

DOI: 10.13382/j.jemi.B2508332

5G-A 正交失配干扰测试平台研究与实现*

王 志 陈向民

(创远信科(上海)技术股份有限公司 上海 201601)

摘 要:为系统评估第五代增强型移动通信(5G-Advanced)系统在复杂电磁环境下的抗干扰性能,本文针对现有干扰测试方法在模拟真实非正交干扰上的不足,设计并实现了一种基于正交失配干扰机制的 5G-A 专用测试平台。该平台创新性地提出通过引入归一化频率偏移以破坏子载波正交性的干扰生成方法,建立攻击信号频偏同干扰能量扩散效率的解析关系。硬件上采用 FPGA 结合高速 ADC/DAC 模块与可配置射频前端,实现了干扰信号的频率,功率,波形以及时序精准产生与高精度控制。为全面验证平台有效性及评估 5G-A 关键信道的抗干扰能力,射频馈线直连与静态/动态空口实测两种场景,并重点分析考察了同步信号块(SSB),物理下行控制信道(PDCCH)与物理上行控制信道(PUCCH)在不同强度正交失配干扰下的性能表现。实验结果表明,相较于传统窄带干扰,正交失配干扰在相同发射功率下可使终端误码率提升 2 倍,同时能够准确地测试上述关键信号及信道的抗干扰性能,对推动 5G-A 的可靠部署具有积极意义。

关键词: 干扰测试平台;正交失配干扰;抗干扰性能;测试验证;5G-A

中图分类号: TN92;TN98 **文献标识码:** A **国家标准学科分类代码:** 510.50

Research and implementation of an orthogonality-sabotaging interference testing platform for 5G-A

Wang Zhi Chen Xiangmin

(Transcom (Shanghai) technologies Co., Ltd., Shanghai 201601, China)

Abstract: For the systematic evaluation of the anti-jamming performance of 5th generation advanced (5G-A) systems in complex electromagnetic environments, this study addresses the shortcomings of existing jamming test methods in simulating realistic non-orthogonal interference. A dedicated 5G-A test platform based on an orthogonal mismatch interference mechanism is designed and implemented. The platform innovatively proposes an interference generation method that destroys subcarrier orthogonality by introducing a normalized frequency offset, establishing an analytical relationship between the attacker's frequency offset and the efficiency of interference energy diffusion. In terms of hardware implementation, the platform employs an FPGA combined with high-speed ADC/DAC modules and a configurable RF front-end, achieving precise generation and high-precision control of interference signals in terms of frequency, power, waveform, and timing. To comprehensively verify the platform's effectiveness and evaluate the anti-jamming capability of key 5G-A channels, two test scenarios—RF cable direct connection and static/dynamic over-the-air measurement—were employed. The performance of the synchronization signal block (SSB), physical downlink control channel (PDCCH), and physical uplink control channel (PUCCH) under orthogonal mismatch interference of varying intensities was analyzed and examined. Experimental results indicate that, compared to traditional narrowband jamming, orthogonal mismatch interference can increase the terminal bit error rate by a factor of two under the same transmit power, while enabling accurate testing of the anti-jamming performance of the aforementioned key signals and channels. This work holds positive significance for promoting the reliable deployment of 5G-A networks.

Keywords: interference testing platform; orthogonality-sabotaging interference; interference resistance evaluation; measurement verification; 5G-A

收稿日期: 2025-04-23 Received Date: 2025-04-23

* 基金项目: 5G-A 通感融合技术测试仪表和综合测试验证系统研发(移动信息网络国家科技重大专项 2025ZD1301700)资助项目

0 引言

第五代增强型无线蜂窝网络 (5th generation advanced, 5G-A) 作为 5G 技术的演进版本, 承诺提供更快数据速率和更可靠的服务交付。它预计将支持许多尖端技术, 如物联网 (internet of thing, IoT)、自动驾驶汽车和智能城市。5G-A 架构建立在 5 个基本支柱之上: 新的无线电频谱、大规模多输入多输出 (multiple-input multiple-output, MIMO)/波束成形 (beamforming)、多连接性、网络灵活性和高水平的安全性^[1-2]。2024 年, 3GPP R18 标准正式冻结, 成为了 5G-A 的第一个版本, 同时这已成为部署这些网络的主要参考^[3]。

与任何无线蜂窝网络一样, 5G-A 网络基于开放共享, 通信介质是自由空间, 这使得它们容易受到干扰, 这是无线网络性能下降的根本原因之一。如果干扰水平很高, 接收机将无法解码传输的信号。这种弱点可以被一些恶意节点利用, 通过在特定无线信道上造成故意干扰来阻碍合法用户的通信, 这被称为干扰攻击。干扰攻击对公共通信服务构成严重风险。早在 20 世纪初, 干扰攻击就被用于军事战斗。如今, 干扰攻击可以用来阻碍公共通信服务。市场上有许多低成本的干扰设备。此外, 最复杂的干扰攻击可以使用低成本的软件定义无线电工具和一些基本的编程技能以低至 1 000 美元的价格实现。此外, 5G-A 预计将作为紧急服务、自然灾害救援、公共安全和军事通信的基础设施, 这使得干扰攻击成为一个真正的威胁。因此, 5G-A 的一个核心要求是高水平的安全性和对干扰攻击的韧性。

在 5G 网络中, 干扰攻击主要由恶意节点 (即干扰器) 发起, 这些干扰器通过多种策略来破坏通信。常规干扰器不遵循任何 MAC 协议, 持续不断地注入射频信号, 这些信号可能是合法的比特序列或随机的比特序列, 目的是干扰合法用户的传输。这种持续的信号注入会占用传输信道, 阻碍合法节点的通信^[4]。由于这种攻击方式需要持续传输, 因此会消耗大量功率, 对干扰器的电池寿命造成影响。随机干扰器通过在活动和空闲状态之间切换来节省能量。在干扰过程中, 恶意节点会在预定的时间内进行干扰, 然后关闭其无线设备。一段时间后, 它会从睡眠模式重新激活干扰过程。这种模式使得随机干扰器能够在保持干扰效果的同时, 有效降低功耗^[5-6]。欺骗性干扰器则通过注入看似合法的比特序列来误导接收机, 使其误以为信号来自合法源。这种干扰器通过模仿合法信号的特征, 迫使接收机保持在监听状态, 从而有效地干扰通信。与常规干扰器相比, 欺骗性干扰器更难被检测, 因为它们的信号与合法信号非常相似^[7-8]。响应式

干扰器 (也称为反应式干扰器) 则通过监控通信信道来实现更高效的干扰。它们仅在检测到发射机活跃时才进行传输, 从而最小化自身的功耗。这种策略使得响应式干扰器能够在不被发现的情况下, 有效地干扰通信^[9-11]。最后, 控制信道干扰器专门针对控制信道进行干扰, 目的是阻塞发射机和接收机之间的通信。这种干扰器可以通过多种方式实现, 包括拒绝服务攻击, 甚至完全阻断节点对网络的访问。这些干扰器对 5G 网络的稳定性和安全性构成了严重的威胁, 因为它们能够有效地破坏通信, 阻碍合法用户的服务^[12-14]。

在部署 5G-A 蜂窝网络之前, 需要研究 3GPP 发布的 5G-A 标准在多大程度上能够抵抗干扰攻击, 并制定可纳入该标准的安全协议。因此, 确定干扰器在何种条件下 (例如发射功率、攻击波形参数、时频资源占用等) 能够破坏通信信道, 成为系统安全评估的关键前提。现有研究已对多种恶意干扰策略进行了分析, 包括常规干扰、随机干扰、欺骗性干扰等, 这些方法虽能有效干扰通信, 但往往需要较高的实现复杂度或较大的功率消耗。相比之下, 基于频率偏移的正交失配干扰可有效破坏 OFDM 子载波的正交性, 并凭借其实现简单、成本低廉和干扰效率高的特点, 成为恶意干扰场景下更为经济且有效的攻击手段。本文提出了一种基于正交失配干扰机制的干扰测试平台, 可用于量化评估 5G-A 系统在复杂电磁环境中的抗干扰韧性。

1) 干扰测试平台架构设计: 5G-A 干扰测试平台基于高性能 FPGA、射频前端 (如 ADC/DAC、混频器等)、ARM 以及必要的接口单元搭建而成。其硬件总体方案包括基带部分和射频部分的设计, 涵盖了接收、处理和发射的全过程。基带部分负责实现灵活干扰算法及基带信号生成。射频部分则通过功率放大器等多个组件, 将基带信号调制到指定频段, 经滤波后输出, 同时实现信号的接收和混频功能。

2) 正交失配干扰机制: 提出一种通过引入归一化频率偏移破坏 OFDM 子载波正交性的新型干扰机制。通过理论建模与推导, 建立攻击信号频偏同干扰能量扩散效率的解析关系, 揭示其相对于传统精准子载波干扰的效能增益。

3) 5G-A 干扰测试平台验证: 针对所构建的 5G-A 干扰测试平台, 采用射频馈线直连与空口实测 (静态/动态) 两种验证方法。前者完成同步信号块 (synchronization signal block, SSB)、物理下行控制信道 (physical downlink control channel, PDCCH) 以及物理上行控制信道 (physical uplink control channel, PUCCH) 误码抗干扰性能的定量评估, 后者评估测试平台在真实空口 (静态/动态) 环境下的干扰效能。

1 5G-A 灵活干扰测试平台

详细介绍了 5G-A 灵活干扰测试平台的总体架构、5G-A 关键信道分析以及正交失配干扰机制等内容。

1.1 总体架构

5G-A 正交失配干扰测试平台总体架构如图 1 所示。平台以 FPGA 为核心,连接多个关键模块,形成一个有机整体。FPGA 作为整个平台的控制中心和数据处理中心,其作用至关重要。它通过与 NOR Flash、DDR、eMMC NAND Flash 的连接,实现数据的存储与读取。NOR Flash 主要用于存储启动代码和关键配置信息,确保平台在启动时能够快速加载必要的数据。DDR 则作为运行内存,为 FPGA 提供高速的数据暂存空间,使得复杂的干扰算法能够流畅运行。eMMC NAND Flash 用于存储大量的干扰数据、信号特征库以及系统日志等信息,为平台的长期稳定运行提供数据支持。

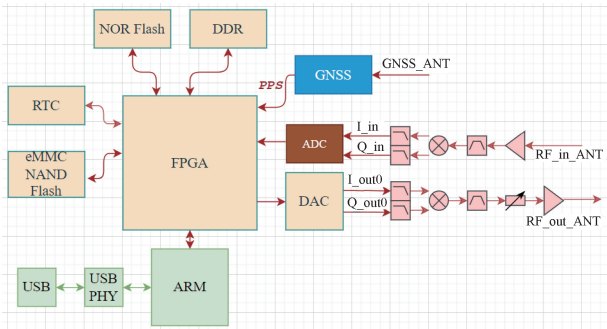


图 1 5G-A 正交失配干扰测试平台总体架构
Fig. 1 The architecture of 5G-A orthogonality-sabotaging interference test platform

在信号输入侧,由天线接收的现网信号通过放大混频最终经过 ADC 将模拟信号转换为数字信号,传输至 FPGA 进行实时解析与特征提取,如频点、小区 ID 等信息,同时可以锁定帧头位置并完成同步操作。

在信号输出侧,FPGA 与 DAC 模块紧密相连,DAC 负责将 FPGA 输出的数字干扰信号转换为模拟信号。转换后的模拟信号经过滤波、放大等处理后,通过射频前端电路传输至天线,最终以射频信号的形式发射出去,实现对目标信号的干扰。这一过程中,射频前端电路对信号的质量和强度进行精确控制,确保干扰信号能够有效覆盖目标区域。

ARM 模块通过 USB PHY 与上位机进行连接,实现数据的传输和系统的升级。ARM 与 FPGA 之间进行双向通信,ARM 负责处理一些外围设备的管理和控制任务,如人机交互界面、外部存储设备等。FPGA 则专注于核心的干扰算法和信号处理任务。两者之间通过高速的

数据总线进行数据交换,确保平台能够快速响应外部指令和内部数据处理需求。

5G-A 正交失配干扰测试平台通过各模块的紧密配合,实现了高效、精准的干扰功能。FPGA 作为核心控制和数据处理单元,与存储模块、DAC 模块、GNSS 模块以及 ARM 模块等协同工作,确保平台能够快速响应各种干扰需求。

1.2 5G-A 关键信道分析

5G-A 系统采用新型物理层架构设计,其关键信道在时频资源映射和信号结构层面展现出独特的抗干扰特性^[15-16]。系统核心信号及信道主要包括 SSB、PDCCH 以及 PUCCH,各信道在抗干扰性能评估中具有关键作用。如表 1 所示,给出了 5G-A 关键信道的对应指标。

表 1 5G-A 关键信道
Table 1 5G-A key channels

信道类型	子载波间隔	时域符号数	频域子载波数	调制方式	编码方案
PSS	15/30 kHz	1	127	BPSK	M 序列
SSS	15/30 kHz	1	127	BPSK	Gold 序列
PBCH	15/30 kHz	3	240	QPSK	Polar
PBCH DMRS	15/30 kHz	3	60	QPSK	无
PDCCH	15/30/60 kHz	1~3	72 的整数倍	QPSK	Polar
PUCCH	15/30/60 kHz	1~2	12~192	QPSK	Variety

SSB 作为 5G 终端初始接入的关键信令单元,由主同步信号(primary synchronization signal, PSS)、辅同步信号(secondary synchronization signal, SSS)、物理广播信道(physical broadcast channel, PBCH)及其解调参考信号(demodulation reference signal, DMRS)复合构成,如图 2 所示,承担着时频同步、小区识别及系统参数广播的核心功能。

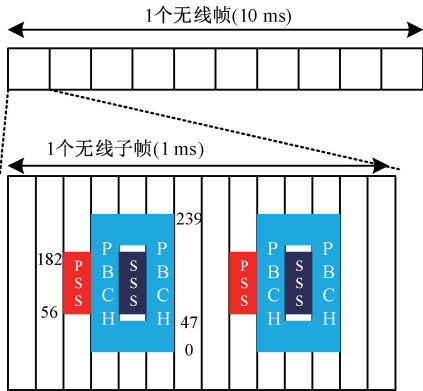


图 2 SSB 时频图
Fig. 2 Time-frequency diagram of SSB

其中,PSS 采用长度为 127 的 m 序列实现时频同步,

通过循环移位生成 3 种物理层小区 ID;SSS 基于 Gold 序列设计,产生 336 种低互相关序列组合,共同形成 1008 种物理层小区 ID 的识别机制^[17]。当 SSB 遭受强干扰时,会导致终端无法完成同步或误判 PCI,进而引发小区搜索失败、系统消息解析错误,严重时可能导致网络脱网或切换失败^[18]。

PDCCH 是 5G 系统中承载下行控制信息(DCI)的核心物理信道,负责调度 PDSCH/PUSCH 资源分配、功率控制及链路自适应。该信道采用基于控制资源集(CORESET)的灵活映射机制^[19],通过参数 CORESET-freq-dom 和 CORESET-time-dur 实现频域位置与时间持续周期的动态配置。采用 Polar 码结合 24 位 CRC 校验^[18],通过交织算法将控制信息分散至整个带宽,可提升窄带抗干扰能力。PDCCH 受到持续干扰时,DCI 指令误检率将激增,导致上行授权失效、HARQ 重传次数超限,最终引发用户面数据传输中断或无线链路失败(RLF)^[20-21]。

PUCCH 是 5G 系统中承载上行控制信息(upper control information, UCI)的核心物理信道,负责传输混合自动重传确认(hybrid automatic repeat request-acknowledgement, HARQ-ACK)、信道状态反馈(channel state information, CSI)及调度请求(scheduling request, SR)等关键控制信号。该信道采用基于资源集的动态配置机制,可实现频域资源块(physical resource block, PRB)数量与时域符号长度的灵活适配。当 PUCCH 持续遭受深度干扰时,上行控制信息误码率将导致 HARQ 反馈失效、CSI 测量失真及 SR 请求丢失等连锁效应,进而引发下行调度失准、上行资源分配冲突,最终造成用户面数据传输时延激增或无线链路同步失败。

1.3 正交失配干扰机制

5G-A 仍然是一个基于 OFDM 的无线网络,这里假设共有 N 个子载波,其中有 M 个特定子载波为本文关注的特定物理层信道子载波,其余 $N - M$ 个子载波为其他子载波(用于传输)。定义 Z 为所有特定子载波的集合,其索引集为 $Z = \{m_0, m_1, \dots, m_{L-1}\}$ 。

令 $[X_0, X_1, \dots, X_{L-1}]$ 表示特定物理层信道待传输的 L 个调制符号。在发送前,这些符号将被映射到其分配的子载波上,形成 N 个符号 $\{S_i\}_{0 \leq i \leq N-1}$ 。通过 N 点快速傅里叶逆变换(inverse fast Fourier transform, IFFT),OFDM 符号块从频域转换至时域。IFFT 输出的第 $n(0 \leq n \leq N - 1)$ 个时域采样可表示为:

$$x_n = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} S_i e^{j2\pi ni/N} \quad (1)$$

该信号经上变频后形成射频信号,经过无线信道最终传输至接收端。接收端将聚合的射频信号下变频至基带后,第 n 个时域接收信号可表示为:

$$y_n = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} S_i H_i e^{j2\pi ni/N} + \omega_n \quad (2)$$

式中: H_i 表示接收端在子载波 i 上的频域信道响应; ω_n 为零均值、方差为 δ^2 的加性高斯白噪声(additive white gaussian noise, AWGN)。令 W_i 为 ω_n 的快速傅里叶变换(fast Fourier transform, FFT)结果,接收端通过 FFT 将信号转换回频域,得到子载波 i 上的频域符号:

$$Y_i = S_i H_i + W_i \quad (3)$$

为了破坏无线传输,传统的干扰攻击通常会覆盖通信信号的全部带宽,从而使接收机的接收信号干扰加噪声比(signal-to-interference-pulse-noise ratio, SINR)低于解码阈值。窄带干扰通常被认为对宽带信号无效,因为干扰功率在窄带频谱上平均到全带宽频谱上可能不足以在纠错机制下破坏宽带信号。本文的目标是设计一种灵巧攻击机制,利用窄带干扰信号破坏基于 OFDM 的 5G-A 信号。

OFDM 解码依赖于任何两个子载波之间的间隔恰好是子载波带宽的整数倍,以在接收机的 FFT 过程中保持正交性。如果攻击者故意传输一个与所有其他子载波频率不一致的干扰信号,将破坏正交性,并在全带宽频谱上对所有子载波造成干扰。

为了详细说明,将评估并比较精确子载波干扰攻击和正交性破坏攻击的基本策略,同时探究正交性破坏攻击的最优攻击策略推导和仿真。

1) 精确子载波干扰

假设攻击者针对子载波 m 发射干扰信号 $\hat{S}_m$, 其时域表达式为:

$$\hat{x}_n = \frac{1}{\sqrt{N}} \hat{S}_m e^{j2\pi nm/N} \quad (4)$$

接收机在子载波 i 上的频域信号为:

$$Y_i = \begin{cases} S_i H_i + W_i, & i \neq m \\ S_i H_i + W_i + \hat{S}_m \hat{H}_i, & i = m \end{cases} \quad (5)$$

其中, $\hat{H}_i$ 是干扰信号从攻击者到接收机的信道响应。可以看出,干扰部分仅在 $i = m$ 时存在,这意味着攻击者只能干扰子载波 m , 而对其他子载波没有影响。

2) 正交失配干扰

本文基于精确子载波干扰攻击定义了一种基本的正交性破坏攻击,通过引入归一化频率偏移 $\varepsilon_m \in [-0.5, 0.5]$, 攻击信号时域表达式修正为:

$$\hat{x}_n = \frac{1}{\sqrt{N}} \hat{S}_m e^{j \frac{2\pi(e_m + m)n}{N}} \quad (6)$$

接收端 FFT 处理后,干扰扩散至所有子载波,子载波 i 上的对应频域信号可以表示为:

$$Y_i = S_i H_i + W_i + \hat{S}_m \hat{H}_m I(i, m, \varepsilon_m) \quad (7)$$

其中干扰分量频域为：

$$I(i,m,\varepsilon_m)=\frac{1}{N}\sum_{n=0}^{N-1}e^{j2\pi((i-m)+\varepsilon_m)n/N}$$

(8)

干扰分量 $I(i,m,\varepsilon_m)$ 在所有子载波上均产生非零值,导致全频段正交性破坏。即使攻击带宽仅覆盖少数子载波,其引发的频率失配通过 FFT 运算扩散至全部子载波,形成广谱干扰。传统载波间干扰 (inter-carrier interference, ICI) 可通过频率同步消除,而本攻击通过恶意设计的不可校正频率偏移 $\varepsilon_m \in [-0.5, 0.5]$ 使干扰持续存在并最大化破坏效果。如图 3 所示,给出了上述两种干扰方式的示意图。

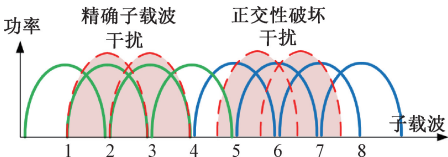


图 3 两种干扰方式示意图

Fig. 3 Schematic diagram of two interference mechanisms

3) 最优攻击配置推导

当子载波数 $N \rightarrow \infty$ 时,干扰扩散函数的极限形式如式(9)所示。

$$\lim_{N \rightarrow \infty} |I(i,m,\varepsilon_m)|^2 = \text{sinc}^2(\pi(i-m+\varepsilon_m))$$

(9)

其中, $\text{sinc}(x) = \sin(x)/x$ 。

对于未被攻击子载波 $i \neq m$, sinc^2 函数的旁瓣在 $\varepsilon_m = \pm 0.5$ 时,主瓣宽度最大化,使得干扰能量扩散到最多子载波,同时旁瓣幅度保持较高水平,产生长尾效应,使得干扰效果在全频段内显著提升。

对于被攻击子载波 $i = m$, $\varepsilon_m = \pm 0.5$ 时,干扰能量为 $\text{sinc}^2(\pi \times 0.5) = (2/\pi)^2 \approx 0.405$,相较于 $\varepsilon_m = 0$,也即精确子载波干扰的干扰能量仅降低至 40%。综上,攻击效果在 $\varepsilon_m = \pm 0.5$ 时达到全局最优。

为进一步明确正交性破坏干扰机制在不同频率偏移 ε_m 和干扰信号子载波长度 $\hat{L}$ 下的性能表现,本文搭建了仿真平台,并使用误比特率 (bit error rate, BER) 指标反应最终的干扰效果,具体参数配置如表 2 所示。

表 2 仿真平台配置参数

Table 2 Parameters for direct connection verification

参数	值
子载波总数	240
子载波间隔	30 kHz
调制方式	QPSK
数据包长度	100 byte
干扰信号归一化频率偏移	$[-0.5, 0.5]$
干扰信号子载波长度	20/35/55

正交性破坏干扰信号的时频资源位置如图 4 所示,时域上连续发送,频域上占据 20 个子载波,中心频点位于整个频谱的中心位置,频域其他位置空置,也即干扰信号并未在其他时频资源上对数据信号进行直接干扰。

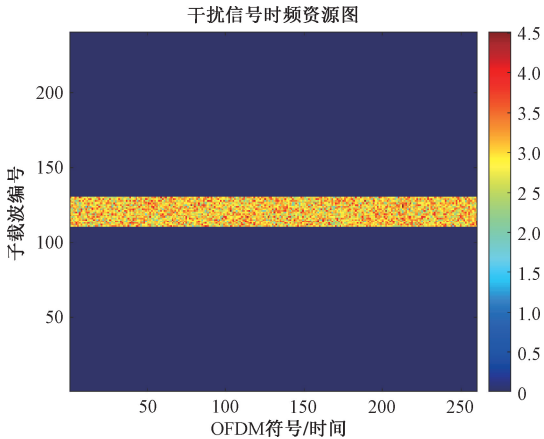


图 4 正交性破坏干扰信号时频图

Fig. 4 Time-frequency diagram of orthogonality-disrupting interference signals

仿真遍历了频率偏移在 $[-0.5, 0.5]$ 范围内不同频移对网络性能的影响。如图 5 所示,显示了归一化频移与用户平均误码率 (BER) 的关系。结果表明,当归一化频移为 ± 0.5 时,BER 达到最大值,验证了前文关于最优攻击策的描述,散射子载波攻击的影响显著高于连续子载波攻击,频移为 0 时 (即传统精确子载波干扰),攻击效果最弱,正交性破坏干扰方式的破坏力远超传统精确子载波干扰。

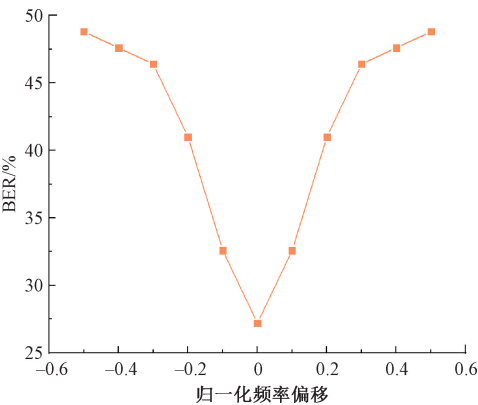


图 5 不同频偏下的 BER 性能表现

Fig. 5 BER performance under different frequency offsets

在固定归一化频偏为 0.5 的条件下,评估不同干扰带宽 $\hat{L}$ 对 240 个数据子载波的影响。如图 6 所示,当 $\hat{L} = 20$ 个子载波时,可影响至少 80 个相邻子载波;当 $\hat{L} = 55$ 个子载波时,影响范围扩展至 220 个子载波,正交性破坏

攻击的有效干扰带宽可达自身带宽的 400%。

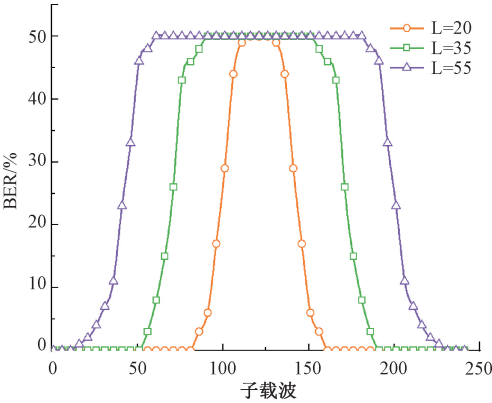


图 6 不同干扰带宽下的 BER 性能表现
Fig. 6 BER performance for different bandwidths of the attacker

2 测量平台验证

为验证 5G-A 正交失配干扰测试平台干扰性能,本章采用射频馈线直连验证和空口实测(静态/动态)两种方法开展干扰测试平台的验证测试。

2.1 射频馈线直连验证

射频馈线直连验证连接如图 7 所示,上位机通过 USB 连接线可对干扰设备的中心频点、子载波个数、发射功率等参数进行配置。综测仪一方面与测试终端 UE 建立通信链路,另一方面为干扰设备提供通信信号以完成帧头同步。干扰设备发送的干扰信号通过信道模拟器进入 UE 的通信链路中并对其进行干扰,最终的通过 PC 读取到的 UE 吞吐率判断干扰效果。射频馈线直连验证测试配置参数如表 3 所示。

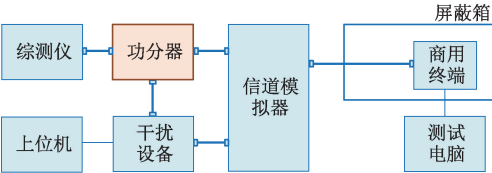


图 7 射频馈线直连验证设备连接
Fig. 7 Device connection of direct connection verification

表 3 射频馈线直连验证测试配置参数	
Table 3 Parameters for direct connection verification	
参数	值
信号中心频点	2 565 MHz
信号传输带宽	100 MHz
子载波间隔	30 kHz
终端 SSB-RSRP	-80 dBm
SSB/PDCCH/PRACH 子载波长度	240/216/139
窄带/正交干扰信号子载波长度	55
正交干扰信号归一化频偏	0.5

如图 8 所示,展示了在射频馈线直连验证中,SSB、PDCCH 和 PRACH 信道在窄带干扰与正交破坏干扰条件下的断网功率阈值对比。纵轴表示干扰信号发射功率,横轴为同样环境下重复 3 次测试。通过柱状图对比可发现,正交失配干扰方式相较于精准子载波干扰具有显著优势:以 SSB 信道为例,窄带干扰在约-24 dBm 时即可触发终端断网,而正交失配干扰需将发射功率提升至约-21 dBm 才能达到相同效果,此 3 dB 的性能差距在 PDCCH 和 PRACH 信道的干扰对比中同样存在。

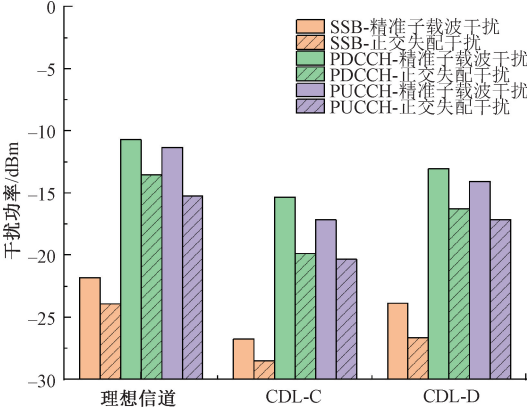


图 8 断网功率阈值
Fig. 8 Network disconnection power thresholds

进一步分析正交失配干扰的内部差异,理想信道下,SSB 信道在断网时的干扰功率阈值(约-24 dBm)分别比 PDCCH(约-14 dBm)和 PUCCH(约-15 dBm)低 10 和 9 dB,而在 3GPP 标准信道 CDL-C NLOS 模型和 CDL-D LOS 模型下^[22],SSB 的干扰功率阈值仍远低于 PDCCH 和 PUCCH,表明 SSB 的抗干扰能力显著低于后两者。这一现象揭示了不同物理信道对干扰信号的敏感度差异:控制信道(如 PDCCH)和随机接入信道(PRACH)由于功能特性差异,其抗干扰鲁棒性强于同步广播信道(SSB)。

2.2 空口测试验证

为进一步验证干扰测试平台干扰能力,在室内空口环境下开展了测试验证。室内空口干扰测试设备连接如图 9 所示,干扰测试平台由上位机、干扰设备和发射天线组成。被干扰平台由商用终端和测试 PC 组成。干扰设备与功率放大器通过射频线连接,功率放大器输出与发射天线连接,天线采用全向鞭状天线。

如表 4 所示,室内空口干扰测试平台配置参数与射频馈线直连验证测试相同,但仅针对抗干扰能力最弱的 SSB 进行干扰。如图 10 所示,为室内空口(静态/动态)实测场景。静态场景下商用终端位于干扰测试平台正前方 5 m 处,动态场景下,商用终端所在移动平台以约 1.5 m/s 速度从干扰测试平台前方横穿通过。

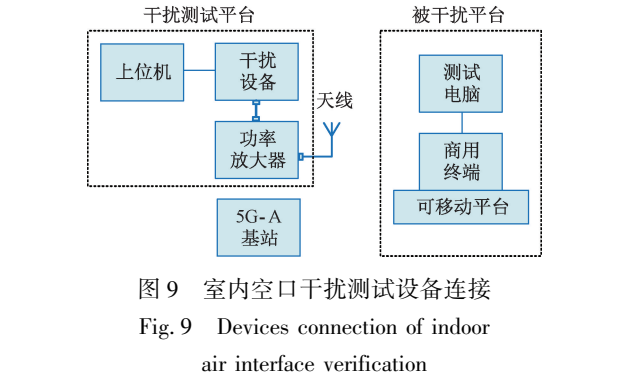


图 9 室内空口干扰测试设备连接

Fig.9 Devices connection of indoor air interface verification

表 4 干扰生效功率数据

Table 4 Interference activation power data		
场景	干扰类型	发射功率/dBm
静态	窄带干扰	25.2
	正交干扰	21.5
动态	窄带干扰	23.8
	正交干扰	19.9

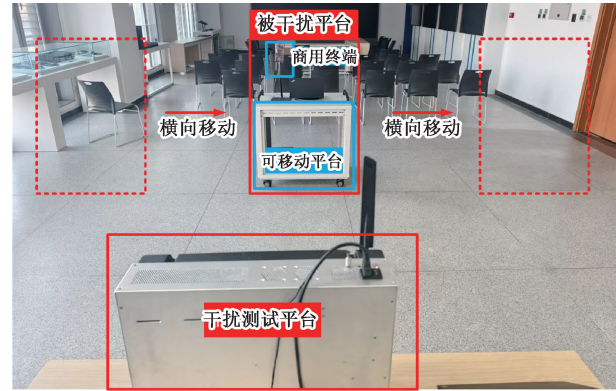


图 10 室内空口(静态/动态)实测场景

Fig. 10 Scenario of indoor air interface verification

干扰测试平台开启前,商用终端 RSRP 能稳定在 -73 dBm 左右,SINR 为 29 dB 。干扰测试平台开启后,RSRP 略上升,SINR 和 RSRQ 都急速下降,分别降为 -4 和 -16 dB 。如图 11 所示,图 11(a)为干扰开启前终端信号质量,图 11(b)为干扰开启后瞬间终端信号质量。如图 12 所示,为干扰一段时间后终端信令流程。当商用终端被干扰后发起 5G 重选流程,但多次尝试未能成功,最终选择重选到 LTE 小区。在静态和动态环境下,对窄带干扰和正交干扰两种干扰方式分别进行了对比测试验证。如表 4 所示,可以看到正交干扰在同等干扰效能下节省了约 3 dB 发射功率,这与预期结果是一致的。



(a) 干扰发射前UE信号质量
(a) UE signal quality before interference transmission

(b) 干扰发射后UE信号质量
(b) UE signal quality after interference transmission

图 11 干扰发射前后 UE 信号质量

Fig. 11 UE signal quality before and after

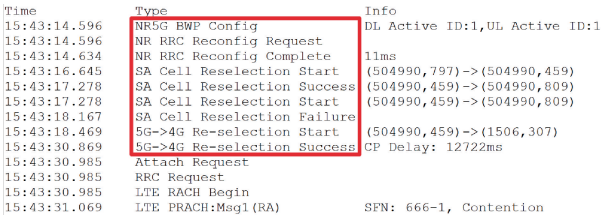


图 12 干扰发射后 UE 掉网信令

Fig. 12 Signaling for UE network disconnection after interference transmission

3 结 论

本文设计并实现了一种面向 5G-Advanced 系统的正交失配干扰测试平台并对平台功能进行验证。实现了干扰测试平台的总体结构和信号生成流程设计,并基于 FPGA、ADC/DAC 模块和射频前端搭建了干扰测试平台。通过引入归一化频率偏移参数,创新性地实现了针对 OFDM 子载波正交性破坏的广谱干扰机制,理论推导表明该策略可使干扰能量扩散效率提升至传统窄带干扰的 4 倍。同时研究对比了 SSB、PDCCH 及 PUCCH 在正交失配干扰下的性能劣化规律,实验数据表明干扰 SSB 相较于 PDCCH 和 PUCCH 具有更高的干扰能效比。最终通过射频馈线直连验证与空口(静态/动态)实测两种方法,验证了干扰测试平台的干扰能力。本平台为 5G-A 系统抗干扰性能评估提供了标准化测试工具,后续将拓展至毫米波频段干扰测试及动态多场景联合仿真研究。

参考文献

[1] GIORDANI M, POLESE M, MEZZAVILLA M, et al. Toward 6G networks: Use cases and technologies [J]. IEEE Communications Magazine, 2020, 58(3): 55-61.

- [2] BENNIS M. Ultra-Reliable and low-latency communication in 5G-advanced [J]. IEEE Network, 2020, 36(4) : 118-125.
- [3] 3GPP. Study on NR Network-Controlled Repeaters: TR 38. 833[R]. 2023.
- [4] PELECHRINIS K, ILIOFOTOU M and KRISHNAMURTHY S V. Denial of service attacks in wireless networks: The case of jammers [J]. IEEE Communications Surveys & Tutorials, 2010, 13(2) : 245-257.
- [5] XU W, TRAPPE W, ZHANG W, et al. The feasibility of launching and detecting jamming attacks in wireless networks [C]. Proceedings of the 6th ACM International Symposium on Mobile ad Hoc Networking and Computing, 2005.
- [6] GROVER K, LIM A, YANG Q. Jamming and anti-jamming techniques in wireless networks: A survey [J]. International Journal of Ad Hoc and Ubiquitous Computing, 2014, 17(4) : 197-215.
- [7] NGUYEN D, SAHIN C, SHISHKIN B, et al. A real-time and protocol-aware reactive jamming framework built on software-defined radios [C]. Proceedings of the 2014 ACM Workshop on Software Radio Implementation Forum, 2014.
- [8] STRASSER M, DANEV B, CAPKUN S. Detection of reactive jamming in sensor networks [J]. ACM Transactions on Sensor Networks, 2010, 7(2) : 16.
- [9] LIN H, HUANG S, LIU Y, et al. AI-Driven jamming attacks and defense in 5G Massive IoT networks [J]. IEEE Internet of Things Journal, 2021, 8 (12) : 10215-10228.
- [10] FRPEK T, SAGDUYU Y E, SHI Y. Deep learning for launching and mitigating wireless jamming attacks [J]. IEEE Transactions on Cognitive Communications and Networking, 2018, 5(1) : 2-14.
- [11] WEI X, WANG Q, WANG T, et al. Jammer localization in multihop wireless network: A comprehensive survey [J]. IEEE Communications Surveys & Tutorials, 2016, 19(2) : 765-799.
- [12] ZHAO S, LU Z, LUO Z, et al. Orthogonality-Sabotaging attacks against OFDMA-based wireless networks [C]. IEEE Conference on Computer Communications, 2019: 1603-1611.
- [13] KRENZ R , BRAHMA S. Jamming LTE signals [C]. IEEE International Black Sea Conference on Communications and Networking, 2015: 72-76.
- [14] LICHTMAN M, RAO R, MAROJEVIC V, et al. 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation [C]. IEEE International Conference Communication Workshop, 2018: 1-6.
- [15] LIU Y, CHEN H H, WANG L, et al. Physical layer security for 5G: Challenges and opportunities [J]. IEEE Wireless Communications, 2020, 27(5) : 162-168.
- [16] WILD T, CHEN Y, HOSSEINI K, et al. Joint channel estimation and interference cancellation for 5G NR [J]. IEEE Transactions on Signal Processing. 2022, 70: 1124-1138.
- [17] RODRIGUEZ FERNANDEZ J, GONZALEZ-PRELCLC N, LOPEZ-VALCARCE R, et al. SSB design for robust initial access in 5G mm wave networks [J]. IEEE Transactions on Wireless Communications, 2021, 20(7) : 4529-4543.
- [18] OHWATARI Y, SAGAE Y, SAWAMUKAI S, et al. Experimental evaluation of SSB interference tolerance in 5G NR [C]. IEEE ICC Workshops. 2021: 1-6.
- [19] ATTARIFAR M, SHE C, QUEK T Q S, et al. Dynamic CORESET configuration for URLLC in 5G-Advanced [J]. IEEE Journal on Selected Areas in Communications. 2022, 40(4) : 1188-1200.
- [20] AU KLI H, CHEN R, et al. Polar code optimization for control channels in 5G NR [J]. IEEE Transactions on Vehicular Technology. 2020, 69(6) : 6241-6254.
- [21] PARK S, LEE J, KIM J, et al. Deep learning-based PDCCH blind detection in 5G NR [J]. IEEE Wireless Communications Letters. 2022, 11(3) : 602-606.
- [22] 3GPP. Study on channel model for frequencies from 0.5 to 100 GHz: TR 38. 901[R]. 2025.

作者简介



王志(通信作者), 2005年于安徽大学获得双学士学位, 现为创远信科(上海)技术股份有限公司高级工程师, 研究方向为微波电子测试技术研究和无线通信测量仪器研制。
E-mail: hao. wang@transcom. net. cn

Wang Zhi (Corresponding author)

received his dual B. Sc. degrees from Anhui University in 2005. Now he is a senior engineer at Transcom Technology (Shanghai) Co., Ltd. His main research focuses on microwave electronic testing technology and the development of wireless communication measurement instruments.



陈向民, 1991年于西安电子科技大学获得学士学位, 2006年于合肥工业大学获得硕士学位, 现为创远信科(上海)技术股份有限公司研究员级高级工程师, 主要研究方向为微波电子测试技术研究和无线通信测量仪器研制。

E-mail: tim. chen@transcom. net. cn

Chen Xiangmin received his B. Sc. degree from Xidian University in 1991 and M. Sc. degree from Hefei University of Technology in 2006. Now he is a Researcher-level Senior Engineer at Transcom Technology (Shanghai) Co., Ltd. His main research mainly focuses on microwave electronic testing technology and the development of wireless communication measurement instruments.