通过智能频谱控制实现多用户隐蔽通信

Yujie Ling，*IEEE*研究生会员，Zan Li，*IEEE*会士，Lei Guan，*IEEE*会员，Zheng Zhang，*IEEE*会员，Dusit Niyato，*IEEE*会士

arXiv:2601.05281v1 [cs.IT] 6 Jan 2026

摘要—**本文研究了在存在窃听者和恶意干扰器的多小区场景中，固定带宽下多用户隐蔽通信的性能。我们提出一种智能频谱控制（ISC）方案，将高精度频谱感知与人工智能辅助的实时决策相结合，为多个合法用户生成时频动态占用模式。该方案能够主动规避外部干扰和系统内同信道冲突，从而提升隐蔽性和可靠性。在此框架下，我们推导出多用户联合检测条件下窃听者的检测错误概率（DEP）和合法用户的可靠传输概率（RTP）的闭式表达式。随后，我们对能够最大化隐蔽速率（CR）的传输功率进行解析优化，并求出在给定隐蔽性和可靠性约束下，可隐蔽且同时接入系统的最大用户数。仿真结果证实，解析曲线与蒙特卡罗曲线高度吻合，并表明与基准方案相比，所提方案能够实现更高的DEP、更大的RTP和更高的多用户容量。**

关键词—**隐蔽速率（CR）、智能频谱控制、检测错误概率（DEP）、多用户隐蔽通信、可靠传输概率（RTP）。**

I. 引言

随着蜂窝网络和物联网（IoT）的快速发展，无线通信已深度融入许多关键应用。与有线链路不同，无线信道天然开放且具有广播特性。无线电信号以非定向方式在空间中传播，使潜在对手能够被动窃听或主动监测合法传输而不被察觉。一旦传输被识别并可能被定位，合法节点仍可能遭受干扰和物理攻击。在此背景下，隐蔽通信已成为一个重要的研究方向 [1], [2]。其主要目标是隐藏通信的存在，使监测者无法辨别，同时仍满足服务要求。

近年来，研究人员在隐蔽通信的建模与分析方面开展了大量工作。文献 [3] 考虑了一个全双工中继系统，并构建了一个联合设计功率控制和中继策略的优化框架。在此基础上，作者推导了最小检测错误概率（DEP）和最大可实现隐蔽速率（CR）的闭式表达式。文献 [4]研究了采用双功能人工噪声（AN）的感知与通信一体化系统。通过联合设计数据波束和人工噪声波束，作者最大化了最坏情况下的隐蔽速率，并展示了人工噪声提升隐蔽性能的潜力。文献 [5] 研究了存在信道不确定性的下行多天线非正交多址接入（NOMA）系统。基于最小检测错误概率和最优检测阈值，作者通过功率分配和天线选择最大化了隐蔽吞吐量。文献 [6] 提出了一种相位扰动开关键控（OOK）调制方案，其中将精心设计的相位偏移叠加到开关键控符号上。合法接收机仍可可靠解码，而监测者无法区分符号分布。 [7] 的作者聚焦于中继辅助物联网场景，并基于最优似然比检测和KL散度约束，开发了一种有限码长隐蔽通信框架。然而，他们中的大多数研究都聚焦于单条链路，通常假设同一时间只有一名合法用户尝试接入信道。

在新兴的多小区多用户系统中，大量基站（BS）和用户终端在强干扰和异步运行条件下共享碎片化频谱资源。在此类环境中，小区间频谱复用和时钟失配会导致严重的同频干扰和邻道干扰。这引出了一个根本问题：在给定隐蔽性和可靠性约束的情况下，多个用户如何才能同时以隐蔽方式接入通信系统，同时避免造成有害的相互干扰？与传统的单链路模型不同，多用户环境中的隐蔽性能和通信质量不仅取决于信道统计特性以及窃听者采用的检测方法，还会受到活跃用户数量、其时频占用模式以及底层调度方案的显著影响。

受上述观察启发，我们提出一种智能频谱控制（ISC）方案，以支持多个用户进行隐蔽接入。在每个传输周期内，该方案利用智能决策模块为所有合法用户生成动态频隙占用模式，并通过改进的频谱感知方法驱动，从而主动避免恶意干扰器和系统内同频冲突。此外，我们分析并推导了窃听者在多时隙联合检测下的检测错误概率（DEP），以及采用所提方案时合法用户的可靠传输概率（RTP）。基于这些解析结果，我们进一步分析并确定了满足隐蔽性和可靠性约束时的最大隐蔽速率（CR）及其对应的最优传输功率，以及能够同时隐蔽接入系统的最大用户数。最后，我们通过仿真结果验证了所提ISC传输方案的有效性。

II. 系统模型

我们考虑如图 1 所示的多小区、多用户通信场景。该网络由多个覆盖区域互不重叠的基站组成，每个基站以固定发射功率 p_b 为其通信小区内的若干合法用户提供服务。所有基站的集合表示为$\mathcal{N}_{\mathcal{B}} = \{\mathrm{BS}_1, \mathrm{BS}_2, \ldots\ldots, \mathrm{BS}_m\}$，其中 m 为该场景中的基站总数。为在多用户共存环境下实现隐蔽通信，所有地面基站均配备均匀线性阵列（ULA）天线，从而能够对用户信号进行灵活的空域控制。我们主要关注下行链路 [8], [9], [10] 上信息传输的隐蔽性和质量。在一个传输周期内，每个合法用户始终与其服务基站保持关联，由该基站向用户传输机密消息。

Yujie Ling、Zan Li、Lei Guan 和 Zheng Zhang 均供职于西安电子科技大学综合业务网络国家重点实验室，地址：中国西安 710071（电子邮箱：yujieling@stu.xidian.edu.cn；zanli@xidian.edu.cn；lguan@xidian.edu.cn；zhangzheng@xidian.edu.cn）。

Dusit Niyato 任职于新加坡南洋理工大学计算与数据科学学院（电子邮箱：dniyato@ntu.edu.sg）。

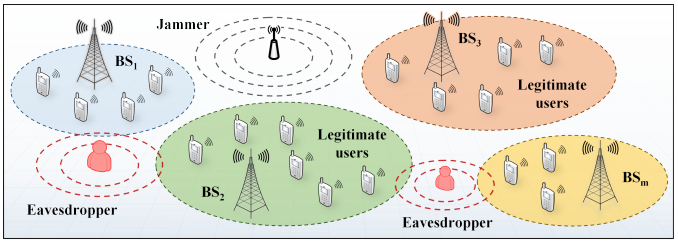


图 1. 多用户隐蔽通信场景示意图。

具体而言，我们假设所有链路均经历相互独立的平坦瑞利衰落，因此相应的信道功率增益服从指数分布。合法用户集合表示为 $\mathcal{N}_{\mathcal{U}} = \{\mathrm{U}_1, \mathrm{U}_2, \ldots\ldots, \mathrm{U}_k\}$，其中$k$ 为参与隐蔽通信的合法用户总数。由于基站可能因所处位置和业务需求不同而采用不同的时钟运行，因此它们彼此不同步，进而导致小区间产生同频干扰。此外，该系统使用的频谱是一种公共共享资源，未知的外部设备也可能占用同一频段，从而引入不受控干扰。该区域内还可能存在一些不友好的干扰器，它们会故意发射干扰信号，进而降低合法链路的质量。

更为重要的是，如图 1 所示，随机分布在网络覆盖范围内的窃听者会使用能量检测器来感知合法用户的传输。它们试图解码机密消息，其行为构成了对整体隐蔽通信性能的主要威胁。在接下来的分析中，我们重点考虑位于最坏情况位置的单个被动窃听者。

III. ISC方案

为协调多个用户之间的隐蔽通信，我们提出一种 ISC辅助传输方案。假设合法用户通过总带宽 $\mathcal{W}$传输数据。该总带宽均匀划分为 q个互不重叠的频隙，构成可用频隙集合 $\mathcal{F} = \{f_1, f_2, \ldots, f_q\}$。在一个传输周期内，通信时间线被划分为$p$ 个离散时隙 $\mathcal{T} = \{t_1, t_2, \ldots, t_p\}$，每个合法用户需要占用连续的 L（$L \le p$）个时隙来传送一个数据块。在每个时隙中，合法用户最多可占用一个频隙进行下行传输。

为提高频谱效率并抑制干扰，我们将每个时隙划分为感知阶段和决策阶段。感知阶段较短，依靠高精度频谱感知技术，例如基于卷积神经网络（CNN）和支持向量机（SVM）的感知方法 [11], , 检测每个频隙的占用状态。在决策阶段，将每个基站视为一个智能体，并通过深度双Q网络（DDQN）进行训练，以生成控制矩阵，引导所有用户进行频隙占用 [12], [13]。在感知阶段获取的频隙占用状态和信道质量指标构成这些智能体的状态输入。借助控制矩阵，基站可以直接检查是否有多个用户占用同一频隙，并将此类冲突分配作为负反馈予以惩罚。良好的信道条件则视为正反馈。基于这些反馈，每个智能体为其服务的用户输出频隙占用动作，并确保每个用户在不同的时隙切换到不同的频隙。所提出方案的结构如图2所示。

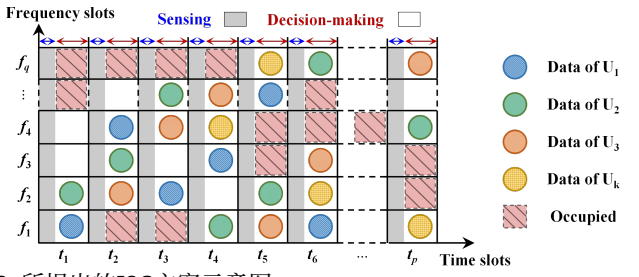


图2. 所提出的ISC方案示意图。

通过应用该方案，可以在感知阶段识别恶意干扰器，以及由不同基站控制的合法用户之间的同频干扰，并在决策阶段避开这些干扰 [14]。同时，每个基站协调其服务用户的频隙占用，以抑制小区内同信道干扰。因此，所提出的方案为所有合法用户提供高质量、低干扰的有效信道。需要注意的是，感知结果可能并不准确。因此，我们将其视为噪声观测，并利用历史观测估计每个频隙的占用状态。此外，由于合法用户可以在时域和频域进行动态控制，所提出的方案也为隐蔽通信创造了有利条件。即使窃听者观察到可疑能量峰值或噪声信号片段，也无法可靠地推断出完整的频隙占用模式。因此，窃听者难以重构完整的机密消息。

IV. 性能分析

本节分别从窃听者的检测错误概率和合法用户的可靠传输概率两个方面，分析系统的隐蔽通信性能。

A. 检测错误概率

如前所述，合法用户可以在全部可用频隙中动态跳频。在这种情况下，若假设窃听者驻留在单个频隙上，则所得检测错误概率只能反映该频隙上是否存在正在进行的传输 [15]。

为了更有效地表征多用户环境下的隐蔽性能，我们考虑窃听者对数据传输进行联合检测。假设窃听者具备宽带观测能力，并能对所有频隙进行能量检测。根据各频隙上的能量独立同分布这一条件，窃听者处的联合检验统计量为

$$T_e = \sum_{j=1}^{q} \sum_{i=1}^{L} \left| y_{e,f_j}[i] \right|^2, \tag{1}$$

其中，$y_{e,\ f_j}[i]$ 表示在频隙 f_j 的第 i次采样上的观测值，并满足

$$y_{e,f_j}[i] = \begin{cases} \sqrt{\frac{mp_b}{qkL}} h_{e,f_j} x[i] + n_0[i], & \mathcal{H}_1, \\ n_0[i], & \mathcal{H}_0, \end{cases} \tag{2}$$

其中，$\mathcal{H}_1$ 表示在恰好k 个频隙（用户）承载合法数据，而其余 $q-k$个频隙包含噪声的假设，$\mathcal{H}_0$ 表示所有 q 个频隙均仅包含噪声的假设。

给定窃听者的检测阈值 γ_e 和噪声功率 σ_0^2，虚警（FA）概率定义为在$\mathcal{H}_0$ 成立时判定存在传输的概率，可由式（3）获得，其中 $Q(\cdot,\ \cdot)$为上正则化不完全伽马函数。

类似地，漏检（MD）概率定义为在 $\mathcal{H}_1$ 为真时宣告不存在传输的概率，可由式（4）给出。令 $\rho = \frac{mp_b}{qkL}$ 并定义 $g = |h_{e,\ f_j}|^2$，其服从参数为 ω_e 的指数分布。基于给定的 g值，随机变量X 服从形状参数为 kL、尺度参数与 $\rho g + \sigma_0^2$相关的伽马分布，而 Y服从形状参数为 $(q-k)L$、尺度参数为 σ_0^2的伽马分布。通过对这两个分布进行卷积，$Z = X + Y$ 的概率密度函数可表示为式（5），其中 ${}_1F_1(\cdot;\ \cdot;\ \cdot)$为库默尔合流超几何函数，$\Gamma(\cdot)$为伽马函数。根据上述表达式，给定 g 时的条件MD概率可由式（6）获得，其中 $(\cdot)^n$ 表示波赫哈默符号，$P(\cdot,\ \cdot)$为下正则化不完全伽马函数。最后，通过对 g的指数分布取平均，可将MD概率写为式（7），且$U(\cdot;\cdot;\cdot)$为特里科米合流超几何函数。因此，窃听者的检测错误概率（DEP）由式（8）给出。

B. 可靠传输概率

系统的通信性能通过可靠传输概率（RTP）来表征，其定义为合法用户成功解码接收信号的概率。采用所提出的方案时，合法用户的接收信号主要受到热噪声的影响。因此，合法用户的信干噪比（SINR）可表示为

$$\mathrm{SINR}_u = \frac{mp_b}{Lk\sigma_0^2}\sum_{i=1}^{L}\sum_{j=1}^{q}\Pr(f_j)\left|h_{u,f_j}\right|^2, \tag{9}$$

其中，$\Pr(f_j)$ 表示频隙 f_j 被占用的概率，$h = |h_{u,f_j}|^2$ 表示基站与用户之间的信道功率增益，其服从参数为 ω_u的指数分布。由于频隙占用概率满足 $\sum_{j=1}^{q}\Pr(f_j) = 1$，因此，当合法用户的译码阈值为 γ_u时，RTP可表示为

$$P_u(\gamma_u) = \Pr(\mathrm{SINR}_u \geq \gamma_u) = \exp\left(-\frac{\gamma_u k\sigma_0^2}{mp_b\omega_u}\right). \tag{10}$$

V. 最优功率与接纳容量

由于我们关注多用户场景下的隐蔽通信，除了系统的隐蔽性能外，另一个关键指标是用户容量。因此，本节首先在可靠性和隐蔽性约束下优化发射功率，以最大化可实现的隐蔽速率。在此最优功率策略的基础上，我们进一步研究系统在既定通信约束下可接纳的合法用户最大数量。

根据第四节推导出的两个性能指标，即窃听者 $P_e(\gamma_e)$ 的检测错误概率和合法用户 $P_u(\gamma_u)$ 的可靠传输概率，我们假设系统满足以下约束：$P_e(\gamma_e) \geq 1-\varepsilon_e$、$P_u(\gamma_u) \geq 1-\varepsilon_u$，其中 ε_e 和 ε_u 是接近于零的较小正数。在此基础上，我们可以给出如下两个定理。

$$P_{\mathrm{FA}}(\gamma_e) = \Pr(T_e > \gamma_e|\mathcal{H}_0) = \Pr\left(\sum_{j=1}^{q}\sum_{i=1}^{L}|n_0[i]|^2 > \gamma_e\right) = Q\left(qL, \frac{\gamma_e}{\sigma_0^2}\right). \tag{3}$$

$$P_{\mathrm{MD}}(\gamma_e) = \Pr(T_e < \gamma_e|\mathcal{H}_1) = \Pr\left(\underbrace{\sum_{j=1}^{k}\sum_{i=1}^{L}\left|\sqrt{\frac{mp_b}{qkL}}h_{e,f_j}x[i] + n_0[i]\right|^2}_{X} + \underbrace{\sum_{j=1}^{q-k}\sum_{i=1}^{L}|n_0[i]|^2}_{Y} < \gamma_e\right). \tag{4}$$

$$\begin{aligned} f_Z(z) &= \int_0^z f_X(x) f_Y(z-x)\,dx = \frac{(\rho g+\sigma_0^2)^{-kL}(\sigma_0^2)^{-(q-k)L}}{\Gamma(kL)\Gamma((q-k)L)}e^{-\frac{z}{\sigma_0^2}}\int_0^1 t^{kL-1}(1-t)^{(q-k)L-1}e^{\frac{\rho g}{\sigma_0^2(\rho g+\sigma_0^2)}tz}z\,dt \\ &= \frac{1}{\Gamma(qL)(\rho g+\sigma_0^2)^{kL}(\sigma_0^2)^{(q-k)L}}z^{qL-1}e^{-\frac{z}{\sigma_0^2}}{}_1F_1\left(kL; qL; \frac{\rho g z}{\sigma_0^2(\rho g+\sigma_0^2)}\right). \end{aligned} \tag{5}$$

$$\begin{aligned} P_{\mathrm{MD}}(\gamma_e|g) &= \frac{1}{\Gamma(qL)(\rho g+\sigma_0^2)^{kL}(\sigma_0^2)^{(q-k)L}}\int_0^{\gamma_e} z^{qL-1}e^{-\frac{z}{\sigma_0^2}}{}_1F_1\left(kL; qL; \frac{\rho g z}{\sigma_0^2(\rho g+\sigma_0^2)}\right)dz \\ &= \frac{1}{\Gamma(qL)(\rho g+\sigma_0^2)^{kL}(\sigma_0^2)^{(q-k)L}}\sum_{n=0}^{+\infty}\frac{(kL)_n}{(qL)_n}\frac{1}{n!}\left(\frac{\rho g}{\sigma_0^2(\rho g+\sigma_0^2)}\right)^n\int_0^{\gamma_e} z^{n+qL-1}e^{-\frac{z}{\sigma_0^2}}dz \\ &= \left(\frac{\sigma_0^2}{\rho g+\sigma_0^2}\right)^{kL}\sum_{n=0}^{+\infty}\frac{(kL)_n}{n!}\left(\frac{\rho g}{\rho g+\sigma_0^2}\right)^n P\left(qL+n, \frac{\gamma_e}{\sigma_0^2}\right). \end{aligned} \tag{6}$$

$$\begin{aligned} P_{\mathrm{MD}}(\gamma_e) &= \int_0^{+\infty}\frac{1}{\omega_e}e^{-\frac{1}{\omega_e}g}\left(\frac{\sigma_0^2}{\rho g+\sigma_0^2}\right)^{kL}\sum_{n=0}^{+\infty}\frac{(kL)_n}{n!}\left(\frac{\rho g}{\rho g+\sigma_0^2}\right)^n P\left(qL+n, \frac{\gamma_e}{\sigma_0^2}\right)dg \\ &= \sum_{n=0}^{\infty}\frac{(kL)_n}{n!}P\left(qL+n, \frac{\gamma_e}{\sigma_0^2}\right)\int_0^{+\infty}\frac{1}{\omega_e}e^{-\frac{1}{\omega_e}g}\left(\frac{\sigma_0^2}{\rho g+\sigma_0^2}\right)^{kL}\left(\frac{\rho g}{\rho g+\sigma_0^2}\right)^n dg \\ &= \frac{\sigma_0^2}{\rho\omega_e}\sum_{n=0}^{\infty}(kL)_n U\left(n+1, 2-kL, \frac{\sigma_0^2}{\rho\omega_e}\right)P\left(qL+n, \frac{\gamma_e}{\sigma_0^2}\right). \end{aligned} \tag{7}$$

$$P_e(\gamma_e) = P_{\mathrm{FA}}(\gamma_e) + P_{\mathrm{MD}}(\gamma_e) = Q\left(qL, \frac{\gamma_e}{\sigma_0^2}\right) + \frac{qkL\sigma_0^2}{mp_b\omega_e}\sum_{n=0}^{\infty}(kL)_n U\left(n+1, 2-kL, \frac{qkL\sigma_0^2}{mp_b\omega_e}\right)P\left(qL+n, \frac{\gamma_e}{\sigma_0^2}\right). \tag{8}$$

定理 *1*：在可靠性和隐蔽性约束下，基站的最优发射功率为

$$p_b{}^* = \sup\{p_b \in [p_{\min}, p_{\max}] : P_e(p_b) \geq 1-\varepsilon_e\}. \quad (11)$$

证明： 为此，我们考虑以下最大化隐蔽速率的功率优化问题:

$$\max_{p_b} \quad R(p_b) = \mathbb{E}_h\left[\log_2(1+\mathrm{SINR}_u)\right] \quad (12a)$$
$$\text{s.t.} \quad P_e(p_b) \geq 1-\varepsilon_e, \quad (12b)$$
$$P_u(p_b) \geq 1-\varepsilon_u, \quad (12c)$$
$$p_{\min} \leq p_b \leq p_{\max}. \quad (12d)$$

由式（12a）可验证， $R(p_b)$ 是 p_b 的单调递增函数。因此，最优解必定位于可行功率区间的上边界。

将式（8）代入式（12b），可得基于隐蔽性约束的功率上界 p_{up}：

$$p_{\mathrm{up}} \triangleq \sup\{p_b \in [p_{\min}, p_{\max}] : P_e(p_b) \geq 1-\varepsilon_e\}. \quad (13)$$

结合式（10）与式（12c），可得基于可靠性约束的功率下界 p_{low}：

$$p_{\mathrm{low}} \triangleq -\frac{\gamma_u k\sigma_0^2}{m\omega_u \ln(1-\varepsilon_u)}. \quad (14)$$

只要满足 $p_{\mathrm{up}} \geq p_{\mathrm{low}}$，该优化问题就具有唯一解，并且可以得到

$$p_b{}^* = \min\{p_{\max}, p_{\mathrm{up}}\} = p_{\mathrm{up}}. \quad (15)$$

上述结论之所以成立，是因为我们通常将功率设置的允许范围 $[p_{\min}, p_{\max}]$ 设定得相对较宽，因此默认 $p_{\max} \geq p_{\mathrm{up}}$。

在此最优功率下，合法用户处的最大平均可达隐蔽速率可表示为

$$R^* = \int_0^{+\infty} \log_2\left(1+\frac{mp_b{}^*}{k\sigma_0^2}h\right)\frac{1}{\omega_u}e^{-\frac{h}{\omega_u}}dh = \frac{1}{\ln 2}\exp\left(\frac{k\sigma_0^2}{m\omega_u p_b{}^*}\right)E_1\left(\frac{k\sigma_0^2}{m\omega_u p_b{}^*}\right), \quad (16)$$

其中，$E_1(\cdot)$ 是指数积分函数。

定理 *2*：在可靠性和隐蔽性约束下，允许接入的合法用户最大数量为

$$k^* = \max\{k \in \{1,\ldots,q\} : p_{\mathrm{up}}(k) \geq p_{\mathrm{low}}(k)\}. \quad (17)$$

证明：为求得系统能够支持的合法用户最大数量，我们建立并考虑如下优化问题:

$$\max \quad k \quad (18a)$$
$$\text{s.t.} \quad P_e(k, p_b^*) \geq 1-\varepsilon_e, \quad (18b)$$
$$P_u(k, p_b^*) \geq 1-\varepsilon_u, \quad (18c)$$
$$q \geq k \geq 1. \quad (18d)$$

通过考察该优化问题的约束结构可以看出，它与式 (12) 具有相同的形式。在定理 *1*中，我们首先固定 k 并优化 p_b，由此根据隐蔽性约束得到功率上界 p_{up}，并根据可靠性约束得到功率下界 p_{low}。仅当可行功率区间非空时，最优发射功率 $p_b{}^*$ 才存在，也就是说，当 $p_{\mathrm{up}} \geq p_{\mathrm{low}}$时才存在。相比之下，式 (18) 固定 $p_b{}^*$，然后反向确定最大用户数 k^*。因此，我们将 $p_{\mathrm{up}}(\cdot)$ 和 $p_{\mathrm{low}}(\cdot)$ 明确视为 k的函数。根据定理 *1*，对于任意给定的 k，一旦满足 $p_{\mathrm{up}}(k) \geq p_{\mathrm{low}}(k)$，约束式 (18b) 和式 (18c) 就会自动满足。这是因为隐蔽性约束规定了 $p_{\mathrm{up}}(k)$，而可靠性约束规定了 $p_{\mathrm{low}}(k)$，它们交集中的任意元素都能同时满足这两个约束。因此，最大用户数可解释为可行功率区间仍然保持非空时最大的 k

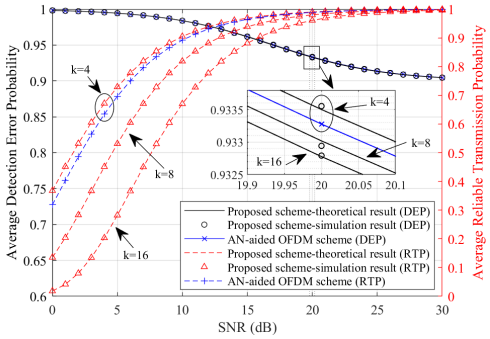


图 3. 不同 SN 下的性能比较 R.

，即，满足 $p_{\mathrm{up}}(k) \geq p_{\mathrm{low}}(k)$ 的最大 k。进一步纳入式 (18d) 后，即可得到能够容纳的最大合法用户数 k^*。

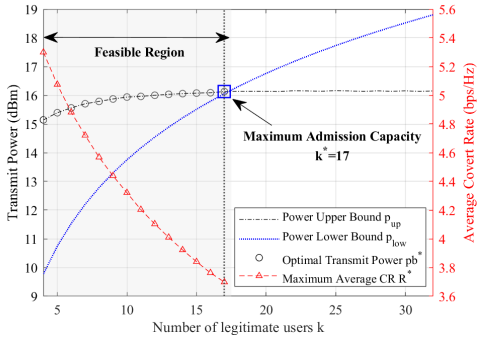
为此，对于具有给定性能要求的实际场景，所得结果可提供最优功率和最大接纳容量。通过利用最优功率适当控制活跃链路的数量，系统既能保持隐蔽性，又能提高多个用户成功传输其私有数据的概率。

VI. 数值结果

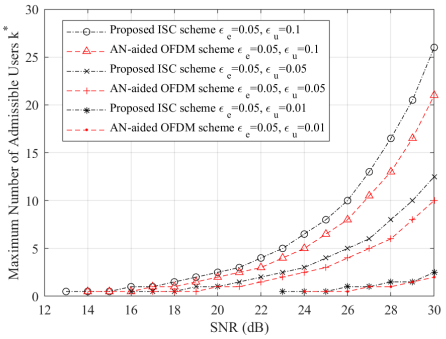
我们通过仿真结果评估所提出的ISC方案在多用户场景下的性能。在仿真中，我们考虑了一个包含4个基站的多小区网络，总带宽为500 MHz。该网络还包括一个主动干扰机和一个被动窃听者。此外，我们设置 $L=8$、$q=64$、$\gamma_e=2$ $\gamma_u=2$、$\omega_u=2$、$\omega_e=1$，并将所提出方案的性能与人工噪声辅助OFDM传输方案 [16]的性能进行比较。

图 3展示了不同方案的DEP和RTP随信噪比变化的情况，其中 $k=4$，8、16。由图 3可见，解析结果与仿真点高度吻合，验证了理论推导的正确性。图 3还表明，对于所有方案，DEP均随信噪比的增加而降低，而RTP则随信噪比增大而提高。DEP的降低是由于窃听者的观测质量得到改善。随着能量观测值增大，窃听者能够更容易地区分主动传输和背景噪声，从而提高系统的可检测性，进而降低其隐蔽性。相比之下，RTP的提高源于合法链路质量的改善，此时期望信号相对于噪声变得更强，使接收信干噪比更有可能超过译码阈值，因此译码错误或中断事件发生得更加不频繁。

从图 3 中还可以发现，当合法用户数量 k 从 4 增加到 16 时，所有方案的 DEP 和 RTP 都会下降。一方面，活跃用户数量增加意味着合法传输信号占用更多频隙，因此频域中的发射能量会增强。这使窃听者更容易识别通信活动，从而降低隐蔽性。另一方面，更多用户必须共享相同的功率和频谱预算，并引发更强的同频干扰和资源竞争。因此，每条合法链路的有效接收信干噪比都会降低。此外，与基准方案相比，所提出的方案能够同时实现更高的 DEP 和更大的 RTP。具体而言，人工噪声辅助 OFDM 方案通过注入人工噪声来降低窃听者的信干噪比。



Fi图4. 不同用户数量下的性能分析 rs.



Fig。5. 不同条件下的最大合法用户数 SNR.

该方案往往会占用一个采用固定子载波集合的连续频带。相比之下，我们提出的 ISC方案会在多个频隙上执行智能频谱控制，并采用动态占用模式，使窃听者更难截获传输的隐私信息。同时，我们的方案利用先进的频谱感知方法来改进频隙占用决策，从而主动避开外部干扰和同信道碰撞，进而提高 RTP。

图4展示了在联合隐蔽性和可靠性约束下，针对不同 k，所提出方案实现的最优发射功率及相应的最大隐蔽速率。可以观察到，随着 k 增大，可行功率区域的上界和下界均向更高值移动。为满足给定的可靠性要求，基站必须提高发射功率，以弥补链路质量下降带来的影响，这使得功率下界 p_{low} 随着k 增加而上升。在隐蔽性约束下，系统因而能够容忍更高的发射功率，同时仍使检测错误概率高于规定水平，这体现为功率上界 p_{up} 随 k增大而上升。图4还表明，只有当功率上界大于下界时，才存在可行的最优发射功率及其对应的最大平均隐蔽速率。在这一可行区域内，隐蔽性和可靠性约束均可得到满足，而最大接纳容量则由功率区域仍非空时最大的k 决定。

图5展示了不同方案下，随着信噪比变化，可接入的合法用户最大数量 k^* 。从图5可以看出，随着信噪比增加，所有方案的最大用户数 k^*都会增长。这是因为系统获得了更多的信干噪比裕量，因此能够允许更多用户同时传输，而不会降低各用户的译码成功概率。图5还表明，随着可靠性约束变得宽松，最大容量 k^* 也会增加。这是因为，当 ε_u 增加时，系统可以牺牲部分译码可靠性，以换取更多用户同时接入。图5还表明，与基准方案相比，所提出的方案能够支持更多合法用户。这是因为所提出的设计将频谱感知与智能调度相结合，能够主动消除同信道冲突和外部干扰源，且不会带来额外的功率开销。因此，该方案能够在并行服务更多合法用户的同时，满足隐蔽性和可靠性约束。

第七节：结论与未来工作

本文研究了多用户场景，并开发了一种 ISC方案，以为多个合法用户提供可靠且隐蔽的私密信息传输。在所提出的 ISC 框架中，我们定义并分析了检测错误概率和可靠传输概率。基于这些指标，我们进一步推导出最优功率和可支持的合法用户最大数量。这些结果为多用户系统中隐蔽接入方案的设计提供了有益指导。未来的工作中，我们计划将协作干扰节点纳入框架，以在保持隐蔽性和可靠性的同时提升容量。

参考文献

[1] Z. Li、Y. Ling、C. Li 等，“基于动态频谱控制的隐蔽空地一体化通信”，IEEE J. Sel. Areas Commun.，2025，提前访问，doi:10.1109/JSAC.2025.3639014。[2] X. Chen、J. An、Z. Xiong 等，“隐蔽通信：全面综述”，IEEE Commun. Surveys Tuts.，第 25 卷，第 2 期，第 1173–1198 页，2023 年。[3] R. Sun、B. Yang、S. Ma 等，“功率控制无线全双工中继系统中的隐蔽速率最大化”，IEEE Trans. Commun.，第 69 卷，第 9 期，第 6198–6212 页，2021 年。[4] R. Tang、L. Yang、L. Lv 等，“感知与通信一体化中双功能人工噪声辅助的鲁棒隐蔽通信”，IEEE Trans. Commun.，第 73 卷，第 2 期，第 1072–1086 页，2025 年。[5] Y. Z hang、W. He、X. Li 等，“信道不确定性下下行非正交多址系统中的隐蔽通信”，IEEE Sensors J.，第 22 卷，第 19 期，第 19101–19112 页，2022 年。[6] X. Ji、R. Zhu、Q. Zhang 等，“通过相位偏转增强开关键控方案中的隐蔽通信”，IEEE Trans. Inf. Forensics Security，第 19 卷，第 9775–9788 页，2024 年。[7] B. Wang、Y. Zhang、R. Xu 等，“面向物联网的中继辅助有限块长隐蔽通信”，IEEE Internet Things J.，第 11 卷，第 24 期，第 39984–39993 页，2024 年。[8] S. Ma、Y. Zhang、H. Li 等，“隐蔽通信的鲁棒波束成形设计”，IEEE Trans. Inf. Forensics Security，第 16 卷，第 3026–3038 页，2021 年。[9] Y. Zhang、W. Ni、Y. Mao 等，“面向隐蔽通信的速率分割多址”，IEEE Wireless Commun. Lett.，第 13 卷，第 6 期，第 1685–1689 页，2024 年。[10] B. Ning、Z. Tian、W. Mei 等，“太赫兹通信中超大规模 MIMO 的波束成形技术”，IEEE Open J. Commun. Soc.，第 4 卷，第 614–658 页，2023 年。[11] X. Li、Y. Zhang、H. Ding 等，“基于分层多智能体深度强化学习的部分观测智能频谱感知与接入”，IEEE Trans. Wireless Commun.，第 23 卷，第 4 期，第 3131–3145 页，2024 年。[12] N. Zhao、Y. Liang、D. Niyato 等，“异构蜂窝网络中用户关联与资源分配的深度强化学习”，IEEE Trans. Wireless Commun.，第 18 卷，第 11 期，第 5141–5152 页，2019 年。[13] H. Zhao、J. Si、Z. Li 等，“规则引导下的多时间尺度跨层抗干扰方案”，IEEE Commun. Lett.，第 29 卷，第 2 期，第 259–263 页，2025 年。[14] X. Li、J. Chen、X. Ling 等，“使用双动作网络的基于深度强化学习的抗干扰算法”，IEEE Trans. Wireless Commun.，第 22 卷，第 7 期，第 4625–4637 页，2023 年。[15] P. Hui、L. Guan、J. Si 等，“面向隐蔽通信的功率-频率联合优化跳频策略”，IEEE Commun. Lett.，第 27 卷，第 2 期，第 452–456 页，2023 年。[16] Y. Jiang、Y. Zou、J. Ouyang 等，“基于人工噪声的基于正交频分复用的认知无线电网络物理层安全保密能效优化”，IEEE Trans. Veh. Technol.，第 67 卷，第 12 期，第 11858–11872 页，2018 年。