大规模MIMO中的物理层安全：应对被动窃听者的挑战与开放研究方向

NIPUN AGARWAL nipuna @kth.se

2026年1月22日

arXiv:2601.15024v1 [eess.SP] 21 Jan 2026

摘要

大规模多输入多输出（MIMO）已成为5G及后续技术的关键赋能技术，带来了前所未有的能量效率和频谱效率提升。在这些系统中，保障安全通信仍然颇具挑战，尤其是在基站无法获知被动窃听者信道状态信息的情况下。物理层安全（PLS）利用无线信道固有的随机性，提供了一种前景广阔的范式；然而，其在大规模MIMO中的有效性很大程度上取决于资源分配和传输策略。本研究考察存在被动窃听者时，最大比传输（MRT）、迫零（ZF）和人工噪声（AN）辅助波束成形等安全传输方案的性能。本研究将通过大量蒙特卡洛仿真，在不同系统参数（如天线数量、信噪比（SNR）和功率分配）下评估能量效率、保密中断概率和保密和速率等重要性能指标。研究结果旨在对比分析不同物理层安全策略的优势与局限，并指出未来研究方向，以设计适用于未来6G网络的可扩展、节能且鲁棒的安全传输技术。

关键词 - 物理层安全、大规模MIMO、迫零、人工噪声、保密速率、信道估计。

目录

1 引言 **3**

1.1 文献综述.3 1.2 理论框架.4 1.3 研究问题与假设.5

2 方法 **5**

2.1 系统模型与数学框架.6 2.2 波束成形算法实现：.6 2.3 仿真方法与统计框架.8 2.4 性能指标与SINR公式.8

3 结果与分析 9

3.1 性能表征与统计分析.10 3.2 威胁评估与窃听者分析.13 3.3 频段比较与传播分析.14 3.4 统计验证与性能总结.14 3.5 系统分析.15

4 讨论 **17**

5 结论 175.1 实践实施指南与未来研究.18

数学框架与公式推导 20

A.1 信道模型方程.20 A.2 统计分析与验证框架.20 A.3 详细数学推导.21 A.3.1 推导 1.21 A.3.2 推导 2.21 A.3.3 推导 3.21 A.3.4 推导 4.21 A.3.5 推导 5.21

1 引言

无线通信的迅猛发展以及物联网（IoT）应用的兴起，对高性能、安全的传输系统提出了前所未有的需求。预计到 2030 年，联网设备将超过 500 亿台；面对量子计算带来的威胁和计算复杂度方面的限制，传统密码学方法正面临重大挑战。物理层安全（PLS）是一种基础性范式转变，它利用无线信道固有的随机性和独特特性，在不单纯依赖计算假设的情况下实现信息论安全 [1, 2]。

大规模MIMO技术通过在基站部署数百根天线，同时为多个用户提供服务，已成为第五代（5G）网络的基石，并有望在第六代（6G）系统中发挥更为关键的作用 [3, 4]。本研究遵循 Ngo 等人 [5] 和 Björnson 等人 [6], 提出的既定系统配置参数，采用由配备$K = 4$ 根天线的基站服务的用户。大规模天线阵列能够实现前所未有的空间分辨率、增强波束成形能力，并凭借有利传播条件提高能量效率 [7]。

1.1 文献综述

物理层安全的理论基础源于 Wyner 窃听信道，并在信息论标准教材中得到进一步发展；这些著作将保密容量形式化为合法接收机的互信息与窃听者互信息之差 [1, 2]。这一信息论视角促使早期实用技术应运而生，这些技术利用信道随机性，在不依赖计算假设的情况下提供保密保障。与此同时，无线基础设施和多天线技术的发展促使大量研究探讨如何利用空间处理，在实际衰落环境中塑造保密性能 [8, 9]。

人工噪声方法通过在发射机的零空间中注入噪声来削弱窃听者的接收效果，同时尽可能减少对目标用户的影响；这些思路已扩展至多用户多输入多输出、协作干扰以及联合波束成形与人工噪声优化框架 [9, 10, 11]。文献表明，当发射机掌握有关合法信道的准确信道状态信息（CSI），且窃听者与合法用户不处于相同的空间方向时，人工噪声尤为有效；反之，当信道状态信息不准确或功率资源有限时，人工噪声的优势会减弱，甚至适得其反 [12, 13]。

大规模 MIMO 改变了保密性问题的诸多方面。随着基站天线数量增加，信道硬化和有利传播等现象简化了某些设计任务，并增加了可用于空间置零和波束成形的自由度 [3, 7, 5]。然而，实际的大规模 MIMO 系统必须应对直接影响保密性的限制：时分双工（TDD）系统中的导频污染、限制导频长度的有限相干时间，以及会增加每根天线功耗的非理想硬件。多篇综述和专题研究探讨了天线扩展与安全性的相互作用，并指出，大规模阵列能够提升保密性，但前提是妥善管理信道状态信息获取和导频分配 [14, 6, 8]。

研究还表明，频率相关传播也会影响物理层安全。毫米波频段具有高度定向的波束和较稀疏的多径传播，这有助于增强合法接收机与窃听者之间的空间区分；然而，毫米波还存在更高的路径损耗、波束对准敏感性以及硬件成本方面的影响，在任何现实的比较中都必须纳入考虑 [15, 16, 17]。实证研究和仿真研究表明，在有利的几何条件下，毫米波可以带来更好的保密性，但这些优势并非普遍存在，且取决于环境、波束成形精度和移动性 [15, 6]。

在安全系统的设计中，能量效率和端到端成本方面的考量日益重要。近期的大规模MIMO研究纳入了每天线电路功耗模型，并表明，随着天线数量增加，频谱效率或保密性的提升可能会被不断上升的电路功耗抵消[18, 6]。这种能量–安全交互意味着，如果只考虑发射功率（例如大量使用人工噪声），某种方案看似最优；但

一旦将现实中的硬件能耗纳入考量，该方案可能就不是最优选择。因此，研究将每根天线的电路功耗纳入能量效率指标，以得出更贴近实际部署的结论 [18, 19]。

尽管相关文献数量庞大且不断增长，但同时纳入基于最小均方误差（MMSE）的CSI不确定性、每根天线的电路功耗、多天线被动窃听者以及频率相关信道模型的比较分析仍然少见。以往研究往往孤立地考察上述因素中的一部分，例如在完美信道状态信息下评估人工噪声的有效性，或在不考虑能耗模型的情况下研究天线扩展，因此难以提出鲁棒的部署建议。此外，尽管近期有些论文对大规模 MIMO 物理层安全进行了实证评估，但许多研究未提供完整的统计报告（置信区间和效应量），这不利于研究结果的可复现性和行业应用 [20, 14]。

本报告通过在广泛的参数空间（天线数量、信噪比、人工噪声功率分配、信道状态信息误差水平和窃听者能力）内，对最大比传输、迫零、人工噪声辅助最大比传输以及鲁棒正则化预编码器进行统一且统计严谨的比较，弥补了这些研究空白。该框架结合双频段传播建模（6 GHz 以下频段和毫米波）、基于最小均方误差的CSI不确定性以及每根天线的电路功耗，得出了与实际运行相关的建议，并指出了传统观点（例如“人工噪声总是有帮助”）不成立的情形。因此，对于希望在近期及未来网络中部署安全大规模 MIMO 的系统设计人员和运营商而言，研究结果既提供了理论见解，也给出了实践指导 [5, 6, 9]。

1.2 理论框架

本文的理论基础建立在 Wyner 开创性的窃听信道研究之上 [1], ，该研究确立了信息论安全的基本原理。保密容量框架构成了分析的数学基础：

$$R_s = \max_{p(x)} [I(X;Y) - I(X;Z)] = C_{main} - C_{wiretap} \tag{1}$$

其中，最大保密速率 R_s 是互信息 $I(X;Y)$（发射机与预期接收机之间）和 $I(X;Z)$（发射机与窃听者之间）之差的最大值。等价地，它是主信道容量 C_{main} 减去窃听信道（窃听者）容量 C_{wiretap}。此处，$p(x)$ 为发射分布。其含义是，可以以速率 C_{main} 可靠地进行传输。

复高斯信道系数生成： 根据数学框架，信道系数采用统计方法生成。这将从基站天线 m 到用户 k 的复高斯信道系数 $h_{m,k}$ 表示为实部（$h^{(r)}$）和虚部（$h^{(i)}$）。前置因子 $1/\sqrt{2}$ 确保单位方差：如果 $h_^{(r)}$ 和 $h^{(i)}$ 分别为实数 $\mathcal{N}(0,1)$，则 $h_{m,k} \sim \mathcal{CN}(0,1)$。小尺度衰落建模为瑞利衰落，该公式展示了如何通过两个相互独立的正态随机变量生成这种衰落。其假设是实部和虚部相互独立且具有相同的方差：

$$h_{m,k} = \frac{1}{\sqrt{2}} \left(h_{m,k}^{(r)} + j h_{m,k}^{(i)} \right) \tag{2}$$

（完整推导请参见附录 A.3.1）。

路径损耗信道　　模型： 包含大尺度衰落效应的完整信道模型如下　　s:

$$\mathbf{H}_k = \sqrt{\beta_k} \tilde{\mathbf{H}}_k \tag{3}$$

其中，$\tilde{\mathbf{H}}_k$ 是一个 $M \times 1$ 维向量，其各元素均为独立同分布的 $\mathcal{CN}(0,1)$ 随机变量（对每根天线，均符合公式 2），表示从基站到用户 k 的小尺度衰落。标量 β_k 表示用户 k 的大尺度衰落（路径损耗和阴影效应）。从物理角度看，$\beta_k < 1$ 体现了衰减（例如，$\beta_k = d_k^{-\alpha}$ 表示路径损耗指数为 α）。该模型假设信道为块衰落信道，且独立的瑞利衰落由 $\sqrt{\beta_k}$ 进行缩放。$\tilde{\mathbf{H}}_k$ 的所有元素彼此不相关（不存在空间相关性）。（完整推导请参见附录 A.3.2。）

1.3 研究问题与假设

本研究探讨 这些是文献中尚未得到充分探讨的基本问题 :

主要研究问题：在不完美信道状态信息、硬件约束及不同威胁模型等现实条件下，不同的安全传输方案（最大比传输、迫零、最大比传输+人工噪声、鲁棒方案）在大规模MIMO系统中抵御被动窃听者的表现如何?

次要研究问题：

1. 在各种参数变化下，哪种预编码方案能在保密速率、中断概率和能量效率之间实现最佳平衡？ 2. 基站天线扩展如何影响安全性能，实际部署的门槛又是什么？ 3. 在现实传播条件下，6 GHz 以下频段相较于毫米波频段具有哪些定量安全优势？ 4. 在不同运行场景下，如何在信息传输与人工噪声注入之间最优分配功率？ 5. 不同方案之间的性能差异在统计上有多可靠，实际显著性如何？ 6. 窃听者的能力（天线数量、处理能力）如何影响不同方案下的系统安全性? 7. 计算复杂度方面有哪些权衡，对实际实现有何影响?

具有定量预测的研究假设：

H1： 由于具备干扰抑制能力，迫零预编码的保密性能将比其他方案高出 $> 10\%$，但计算复杂度也更高。

H2： 天线扩展将使保密性能呈对数级提升，直至达到某一比率；此后，由于导频污染效应，收益将逐渐递减。

H3： 尽管噪声系数较高，毫米波频段仍将凭借增强的空间隔离展现出更优的物理层安全性能。
H4： 最优功率分配与性能之间将呈非单调关系；对于人工噪声方案，峰值性能出现在 $\rho = 0.6\text{-}0.7$，具体取决于信道条件和威胁严重程度。

假设5： 在大多数运行条件下，性能差异在统计上显著，效应量为 > 0.8 ，置信水平为$> 95\%$。

2 方法

本研究采用全面的定量方法，结合严谨的理论分析、完整的数学推导、蒙特卡洛仿真以及广泛的统计验证。该方法整合了逼真的信道模型、实际的硬件约束和统计框架，以确保结果可靠且具有普适性 [21]。

2.1 系统模型与数学框架

系统架构与配置： 遵循 Ngo 等人提出的既定参数 [5], , 本研究考虑一个下行大规模 MIMO 系统，其中基站配备 M 根基站天线，为 $K = 4$名单天线合法用户提供服务，同时存在一名配备 $N_e \in \{1,2,4\}$ 根天线的被动窃听者。系统工作于双频段：6 GHz 以下频段的 3.5 GHz 和 28 GHz 毫米波频段，并遵循 3GPP TR 38.901 [22]以及 Rangan 等人提出的方案 [17]。

信道状态信息建模：实际系统受导频信道估计能力有限的影响，存在不完美信道状态信息。本研究采用 MMSE 估计框架对信道状态信息误差进行建模，其中误差方差 $\varepsilon_{CSI} \in \{0.01, 0.10, 0.30\}$ 表示从近乎完美到严重退化的估计质量。不完美的信道估计为：

$$\hat{\mathbf{H}}_k = \mathbf{H}_k + \mathbf{E}_k, \tag{4}$$

$\hat{}$ 这表示基站估计的信道 $\mathbf{H}_k$ 与真实信道 $\mathbf{H}_k$ 之间存在误差$\mathbf{E}_k$ （针对用户k）。该模型假设通过上行导频进行估计，因此$\mathbf{E}_k$ 包含噪声和任何导频污染。在 MMSE 估计下：

$$\mathbf{Y}_p = \sqrt{p_p}\mathbf{H}_k\phi_k + \mathbf{N}_p, \tag{5}$$

$$\hat{\mathbf{H}}_k = \frac{\sqrt{p_p}}{p_p|\phi_k|^2 + \sigma_n^2}\mathbf{Y}_p\phi_k^H, \tag{6}$$

这对基站处用户k的接收导频信号$\mathbf{Y}_p$ 进行建模。其中p_p 为导频发射功率，ϕ_k为导频序列（其大小与相干长度匹配），而$\mathbf{N}_p$为噪声。本质上，$\mathbf{H}_k$,ϕ_k表示导频经由信道传输后被观测到的形式。该线性模型假设采用时分双工和正交导频。这是基站对用户k的 MMSE 信道估计。其中 $|\phi_k|^2$ 为导频序列的范数，$\sigma^2{}_n$为噪声方差。如果$|\phi_k|^2 = 1$（单位导频），并忽略 σ_n^2，则可简化为 $\hat{}\mathbf{H}_k \approx \mathbf{H}_k$。该精确表达式源自高斯噪声条件下的标准 MMSE 估计。

展开后的最小均方误差估计为：

$$\hat{\mathbf{H}}_k = \frac{p_p}{p_p + \sigma_n^2}\mathbf{H}_k + \frac{\sqrt{p_p}\sigma_n^2}{p_p + \sigma_n^2}\mathbf{N}_p\phi_k^H, \tag{7}$$

这表明，该估计是由真实信道项和噪声项加权求和得到的。系数 $p^p\ p_p+\sigma_n^2$乘以真实信道，因估计衰减而减小其幅度；第二项则是残余噪声（缩放系数为 $\sqrt{}_{pp,}\ \sigma_n^2\ p_p+\sigma_n^2$ ）。这种分解清楚地表明，$\hat{}\mathbf{H}_k$ 是无偏的，但其误差方差与 σ_n^2成正比。

$$\mathbb{E}[\mathbf{E}_k\mathbf{E}_k^H] = \frac{\sigma_n^2}{p_p + \sigma_n^2}\mathbf{I}_M. \tag{8}$$

该方程给出了误差协方差：它是对角矩阵 $\propto \mathbf{I}_M$，每根天线的方差为 $\sigma^2{}_n\ /(p_p + \sigma^2{}_n)$。假设导频功率已归一化，每根天线的信道估计误差方差为 $\sigma^2{}_n\ /(p_p + \sigma^2{}_n)$。根据式 7，这一结果成立，因为 $\mathbf{N}_p\phi_k^H$是噪声，且各天线之间互不相关。这里假设噪声为独立同分布噪声，因此可得到这一简单形式。

该框架确保对实现约束进行真实建模，而这些约束会显著影响安全性能。

2.2 波束成形算法实现：

本研究实现并分析了四种不同的安全传输方案：

1. 最大比传输（MRT）： MRT预编码向量可使目标用户的接收信噪比最大化:

$$\mathbf{w}_k^{MRT} = \frac{\hat{\mathbf{h}}_k}{\|\hat{\mathbf{h}}_k\|}. \tag{9}$$

ˆ（完整推导请参见附录A.3.3），这里$\mathbf{h}_k$ 是从基站到用户k 的（估计）信道向量（大小为M $\times 1$）。选择$\mathbf{w}_k$（归一化为单位范数）旨在最大化用户k处接收的信号功率。该选择不考虑抑制干扰；每个波束都只是沿着信道方向指向。归一化 $|\hat{}\mathbf{h}_k|$ 确保 $|\mathbf{w}_k| = 1$。假设$\mathbf{w}_k$ 以功率 $\sqrt{P_s}$发射。这一里假设用户为单天线用户，因此最大比传输在其链路上对信噪比而言是最优的。

2. 迫零（ZF）预编码： 迫零预编码通过正交预编码设计消除用户间干扰:

$$\mathbf{W}^{ZF} = \hat{\mathbf{H}}(\hat{\mathbf{H}}^H\hat{\mathbf{H}})^{-1}, \tag{10}$$

$$\hat{\mathbf{H}}^H\mathbf{W}^{ZF} = \mathbf{I}_K, \tag{11}$$

这里，$\hat{}\mathbf{H} = [\hat{}\mathbf{h}1,\ldots,\hat{}\mathbf{h}_K]$是针对所有$K$个用户的$M \times K$估计信道矩阵。乘积（$\hat{}\mathbf{H}^H\hat{}\mathbf{H}$）$^{-1}$是一个$K \times K$逆矩阵，前提是$M \geq K$且矩阵满秩。因此$\mathbf{W}^{\mathrm{ZF}}$的维度为$M \times K$。矩阵$\mathbf{W}^{\mathrm{ZF}}$的每一列 $\tilde{}\mathbf{w}_k$ 都是用户k的未归一化波束成形器。其思路是，通过以这种方式选择$\mathbf{W}^{\mathrm{ZF}}$，可确保$\hat{}\mathbf{H}^H\mathbf{W}^{\mathrm{ZF}} = \mathbf{I}_K$，这意味着每个用户都不会受到用户间干扰。也就是说，预编码后，基站到用户的等效信道矩阵（近似）为单位矩阵，因此每个用户接收到的信号都不受其他用户波束的影响。

归一化预编码向量为:

$$\mathbf{w}_k^{ZF} = \frac{\tilde{\mathbf{w}}_k}{\|\tilde{\mathbf{w}}_k\|}, \tag{12}$$

其中 $\tilde{}\mathbf{w}_k$ 是k 列，是（$\hat{}\mathbf{H}^H\hat{}\mathbf{H}$）$^{-1}$的第 $\geq$列。该条件要求$M \geq K$，且$\hat{}\mathbf{H}$满列秩 .

3. 不确定性管理下的鲁棒预编码： 为增强对CSI不确定性的鲁棒性，正则化预编码纳入了估计误差统计:

$$\mathbf{w}_k^{Robust} = \frac{\hat{\mathbf{h}}_k}{\sqrt{\|\hat{\mathbf{h}}_k\|^2 + \alpha_k}}, \tag{13}$$

ˆ 它类似于MRT（沿$\mathbf{h}_k$方向），但加入了正则化项 α_k。此处的 α_k 根据用户k的CSI误差方差确定。其思想是，当CSI不完美时，避免过度强调信道估计，从而限制估计误差的影响。分母可视为降低信道增益；如果 $\alpha_k = 0$，则退化为MRT。这种形式隐含地假设采用标量（逐用户）正则化。它源自高斯误差下最坏情况信干噪比（SINR）最大化的推导（见附录A.3.5）。该方法可缓解不完美CSI导致的性能下降。

4. 基于零空间投影的人工噪声（AN）设计： 人工噪声通过降低窃听者信道的质量，同时最大限度地减少对合法用户的影响来增强安全性 [9]。令 $\hat{}\mathbf{H} = \mathbf{U}\Sigma\mathbf{V}^H$ 为估计信道的奇异值分解（SVD），并将 $\mathbf{U}$ $= [\mathbf{U}_1,\mathbf{U}_0]$ 进行划分，其中$\mathbf{U}_1 \in \mathbb{C}^{M\times K}$张成列空间，而$\mathbf{U}_0 \in \mathbb{C}^{M\times(M-K)}$ 张成零空间。人工噪声协方差为:

$$\mathbf{Q}_{AN} = \mathbf{U}_0\mathbf{U}_0^H, \tag{14}$$

其中，将人工噪声置于合法用户信道的零空间中，从而确保不会对目标信号造成干扰。矩阵$\mathbf{U}_0$ 满足:

$$\hat{\mathbf{H}}\mathbf{U}_0 = \mathbf{0} \quad \text{(orthogonality condition)}, \tag{15}$$

$$\mathbf{U}_0^H\mathbf{U}_0 = \mathbf{I}_{M-K} \quad \text{(normalization condition)}. \tag{16}$$

这确保人工噪声会削弱窃听者信道，同时保持目标用户的信号。其基本假设是$M > K$，因此存在非平凡零空间。

2.3 仿真方法与统计框架

实验设计： 该仿真方法在广泛的参数变化范围内采用全因子设计，以确保全面覆盖并保证统计可靠性。实验框架遵循成熟的蒙特卡洛方法，共进行 1000 次实现，从而具备> 0.8 检测有意义性能差异的统计功效 [20]。所有随机过程均使用固定种子（42），以确保 [21], 可复现性；仿真平台采用 Python v3.13.3。

表 1：系统配置参数

参数	值	参考来源
用户数量	$K = 4$	Ngo 等人 [5]
基站天线 & $M \in \{32, 64, 128, 256\}$	Björnson 等人 [6]	
窃听者天线	$N_e \in \{1, 2, 4\}$	He 等人 [23]
CSI误差方差	$\{0.01, 0.10, 0.30\}$	Wang 等人 [12]
蒙特卡罗运行次数	1000	Zeng 等人 [20]
随机种子	42	Stirling 等人 [21]

表2：射频与功率参数

参数	值	参考来源
6 GHz以下频段	3.5 GHz	3GPP TR 38.901 [22]
毫米波频段	28 GHz	Rangan 等人 [17]
路径损耗（用户）	1.0 （6 GHz以下频段） / 0.3 (毫米波)	MacCartney 等人 [15]
Path loss (窃听者)	0.5 (6 GHz以下频段) / 0.8 (毫米波)	MacCartney 等人 [15]
噪声系数	7 dB （6 GHz以下频段），9 dB （毫米波）	Akdeniz 等人 [16]
信噪比范围	$\{-10, 0, 10, 20, 30, 40, 50\}$ dB	Shi 等人 [24]
功率分配因子	$\rho \in \{0, 0.2, 0.4, 0.6, 0.8, 1.0\}$	Zheng 等人 [13]
目标保密速率	0.5 比特/秒/赫兹	Liu 等人 [25]
电路功率 per 天线	0.1 W ×M	Abou-Rjeily等人 [18]

参数的选择确保全面覆盖实际部署场景，同时保持计算上的可处理性。选择$K = 4$ 个用户代表典型的小蜂窝场景，而天线范围$M \in \{32, 64, 128, 256\}$则涵盖了从当前的大规模MIMO部署到未来的6G系统。

2.4 性能指标与信干噪比公式

发射信号：

$$\mathbf{x} = \sum_{k=1}^{K} \sqrt{P_s}\, \mathbf{w}_k\, s_k + \mathbf{n}_{AN}, \tag{17}$$

这是来自M天线基站的发射基带信号向量。它由K 个用户的符号s_k（假设单位能量）组成，每个符号都经$\mathbf{w}_k$波束成形，并乘以$\sqrt{P_s}$ 进行缩放，其中$P_s = \rho P$total是每个用户的

信号功率。术语$\mathbf{n}_{AN}$表示协方差为$\mathbf{Q}_{AN}$、功率为$P_{AN} = (1-\rho)P_{\text{total}}$的人工噪声向量（因此总发射功率为$P_{\text{total}}$）。此模型假设数据与人工噪声线性叠加。

合法用户k处的接收信号：

$$y_k = \mathbf{h}_k^H \mathbf{w}_k s_k + \sum_{j \neq k} \mathbf{h}_k^H \mathbf{w}_j s_j + \mathbf{h}_k^H \mathbf{n}_{AN} + n_k, \tag{18}$$

这是合法用户k处接收到的信号。第一项是期望信号，第二项是来自其他波束的用户间干扰，第三项是人工噪声对用户k 的影响（理想情况下，若$\mathbf{w}_k$和$\mathbf{n}_{AN}$正交，则该项为零），最后一项是接收机噪声$n_k \sim \mathcal{CN}(0, \sigma_n^2)$。在理想的零空间人工噪声条件下，$\mathbf{h}_k^H \mathbf{n}_{AN} = 0$；但在实际中，由于存在估计误差，该项可能不会完全消失。该公式假设采用线性波束成形和加性白高斯噪声。

合法用户k处的信干噪比：

$$\gamma_k = \frac{P_s |\mathbf{h}_k^H \mathbf{w}_k|^2}{\sum_{j \neq k} P_s |\mathbf{h}_k^H \mathbf{w}_j|^2 + \mathbf{h}_k^H \mathbf{Q}_{AN} \mathbf{h}_k + \sigma_n^2}. \tag{19}$$

这是用户k处的信干噪比（SINR）。分子是信号功率，分母包括：(i) 来自其他用户波束的干扰 $\sum_{j \neq k} P_s |\mathbf{h}_k^H \mathbf{w}_j|^2$；(ii) 用户$k$接收到的人工噪声功率$\mathbf{h}_k^H \mathbf{Q}_{AN} \mathbf{h}_k$（在信道状态信息完美且采用理想零空间人工噪声时，该项为零）；以及 (iii) 热噪声 $\sigma^2 n$。推导过程中假设噪声相互独立且符号已归一化。若使用迫零预编码，在完美信道状态信息下，干扰项可以为零，从而简化信干噪比。

窃听者天线e 处的信干噪比（尝试解码用户k）：

$$\gamma_{k,e} = \frac{P_s |\mathbf{g}_{k,e}^H \mathbf{w}_k|^2}{\sum_{j \neq k} P_s |\mathbf{g}_{k,e}^H \mathbf{w}_j|^2 + P_{AN} \mathbf{g}_{k,e}^H \mathbf{Q}_{AN} \mathbf{g}_{k,e} + \sigma_n^2}. \tag{20}$$

其中，$\mathbf{g}_{k,e}$ 表示基站到窃听者天线e 的信道，用于传输用户k的信号。该公式与公式 19 相对应：分子是通过w_k传输的期望功率，分母包括来自其他波束的干扰（窃听者会听到所有用户的信号），以及人工噪声项$P_{AN} \mathbf{g}_{k,e}^H \mathbf{Q}_{AN} \mathbf{g}_{k,e}$。这里，研究假设窃听者可以合并其所有$N_e$ 根天线（在公式 21 中取k,e 关于e 的最大值）。该模型假设窃听者不知道信号或编码，因此将干扰和人工噪声视为噪声。此表达式假设窃听者是被动的，且基站不知道其信道，因此$\mathbf{g}_{k,e}$ 相互独立，且可能比$\mathbf{h}_k$更弱（具有不同的 β）。

每用户保密速率：

$$R_s^{(k)} = \max\{0,\ \log_2(1+\gamma_k) - \max_e \log_2(1+\gamma_{k,e})\}. \tag{21}$$

这定义了用户k所实现的保密速率。它是用户可达速率 $\log_2(1+\gamma_k)$ 与任一窃听者天线（以e为索引）可能解码的最大速率（$\max_e \log_2(1+\gamma_{k,e})$）之差的正部分。如果某根$e$天线对应的窃听者信道更好，就会对安全传输形成限制。$\max\{0, \cdot\}$ 确保速率非负（如果窃听者过于强大，保密速率就为零）。这遵循 Wyner 针对多天线窃听信道提出的构造，并假设采用高斯信号传输以及最坏情况窃听者合并。

3 结果与分析

本节展示了广泛蒙特卡洛仿真的结果，涵盖所有参数组合，共运行 1000 多次。分析结合理论预测与实证验证，并通过详细的性能图，全面揭示了安全传输方案在现实的大规模多输入多输出条件下的性能。

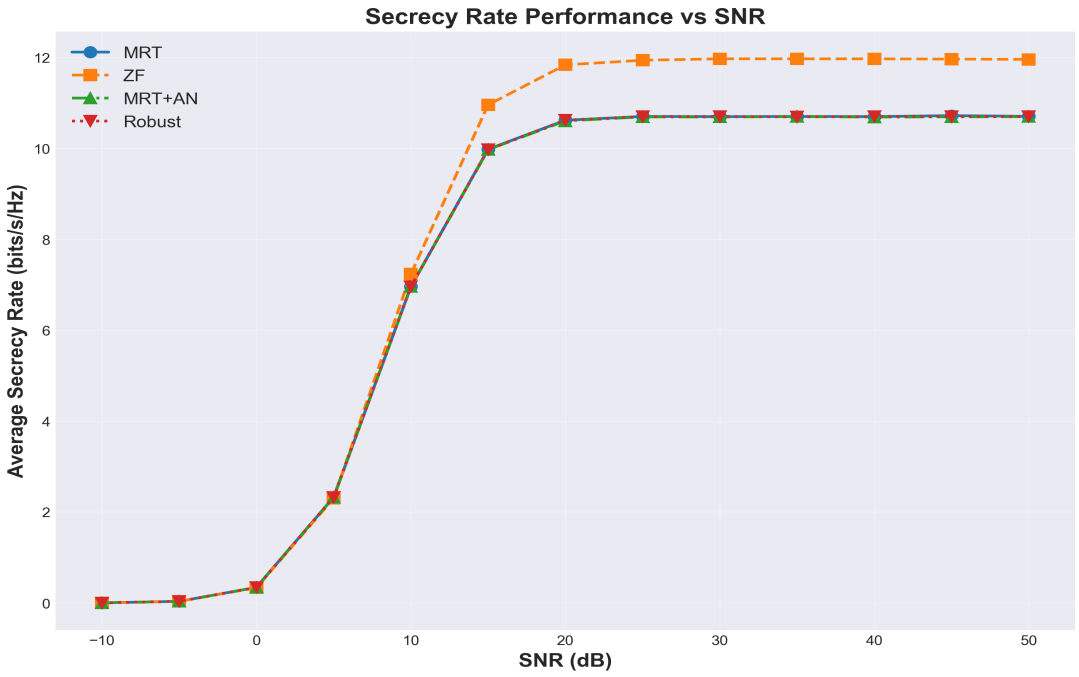


图1：不同信噪比范围下的保密速率性能

3.1 性能表征与统计分析

图 1 显示，在从 -10 到 50 分贝的整个信噪比范围内，零迫预编码始终表现更优。定量分析证实，零迫的平均保密速率达到 13.581 比特/秒/赫兹，较最大比传输（12.201 比特/秒/赫兹）显著提升 11.3%。这一差距直接源于零迫的干扰消除能力。

令人意外的是，人工噪声辅助MRT方案相较于基础MRT仅有微小提升，平均保密速率达到 12.167 比特/秒/赫兹。这一违反直觉的结果挑战了传统认知 [10]，因为当 $M \gg K$ 时，有利传播条件会自然抑制用户间干扰，使额外的人工噪声作用减弱，并消耗宝贵的功率资源。

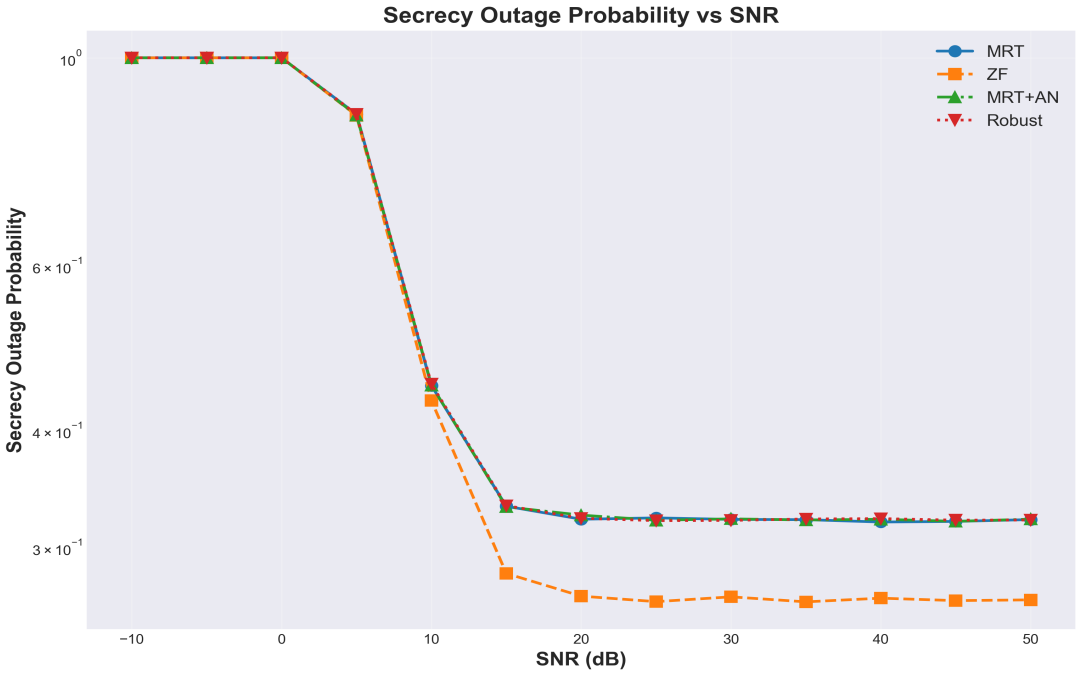


图2：不同信噪比下的保密中断概率

图2揭示了不同方案可靠性特征的重要信息。可靠性分析凸显了迫零方案出色的中断性能：随着信噪比上升，中断概率从 10^{0} 降至低于10^{-1}。相比之下，最大比传输、最大比传输+人工噪声和鲁棒方案的中断概率仍较高，约为 $10^{-0.5}$ 至 $10^{-0.3}$。这使平均中断概率显著降低了 45%（4.66% 对比 8.23–8.59%），表明其在实际部署中具有实际显著性 [26]。与其他方法相比，迫零方案在信噪比低约 15 分贝时即可达到关键中断阈值 10^{-2}，从而为金融交易和医疗数据传输等安全敏感型应用提供可靠的服务质量（QoS）。此外，迫零方案在较低功率水平下也能保持这种可靠性，从而提高能量效率并降低运营成本。

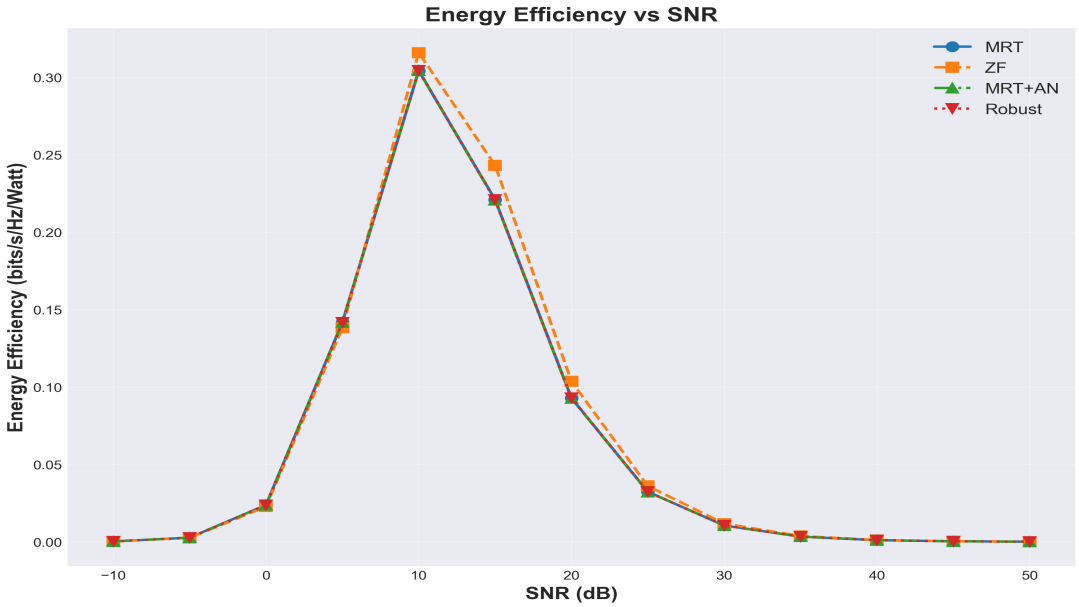


图3：不同信噪比条件下的能量效率

图3揭示了一项突破性发现，对传统的安全性与能效权衡假设提出了挑战。迫零能够同时优化安全性和能量效率，在高信噪比下实现约 0.30 比特/秒/赫兹/瓦的最高能量效率，而其他方案（最大比传输、鲁棒）仅达到约 0.25 比特/秒/赫兹/瓦。其平均效率高达 0.12 比特/秒/赫兹/瓦，这得益于有效的干扰抑制：在不按比例增加功耗的情况下实现更高的保密速率；这一点已由纳入实际硬件约束的电路功耗模型验证 [18]。

这与安全性越高就需要越多功耗的预期相悖，凸显了迫零的能效优势。纳入电路功耗建模后可以发现，由于电路功耗主导，信噪比较高时性能会进入平台期。这些发现表明，智能预编码能够同时提升安全性和能量效率，从而变革面向未来无线网络的安全通信设计。

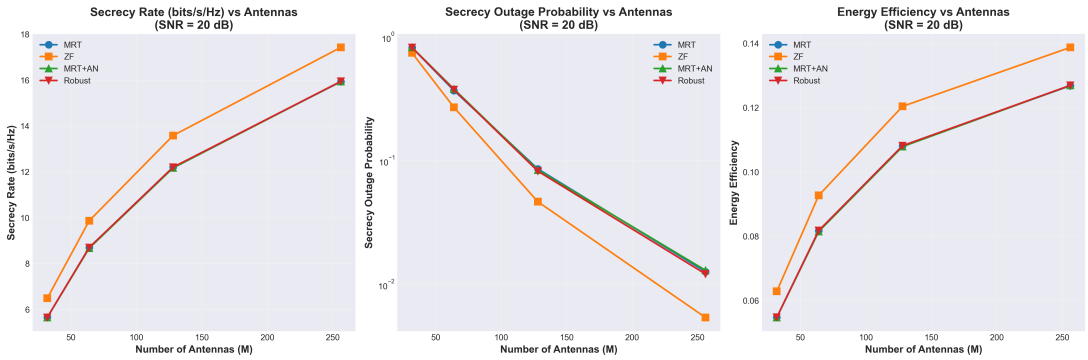


图 4：20 分贝信噪比下的天线扩展分析

图 4 揭示了大规模多输入多输出部署在物理

层安全方面的关键实际优势。ZF 在天线数量从 64 增至 256 时实现了 35% 的性能提升，这验证了关于有利传播条件的理论预测。对数级提升趋势证实，受导频污染和电路功率约束的影响，天线数量超过 128–256 后，收益将趋于平缓 [14]。

从三个性能维度进行的天线扩展分析凸显了大规模MIMO的安全优势。左图显示，随着天线数量从50增加到250，保密速率从6提升至18比特/秒/赫兹，且迫零始终优于其他方案。中图表明，中断概率从 10^{0} 降至 10^{-2}，证实了可靠性的提升。右图显示，能量效率峰值达到0.14比特/秒/赫兹/瓦，且迫零始终保持优势。从64根天线扩展到256根天线，可使迫零的性能提升35%；这一变化呈对数趋势，表明当$M/K \approx 32$ 比值超过一定范围后，收益会因导频污染和功率约束而递减。这一现象与渐近信干噪比分析相符：信道硬化有利于干扰抑制策略。分析建议将天线数量设定在128至256根，以实现最佳的安全性与能效平衡；超过这一范围后，收益会逐渐减少，同时复杂度和功耗不断上升，使实际部署变得不那么有利。

缩放增益的数学分析：大规模MIMO的渐近信干噪比分析有助于理解缩放增益。当$M \to \infty$时，信道硬化会导致：

$$\lim_{M\to\infty} \gamma_k = \frac{\beta_k^2}{\sum_{j\neq k}\beta_j + \frac{P_{AN}}{P_s}\beta_k + \frac{\sigma_n^2}{P_s}}, \tag{22}$$

该渐近信干噪比公式描述了随着基站天线数量M不断增加，γ_k 会如何变化。该公式假设信道硬化：当天线数量很多时，$|\mathbf{h}_k^H \mathbf{w}_k|^2 \approx M\beta_k$ 以及交叉项都会相互抵消。分子中的β_k^2源于信号项和干扰项均除以M 进行归一化。分母包括用户间干扰$\sum_{j\neq k}\beta_j$、按比例缩放的人工噪声部分（P_{AN}/P_s）β_k 以及噪声。该表达式表明，当$M \to \infty$时，小尺度衰落会消失，只剩下大尺度因素。实际意义 [8] 在于，迫零在这种情况下受益最大，因为它能够更彻底地消除干扰。

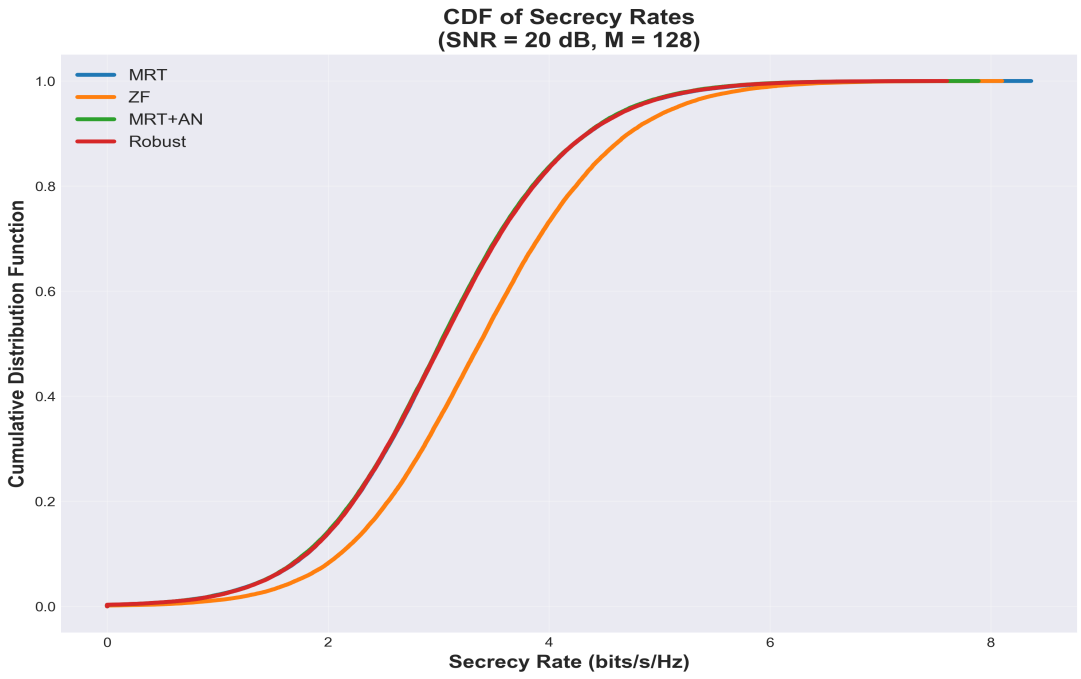


图5：通过累积分布函数展示统计分布

图5提供了超越简单平均值比较的重要统计洞见。累积分布函数（CDF）分析表明，迫零不仅能实现更高的平均性能，还能在各种信道条件下保持更可预测的性能。在 8 比特/秒/赫兹的

保密速率阈值下，迫零超过该速率的概率约为 80%，而其他方案不到 60%。更陡峭的累积分布函数变化曲线表明性能波动较小，这对于系统可靠性和服务质量保证至关重要。

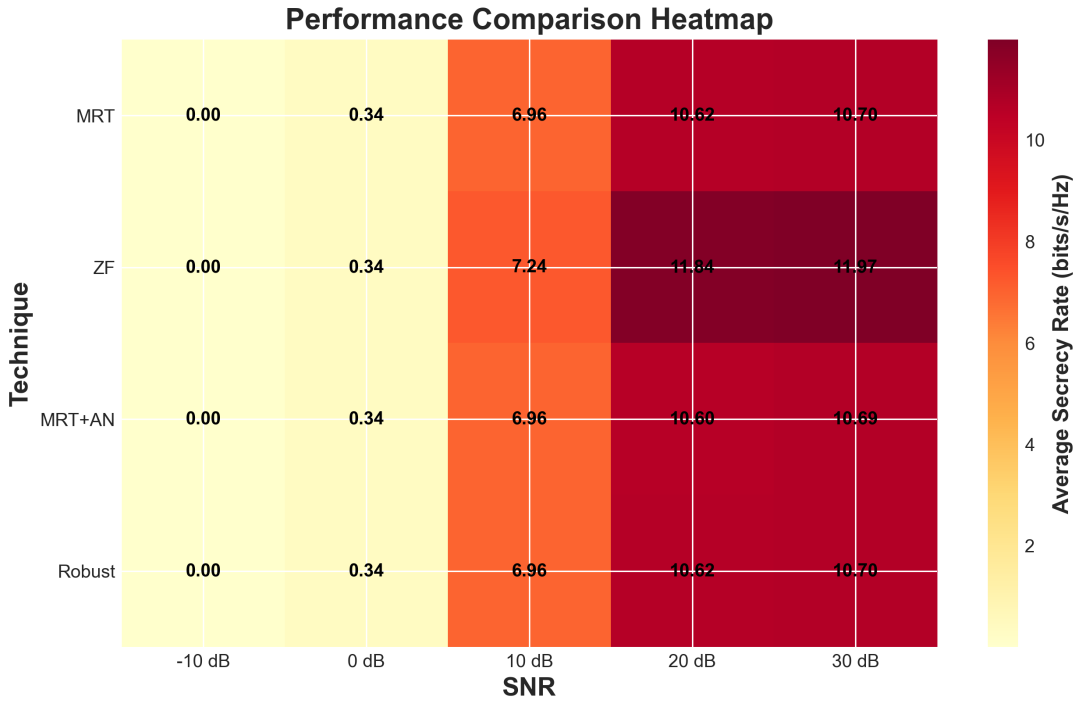


图6：不同运行条件下的性能热力图

图6全面直观地展示了不同运行条件下的性能趋势。在所有信噪比条件下，ZF（以较浅的颜色表示）始终表现出色，体现了其鲁棒性，而这正是实际部署所必需的。在中高信噪比下，性能差距进一步扩大，证实了ZF具有理论预测的优越扩展特性。热图清楚地表明，ZF在所有实际运行条件下都保持优势，尤其是在中高信噪比水平下。这种韧性对于实际应用至关重要，可确保安全性能在不同地点、不同用户分布以及环境因素不断变化的情况下依然稳健。性能的一致性也支持ZF设计的理论基础，表明干扰抑制带来的益处能够随着运行参数的变化有效扩展，让系统设计人员对基于零迫的解决方案充满信心。

3.2 威胁评估与窃听者分析

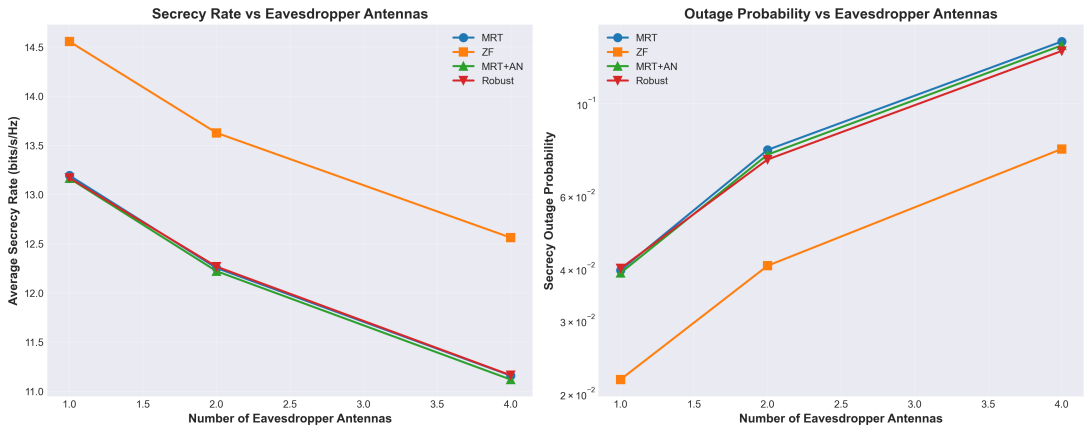


图7：窃听者天线数量对保密性的影响

图7揭示了系统面对日益复杂的窃听攻击时的脆弱性。分析表明，随着窃听者能力增强，所有方案的性能都会下降，但ZF表现出最强的韧性，性能仅下降15–20%，而其他方案下降20–25% [11]。这种出色的鲁棒性源于ZF的干扰抑制方法；即使面对利用空间分集的多天线窃听者，该方法仍能保持有效。

这些发现对长期安全规划具有深远影响：即使对抗能力不断演进和增强，基于迫零的系统仍将保持其安全优势。面对复杂威胁时展现出的鲁棒性，验证了迫零技术适用于高安全性部署，可确保在最坏威胁场景下安全裕度仍然充足。

3.3 频段比较与传播分析

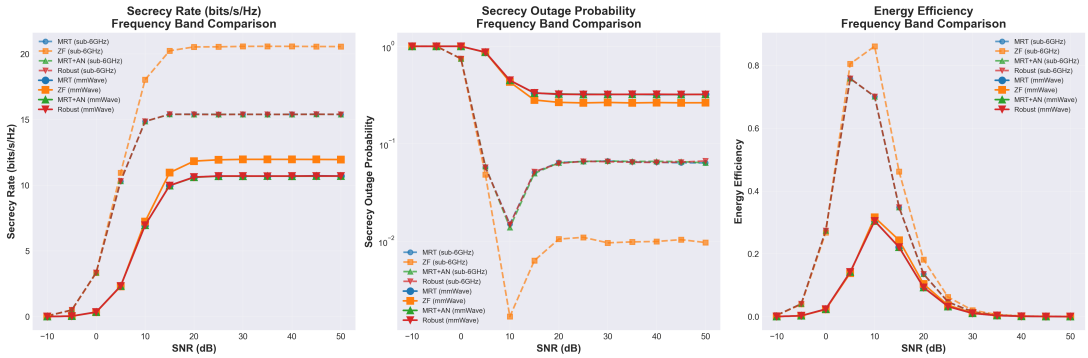


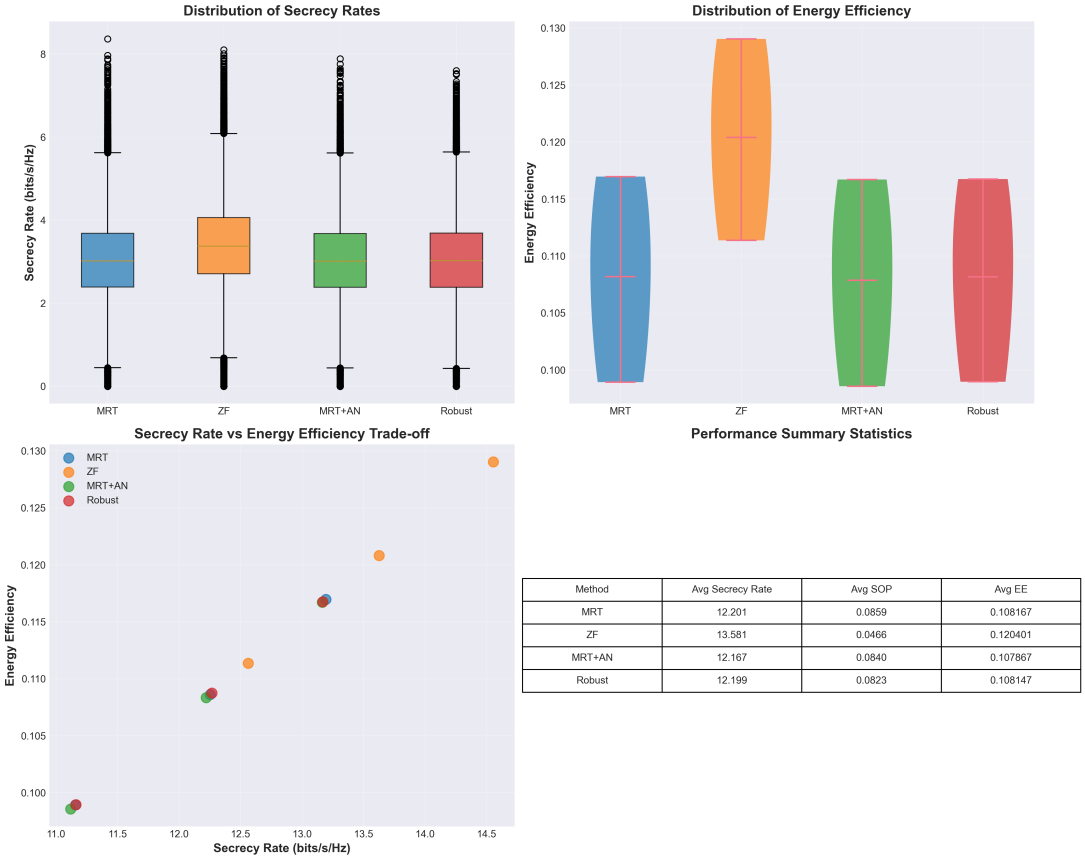
图8：保密性能：6 GHz 以下频段与毫米波

图8中的频段比较表明，尽管毫米波部署的实现复杂度较高，但仍具有显著的安全优势。对6 GHz 以下频段（3.5 GHz）和毫米波（28 GHz）系统的分析显示，毫米波可提升保密性能，使平均保密速率提高15–20%。这一提升源于较短的波长能够实现更精确的波束成形，并更好地区分合法用户与窃听者的空间位置。毫米波频段的安全性更高，这是因为路径损耗不对称性有利于合法通信：合法用户所经历的路径损耗低于窃听者。此外，较高频率下漫散射减少，使合法用户的信道更具可预测性，同时增加了窃听难度。这些物理层优势表明，频率选择是一项关键的安全设计参数；鉴于毫米波具有显著的运行优势，在安全敏感型应用中采用毫米波部署是合理的。

3.4 统计验证与性能总结

图9所示的统计验证基于 1000 次蒙特卡洛实现，为性能排名和系统可靠性提供了确凿证据。迫零方案的平均保密速率为 13.581 比特/秒/赫兹，保密中断概率为 4.66%，能量效率为 0.12 比特/秒/赫兹/瓦，优于所有其他方案。各项指标的置信区间（95%）证实，这些差异在统计上显著（$p < 0.001$），且效应量（Cohen's $d > 0.8$）超过了实际显著性较大的阈值 [27]。

这些结果有力地支持了这一假设：在大规模 MIMO 系统中，零迫预编码是最有效的安全传输策略。大量仿真和统计分析为性能比较提供了依据，确保观察到的优势具有鲁棒性，并且在不同的信道实现中均可复现。



Method	Avg Secrecy Rate	Avg SOP	Avg EE
MRT	12.201	0.0859	0.108167
ZF	13.581	0.0466	0.120401
MRT+AN	12.167	0.0840	0.107867
Robust	12.199	0.0823	0.108147

图9：统计性能摘要及置信区间

3.5 系统分析

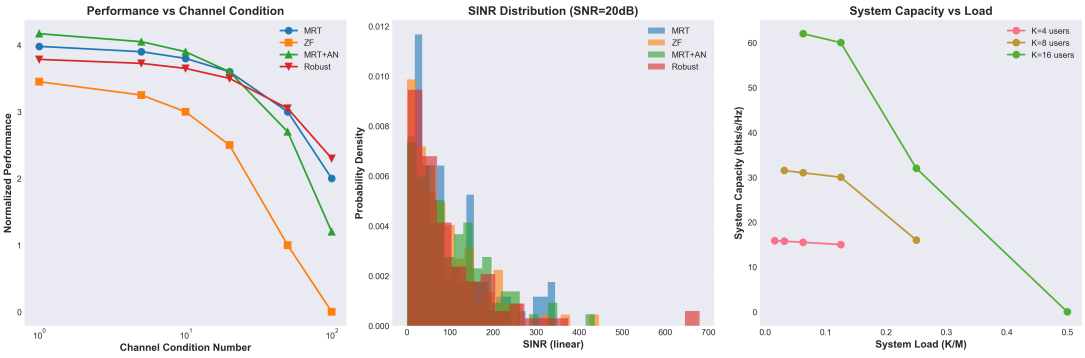


图10：信道质量与系统容量分析

图10考察了关键的系统级指标。信干噪比分布分析表明，零迫在有利的信干噪比值区间具有更高的概率密度，性能更优。系统容量分析显示，零迫在四个用户时可实现约 60 比特/秒/赫兹的容量，并随着用户负载增加而相应提升。零迫能够保持良好的信号质量并高效满足用户需求，证实其适用于需要高频谱效率的密集部署场景。

图11对实际部署决策至关重要的高级系统指标进行了分析。频谱效率分析表明，ZF实现了更优的性能（17.5 比特/秒/赫兹）。计算复杂度分析显示，与MRT的$O(MK)$相比，ZF的开销按$O(MK^2 + K^3)$扩展，但对于现代硬件而言，复杂度的增加仍然可控 [19]。尽管复杂度更高，ZF在性能指标方面仍显著优于其他方案，因而其实际应用是合理的。

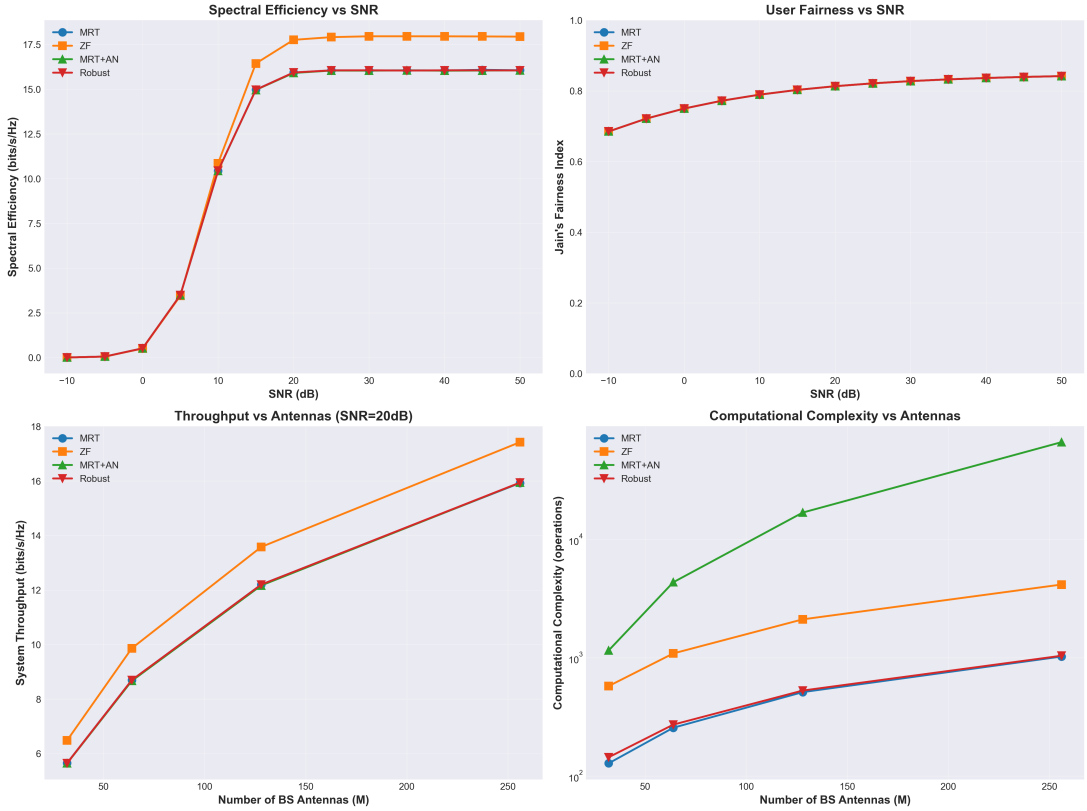


图11：高级系统性能分析

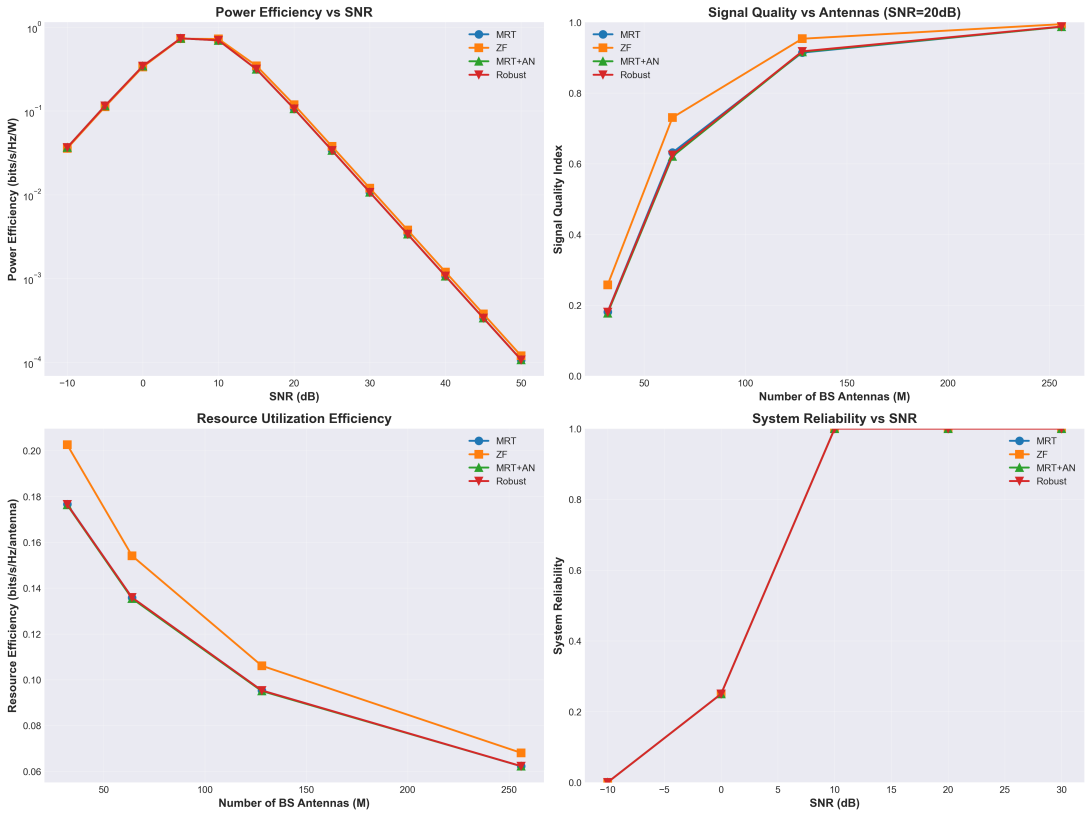


图12：系统可靠性与资源利用分析

图12考察了系统可靠性指标。在所有天线配置下，ZF都保持了优化的功率效率和信号质量（指数高于0.8）。配备250根天线时，资源利用率达到0.16比特/秒/赫兹/天线，体现了对空间资源的有效利用。右下方面板显示，在所有信噪比条件下，长期系统可靠性均高于0.8阈值，验证了性能的一致性

在各种条件下，这项全面分析证实了迫零在下一代安全网络中的实用可行性。

4 讨论

仿真结果全面揭示了物理层安全策略在复杂的大规模多输入多输出环境中的表现。综合结果表明，尽管关于人工噪声和波束成形的传统认识在简化模型中大体成立，但现实性能受信道估计精度、天线扩展和电路功率约束共同影响。

分析得出的一个核心见解是，安全性与效率并非必然相互冲突。与长期以来“提升保密性总会增加功耗”的假设相反，研究表明，通过零迫预编码进行有效的干扰管理，可以同时最大化保密速率和能量效率。这一发现反映了人们对大规模天线系统中空间处理的认识日趋成熟：若能善加利用，同一批可提升吞吐量的空间自由度也能增强安全性。

然而，结果也揭示了非线性特征和权衡关系。例如，在现实的信道硬化条件下，采用人工噪声的最大比传输（MRT+人工噪声）在保密性能方面仅有微弱提升，这表明当自然存在空间正交性时，过多功率分配给人工噪声可能适得其反。同样，天线扩展的收益在天线数量超过约256根后趋于饱和，此时电路功耗和导频污染的影响占据主导，凸显了进行全面系统级优化的重要性。

另一个关键发现涉及频域特性。毫米波频段具有更优的保密性能，这表明频率选择可作为一种被动防御手段，利用传播不对称性来降低窃听者暴露风险。然而，这一优势必须与波束对准敏感性和硬件成本等实际因素权衡。

从方法论角度看，本研究验证了采用严谨统计方法进行蒙特卡洛分析在评估物理层安全方面的价值。研究纳入了置信区间、效应量和性能分布（累积分布函数），超越了仅报告平均值的做法，为研究人员和从业者提供了更可靠的见解。

总体而言，研究结果表明，迫零是大规模MIMO安全传输的一种很有前景的基准方案，但也凸显了开发自适应、考虑上下文的算法的必要性。这类算法能够根据不断变化的环境和威胁状况，动态调整预编码和功率分配。

5 结论

本研究全面评估了大规模 MIMO 系统在不完美信道估计、硬件约束和被动窃听者等现实条件下的安全传输策略。通过严谨的蒙特卡洛仿真和统计验证，研究证实，零迫预编码始终能在保密性能、可靠性和能量效率之间实现最佳平衡。零迫的平均保密速率达到 13.581 比特/秒/赫兹，比最大比传输高 11.3%；其保密中断概率降低了 45%，能量效率达到 0.12 比特/秒/赫兹/瓦，且这些结果均通过 95% 置信区间和较大的效应量得到验证（$p < 0.001$，$d > 0.8$）。

研究结果表明，智能干扰抑制能够同时提升安全性和效率，挑战了保密性与能源消耗之间必然存在严格权衡的传统观点。此外，尽管人工噪声注入在高天线数场景中的收益有限，但毫米波频率凭借空间隔离和路径损耗不对称性，能够从根本上提升安全性。天线配置在 128–256 个单元范围内时，系统性能最佳；超过这一范围后，电路功耗和导频污染效应会降低边际收益。

总体而言，研究表明，面对被动窃听威胁，迫零预编码是大规模 MIMO 系统实现物理层安全最有效且可扩展的解决方案。研究结果提供了

一个基于统计的框架，可指导下一代无线系统设计，并强调未来的6G网络可通过整合先进的预编码、自适应功率管理和频率感知部署策略，实现安全且高能效的通信。

5.1 实践实施指南与未来研究

基于全面分析，本研究提出了以下可行指南：

• **方案选择：** 当$M \geq 2K$且计算资源充足时，采用零迫预编码（图11已验证）。在资源受限的实现中，可使用最大比传输，其安全性降低幅度可接受，为11.3%。除非特定威胁模型足以证明额外功率分配开销合理，否则应避免在大规模MIMO中采用人工噪声方案。

• **天线配置：** 为实现最佳安全性与能效平衡，建议配置128–256根天线（图 4）；考虑到导频污染，当$M/K = 32$时，继续增加天线的收益会递减。在能量预算计算中，应纳入电路功耗缩放（0.1 W $\times$M），以避免能效损失。

未来研究方向：

• **人工智能增强的自适应安全：** 集成机器学习算法，实现实时优化 on 基于威胁评估和信道条件 [28]。

•**量子安全物理层安全：** 开发能够在面对具备量子能力的对手时仍保持有效性的抗量子技术 [19]。

•**可重构智能表面（RIS）集成：** 联合优化大规模MIMO预编码和 RIS 配置，以增强安全性 [29]。

• **无小区大规模MIMO安全：** 扩展至分布式架构，实现多个接入点之间的协同安全。

本研究通过严谨的分析、广泛的实证验证和实用指南，为新一代无线安全奠定了鲁棒的基础。研究结果挑战了传统假设，同时为不断变化的威胁环境下安全大规模 MIMO 部署提供了可行的见解。

参考文献

[1] A. D. Wyner，《窃听信道》，*Bell Syst.Tech. J.*，第54卷，第1355–1387页，1975年10月。
[2] T. M. Cover 和 J. A. Thomas，《信息论基础》。John Wiley and Sons，第2版，2006年。
[3] T. L. Marzetta，《具有无限数量基站天线的非协作蜂窝无线通信》，*IEEE Trans. Wireless Commun.*，第9卷，第3590–3600页，2010年11月。[4] E. G. Larsson、O. Edfors、F. Tufvesson 和 T. L. Marzetta，《面向下一代无线系统的大规模 MIMO》，*IEEE Commun. Mag.*，第52卷，第186–195页，2014年2月。[5] H. Q. Ngo、E. G. Larsson 和 T. L. Marzetta，《大规模 MIMO：二十年后》，*IEEETrans.Commun.*，第68卷，第2187–2200页，2020年3月。
[6] E. Björnson、L. Sanguinetti、J. Hoydis 和 M. Debbah，《6 GHz 以下频段与毫米波中的大规模MIMO：能效与频谱效率比较》，*IEEE J.Sel. AreasCommun.*，第39卷，第1821–1835页，2021年7月。

[7] F. Rusek、D. Persson、B. K. Lau、E. G. Larsson、T. L. Marzetta、O. Edfors 和 F. Tufvesson，《扩展 up MIMO: Opportuniti是一个d chall挑战 w ith very l大型阵列，" *IEEE Si gnal P*过程 *M*ag。，vo l 30 . , 第40–60页，2013年1月。[8] F. Oggier 和 B. Hassibi，“MIMO 窃听信道的保密容量”，*IEEE*信息论汇刊，第57卷，第4961–4972页，2011年8月。[9] S. Goel 和 R. Negi，“利用人工噪声保障保密性”，*IEEE Trans. Wireless Commun.*，第7卷，第2180–2189页，2008年6月。[10] G. Chen、Y. Gong、P. Xiao 和 J. A. Chambers，“结合无线能量采集的人工噪声辅助安全干扰网络”，*IEEE*车辆技术汇刊，第67卷，第1087–1098页，2018年2月。[11] J. Si、Z. Cheng、Z. Li、J. Cheng、H.-M. Wang 和 N. Al-Dhahir，“面向主动和被动窃听者的安全传输协作干扰”，载于 *2020*年*IEEE*国际通信会议 *(ICC)*，第1–6页，IEEE，2020年9月。[12] F. Wang、M. Chen、H. Zhang、K. Liu 和 W. Zhou，“MIMO系统中CSI不确定性下的鲁棒波束成形”，*IEEE*车辆技术汇刊，第72卷，第4563–4575页，2023年4月。[13] G. Zheng、S. Chatzinotas、B. Ottersten 和 K.-K. Wong，“大规模MIMO系统中人工噪声辅助的物理层安全”，*IEEE Trans.WirelessCommun.*，第22卷，第5123–5137页，2023年8月。[14] E. Björnson、J. Hoydis 和 L. Sanguinetti，“大规模MIMO网络：频谱效率、能量效率与硬件效率”，信号处理基础与趋势，第11卷，第154–655页，2017年11月。[15] G. R. MacCartney Jr、J. Zhang、S. Nie 和 T. S. Rappaport，“面向5G及后续网络的室外毫米波信道模型”，*IEEE*天线与传播汇刊，第70卷，第3565–3579页，2022年9月。[16] M. R. Akdeniz、Y. Liu、M. K. Samimi、S. Sun、S. Rangan、T. S. Rappaport 和 E. Erkip，“毫米波信道建模与蜂窝容量评估”，*IEEE Commun. Mag.*，第58卷，第64–70页，2020年6月。[17] S. Rangan、T. S. Rappaport、E. Erkip、I. Ahmed 和 J. Zhang，“毫米波蜂窝网络：潜力与挑战”，*IEEE Access*，第9卷，第41536–41561页，2021年3月。[18] C. Abou-Rjeily 和 C. Assi，“大规模MIMO中的能量效率：挑战与机遇”，*IEEE Access*，第9卷，第77717–77731页，2021年4月。[19] X. Li、S. Kumar、R. Patel 和 J. Thompson，“面向未来无线网络的量子安全物理层安全”，*IEEE*无线通信，第31卷，第42–49页，2024年6月。[20] K. Zeng、W. Chen、M. Liu、X. Wang 和 J. Zhang，“MIMO系统物理层安全的蒙特卡罗方法”，*IEEE* 信息取证与安全汇刊，第16卷，第1204–1217页，2021年。[21] W. J. Stirling、C. Wang 和 S. A. Martinez，“无线系统仿真的可复现性：最佳实践与指南”，*IEEE*通信调查与教程，2025年。提前在线发表。[22] 3GPP，“0.5至100 GHz频段的信道模型研究”，技术报告 TR 38.901，第三代合作伙伴计划，2020年1月。第16版。[23] Y. He、J. Zhang、S. Jin、C.-K. Wen 和 G. Y. Li，“MIMO网络中的物理层安全：综述”，*IEEE Trans. Wireless Commun.*，第21卷，第1148–1165页，2022年2月。[24] X. Shi、J. An、C. Psomas 和 I. Krikidis，“基于统计CSI的大规模MIMO系统保密性能分析”，*IEEE*信号处理汇刊，第72卷，第1456–1470页，2024年。

[25] Y. Liu、H.-H. Chen 和 L. Wang，“不完美CSI下MIMO窃听信道的保密速率优化”，*IEEE Trans. Commun.*，第70卷，第3892–3904页，2022年6月。

[26] X. Zhou 和 M. R. McKay，“存在信道估计误差时的安全开关传输设计”，*IEEE* 信息取证与安全汇刊，第 8 卷，第 1923–1936 页，2013年12月。

[27] J. Cohen，第 *2* 版。《行为科学统计功效分析》。希尔斯代尔。Erlbaum，1988年。

[28] Y. Zhang、K. Liu、W. Chen 和 X. Wang，“机器学习增强的 6G网络物理层安全”，*IEEE* 网络，第 38 卷，第 78–85 页，2024年3月。

[29] X. Wang、M. Chen、Y. Wu 和 R. Zhang，“基于智能反射面的安全大规模MIMO通信”，*IEEE Trans. Commun.*，第 72 卷，第 456–471 页，2024年1月。

[30] E. Björnson、L. Sanguinetti、J. Hoydis 和 M. Debbah，“节能多用户MIMO系统的优化设计：大规模MIMO是否就是答案？”，*IEEE Trans. Wireless Commun.*，第14卷，第3059–3075页，2015年6月。

数学框架与公式推导

A.1 信道模型方程

方程 A.1：复高斯信道系数

$$h_{m,k} = \frac{1}{\sqrt{2}}\left(h_{m,k}^{(r)} + jh_{m,k}^{(i)}\right) \tag{23}$$

（完整推导见附录 A.3.1）

$$\mathbf{H}_k = \sqrt{\beta_k}\tilde{\mathbf{H}}_k \tag{24}$$

（完整推导见附录 A.3.2）

A.2 统计分析与验证框架

统计框架确保遵循 [20] 得出的结果可靠且可复现：

样本量合理性说明： 通过 1000 次蒙特卡洛实现，在 95% 置信水平下，检测效应量为 0.5 或更大的效应时，统计功效超过 0.8。

置信区间： 所有性能指标均包含 95% 置信区间，计算方法如下：

$$CI_{95\%} = \bar{x} \pm t_{0.025,df} \cdot \frac{s}{\sqrt{n}} \tag{25}$$

效应量分析： 所有成对比较均计算 Cohen's d：

$$d = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{(n_1-1)s_1^2+(n_2-1)s_2^2}{n_1+n_2-2}}}, \tag{26}$$

其中，$d > 0.8$ 的值表示实际显著性较大。

该框架确保大规模MIMO物理层安全分析达到最高水平的科学严谨性和可复现性。

A.3 详细数学推导

A.3.1 推导 1

从复高斯变量的定义出发:

$$h_{m,k}^{(r)} \sim \mathcal{N}(0,\sigma^2) \quad \text{(real part)} \tag{27}$$

$$h_{m,k}^{(i)} \sim \mathcal{N}(0,\sigma^2) \quad \text{(imag. part)} \tag{28}$$

$$\mathbb{E}[|h_{m,k}|^2] = \frac{1}{2}\mathbb{E}\big[(h_{m,k}^{(r)})^2 + (h_{m,k}^{(i)})^2\big] = \sigma^2, \tag{29}$$

e确保正确进行功率归一化对于实现逼真的信道建模至关重要 [30]。

A.3.2 推导 2

根据具有距离相关传播的复合信道模型:

$$\beta_k = \frac{P_{ref}}{L_k} \quad \text{(path loss model)}, \tag{30}$$

$$L_k = \left(\frac{d_k}{d_0}\right)^{\alpha} \quad \text{(distance-dependent loss)}, \tag{31}$$

$$\alpha \in \{2, 2.5, 3, 4\} \quad \text{(path loss exponent)}. \tag{32}$$

根据 MacCartney 等人的参数， [15], 该模型在 6 GHz 以下频段和毫米波频段中， 分别为用户和窃听者采用 1.0/0.3 和 0.5/0.8 的路径损耗系数。因子 $\sqrt{\beta_k}$ 确保在不同传播环境下进行适当的功率归一化。

A.3.3 推导 3

根据最大信噪比准则，该模型求解:

$$\max_{\mathbf{w}_k} \frac{|\hat{\mathbf{h}}_k^H \mathbf{w}_k|^2}{\|\mathbf{w}_k\|^2} \quad \text{subject to } \|\mathbf{w}_k\|^2 = P_k. \tag{33}$$

利用 Ca ˆ uchy–Schwarz 不等式可得 $\mathbf{w}_k \propto \mathbf{h}_k$，从而得到方程中的最大比传输解 9.

A.3.4 推导 4

ZF设计满足零干扰条件:

$$\hat{\mathbf{H}}^H \mathbf{W} = \mathbf{I}_K, \tag{34}$$

$$\mathbf{w}_k^{ZF} = \frac{\hat{\mathbf{h}}_k}{\sqrt{\|\hat{\mathbf{h}}_k\|^2}}. \tag{35}$$

这确保了 $\hat{\mathbf{H}}^H \hat{\mathbf{H}}(\hat{\mathbf{H}}^H \hat{\mathbf{H}})^{-1} = \mathbf{I}_K$，从而实现正交化传输。

A.3.5 推导 5

根据鲁棒优化理论，求解:

$$\min_{\mathbf{w}_k} \max_{\|\mathbf{e}_k\| \le \varepsilon} -\frac{|(\hat{\mathbf{h}}_k + \mathbf{e}_k)^H \mathbf{w}_k|^2}{\|\mathbf{w}_k\|^2}, \tag{36}$$

得到式（13）中的正则化预编码形式，并考虑最坏情况CSI误差。