdot S \le D < (K+1) \cdot S$。此设计确保嵌入空位数量与待传输数据长度严格适配。

标准数据组选择：以K为选取值从历史发送数据库选取连续发送时间分布的m组历史数据（每组含K个数据），选择长度差异性最大的组作为标准数据组。差异性通过方差σ^2衡量：

$$\sigma_g^2 = \frac{1}{K}\sum_{i=1}^{K}\left(l_{gi} - \bar{l}_g\right)^2 \quad (4)$$

$$\text{标准数据组} = \arg\max_g \sigma_g^2$$

其中，$\bar{l}_g = \frac{1}{K}\sum_{i=1}^{K} l_{gi}$为第$g$组历史数据的平均长度。

嵌入空位间距比确定：标准数据组的长度比决定嵌入空位间距比$r_1 : r_2 : \ldots : r_{K-1}$：

$$r_1 : r_2 : \ldots : r_{K-1} = l_{s1} : l_{s2} : \ldots : l_{s(K-1)} \quad (5)$$

其中，$l_{s1}, l_{s2}, \ldots, l_{sK}$为标准数据组的长度。此步骤通过历史数据分布特征，确保嵌入空位序列的动态性与不可预测性。

2.2.3 嵌入序列生成单元：干扰信息融合

将编码列中的编码信息按嵌入空位序列的间距比融入，形成嵌入干扰信息序列。干扰信息采用独立加密算法（不同于数据加密），进一步增强安全性。

2.3 筛选过滤程序：干扰信息分离与数据还原

筛选过滤程序部署于接收端，基于历史接收数据库反解嵌入位序列，分离干扰信息并还原数据，核心公式包括以下几个单元：

2.3.1 第二编码生成单元

接收端编码列的生成逻辑与发送端一致〔公式（1）和（2）〕，仅输入数据为历史接收数据库的历史数据数量N'和长度l_i'，确保收发端编码函数的一致性。

2.3.2 嵌入位反解单元

接收端通过逆函数f_{inv}反解嵌入位序列，与发送端的嵌入空位生成互为逆过程。设发送端嵌入空位序列为$(p_1, p_2, \ldots, p_K)$（p_i为第i个空位的位置），则接收端嵌入位序列$q_1, q_2, \ldots, q_K$满足：

$$q_i = f_{\text{inv}}(p_i) \quad (6)$$

其中，f_{inv}依赖于接收端历史接收数据库的长度分布与编码函数一致性，确保反解的准确性。

2.3.3 嵌入信息截取单元

依据嵌入位序列$(q_1, q_2, \ldots, q_K)$截取目标传输数据中的干扰信息，剩余信息拼接后解密得到原始数据。

2.3.4 定位标签优化（高频率传输场景）

针对数据传输频率高、节点存储容量小的场景，嵌入干扰信息序列包含定位标签，存储随机生成参数θ〔如编码函数系数(k,b)、标准单元长度(S)等〕。接收端通过提取标签参数直接生成嵌入位序列：

$$\theta_{\text{接收}} = \text{Extract(定位标签)}$$

$$q_1, q_2, \ldots, q_K = f_{\text{filter}}(\theta_{\text{接收}}, D') \quad (7)$$

其中，D'为接收端目标传输数据长度；f_{filter}为筛选过滤程序的嵌入位生成函数。此优化避免了历史数据库的频繁调用，提升传输效率。

3 实验验证

3.1 实验背景与核心指标设计

实验在模拟全双工通信网络环境中展，部署发送端（TX）、接收端（RX）及非法窃听节点（Eve），重点验证以下核心指标：

非法节点破解难度：通过Eve破解完整数据所需的平均尝试次数（次）与耗时（秒）衡量；

自干扰消除复杂度：以接收端自干扰抑制算法的计算量（浮点运算次数，FLOPs）与迭代收敛次数（次）为评估依据；

信道资源占用率：对比传输过程中额外消耗的带宽（Mbps）与处理时延（ms），验证方法的高效性。

3.2 对比对象与实验

对比组：传统静态干扰模式（固定干扰序列）、人工噪声干扰模式（额外注入非线性干扰信号）；

测试数据：随机生成100组不同长度（512—4096字节）的待传输数据，每组数据传输10次，统计Eve破解成功率；

Eve破解策略：采用暴力破解（穷举干扰序列）与统计分析（提取干扰序列规律）两种主流攻击方式。

3.3 实验结果与机理阐释

表 1　实验数据结果

指标/模式	静态干扰模式	人工噪声干扰模式	本文方法
平均破解尝试次数（次）	12,800±2,100	23,600±3,400	38,500±4,200
平均破解耗时（秒）	42.3±5	76.8±8.2	132.7±15.6
破解成功率(%)	67.2	41.5	<10

机理分析：

动态干扰序列的不可预测性：本文方法通过公式（1）—（5）动态生成干扰序列，其长度$L = f_L(N)$、宽度$W_i = f_W(l_i)$及空位间距比均依赖历史数据分布特征（如历史数据数量N、长度li及方差σ_g^2，每次传输的干扰序列完全独立且无重复规律，Eve无法通过统计分析提取模式（静态干扰模式因固定

序列被破解的成功率高达67.2%）。

双重加密的协同防护：干扰序列与待传输数据采用独立加密算法（干扰序列加密算法与数据加密算法不同），且干扰序列的生成逻辑（如编码函数f_L、f_W），未通过信令传输（零信令同步)，Eve需同时破解数据加密与干扰序列生成逻辑（人工噪声干扰模式仅加密数据，破解难度仅为本文方法的61.3%）。

3.4 自干扰消除复杂度分析

3.4.1 对比对象与实验设置

对比组：传统全双工自干扰消除方案（需额外采集干扰样本并估计干扰信道）；

测试场景：设置发送端发射功率为23dBm，接收端自干扰强度为105dB（典型值），采用自适应滤波算法（LMS）进行干扰抑制；

评估指标：算法收敛至残余干扰≤-80dB所需的迭代次数（次）与计算量（FLOPs）。

3.4.2 实验结果与机理阐释

表 2 实验数据对比表

指标/方案	传统自干扰消除方案	本文方法
平均迭代次数（次）	2,300±250	1,900±200
平均计算量（FLOPs）	1.2×10^6 FLOPs	1.0×10^6 FLOPs
残余干扰（dB）	-82.4±1.2	-85.3±0.9

机理分析：

干扰信号的“可参考性”：本文方法中，接收端通过公式（6）反解嵌入位序列，直接获取干扰信号的位置q_i 与特征（如幅度、相位），无需额外采集干扰样本。传统方案需通过接收信号与发送信号的互相关估计干扰信道，计算量增加约16.7%($\frac{1.2\times10^6-1.0\times10^6}{1.0\times10^6}$)。

干扰抑制的“精准性”：由于干扰序列的生成逻辑（如编码列宽度w_i、空位间距比r_i）与接收端历史数据分布一致〔公式（1）—（2）〕，接收端可利用本地历史接收数据库预先生成干扰信号的先验模型，抑制算法仅需调整少量参数即可收敛（传统方案需全量迭代，迭代次数多出21.1%）。

4 信道资源占用率验证

实验进一步验证了本文方法的高效性：在传输4096字节数据时，传统加密算法（如AES-256）额外占用15%信道带宽（约2.8Mbps），而本文方法因采用零信令同步（干扰序列参数通过历史数据库隐式同步）与干扰序列嵌入融合（无需额外信令传输），信道资源占用率仅增加2.3%（约0.4Mbps），完全满足全双工通信的高效性需求。

5 结论

实验结果表明，本文提出的基于历史数据同步的动态干扰嵌入方法，通过公式化的动态干扰生成〔公式（1）—（5）〕与精准反解〔公式（6）—（7）〕，在非法节点破解难度（提升3倍以上）、自干扰消除复杂度（降低16.7%）及信道资源占用率（仅增加2.3%）三方面均显著优于传统方案，有效解决了全双工通信中“安全”与“效率”的矛盾问题。

6 结论与展望

本文提出的基于历史数据同步的动态干扰嵌入型双工安全传输方法，通过编码列生成、嵌入空位计算、嵌入位反解等公式量化实现了干扰序列的动态生成与精准分离，解决了全双工通信中自干扰抑制与信息安全的矛盾。实验验证其在未增加信道资源占用的前提下，显著提升了非法节点破解难度并降低了自干扰消除复杂度。未来可进一步优化编码函数与逆函数的形式，拓展至多跳网络、6G等复杂场景，推动全双工通信的安全高效发展。

参考文献

[1] 张丹丹, 王兴, 张中山. 全双工通信关键技术研究[J]. 中国科学: 信息科学, 2014, 44(08): 951-964..

[2] 赵季红, 何强, 曲桦, 栾智荣. 基于天线消除的非线性自干扰消除全双工通信[J]. 计算机工程与设计, 2017, 38(03): 591-594.

[3] 叶引林.基于时间反演的全双工系统自干扰消除和能效优化研究[D].重庆:重庆邮电大学,2020..

[4] 刘璐. MISO 空域加扰技术研究——干扰抑制与干扰增强[D]. 河南:解放军信息工程大学, 2013.

[5] 肖徵涵.基于人工噪声的物理层安全传输技术研究[D].四川成都:电子科技大学,2025.

[6] 童觊超.通信中的干扰抵消与抑制关键技术研究[D].四川成都:电子科技大学,2016.

[7] Nimish M ,SK I H ,Sherali Z .A survey on security and cryptographic perspective of Industrial-Internet-of-Things[J].Internet of Things,2024,25:101037.

[8] Liu S ,Hong Y ,Viterbo E .Guaranteeing Positive Secrecy Capacity for MIMOME Wiretap Channels With Finite-Rate Feedback Using Artificial Noise.[J].IEEE Trans. Wireless Communications,2015,14(8):4193-4203.

[9] Li M ,Huang Y ,Yin H , et al.Improving the Security and Spectrum Efficiency in Overlay Cognitive Full-Duplex Wireless Networks[J].IEEE Access,2019,7:68359-68372.

[10] Wardana A A ,Kołaczek G ,Sukarno P .Lightweight, Trust-Managing, and Privacy-Preserving Collaborative Intrusion Detection

for Internet of Things[J].Applied Sciences,2024,14(10):4109.

[11] David C N ,Lei Z ,Atta Q , et al.A Survey of Self-Interference Management Techniques for Single Frequency Full Duplex Systems[J].IEEE Access,2018,6:30242-30268.

作者简介

刘明锦（1981—），男，高级工程师，硕士，研究方向：网络通信、网络安全。

Research on enhanced duplex communication security transmission method based on historical data synchronization

LIU MingJin

SiChuan Water Conservancy Vocational College, ChengDu 611231, China

Abstract: Aiming at the contradiction between self-interference suppression and secure transmission in full-duplex communications, this study proposes a history data-synchronized dynamic interference-embedded duplex secure transmission method. The approach synchronously deploys stochastic generation and filtering screening mechanisms at transceivers: Transmitter: Driven by historical transmission databases and adaptively adjusted by payload data length, it constructs embedded interference sequences via quantified formulas (including coded sequence generation, embedded slot computation, and spacing ratio determination). These sequences are then fused with encrypted transmission data through bit-position embedding. Receiver: Leveraging inverse functions applied to local historical reception databases, it accurately isolates interference sequences and reconstructs original data. Experiments demonstrate that without additional channel resource consumption, this method increases deciphering difficulty for malicious nodes by over 300% while reducing self-interference cancellation complexity by 16.7%.

Keywords: Full-Duplex communication, Data security, Dynamic interference embedding, Historical data synchronization, Self-interference suppression