



研究与开发

双窃听威胁下 ISAC 系统的保密速率 折中分析与安全预编码设计

焦世恒¹, 钟州¹, 马克明¹, 胡晓言¹, 华浩江²

(1. 信息工程大学信息技术研究所, 河南 郑州 450001;

2. 紫金山实验室, 江苏 南京 211111)

摘要: 研究了存在双窃听威胁的单站通信感知一体化 (integrated sensing and communication, ISAC) 系统。该系统中, 基站与合法用户通信的同时, 接收其反射的回波信号进行感知, 而环境中存在窃听通信信息的通信窃听者 (communication eavesdropper, ComEve) 和监听合法用户回波信号进行被动感知窃听的感知窃听者 (sensing eavesdropper, SenEve)。针对感知窃听问题, 推导了感知保密速率的表达式, 并建立了通信和感知保密速率的加权优化模型, 求得兼顾两者安全性能的系统性能上界。为解决实际 ISAC 系统中的安全性能优化问题, 建立了不同约束条件下最大化感知或通信保密速率的优化问题, 得到了不同需求下的最优安全预编码设计方案。仿真结果表明, 所提预编码方案相较于单一考虑通信或感知安全的预编码方案, 系统整体安全性能平均提升约 30%。

关键词: 通信感知一体化; 双窃听威胁; 安全预编码; 保密速率; 安全性能上界

中图分类号: TN918.91

文献标志码: A

doi: 10.11959/j.issn.1000-0801.2026017

On the secrecy rate trade-off analysis and secure precoding design for ISAC systems under dual eavesdropping threats

Jiao Shiheng¹, Zhong Zhou¹, Ma Keming¹, Hu Xiaoyan¹, Hua Haojiang²

1. Information Technology Institute, Information Engineering University, Zhengzhou 450001, China

2. Purple Mountain Laboratories, Nanjing 211111, China

Abstract: A single-station integrated sensing and communication (ISAC) system subject to dual eavesdropping threats was investigated. In this system, the base station communicates with a legitimate user and simultaneously receives the reflected echo signal from it for sensing. However, there is a communication eavesdropper (ComEve) that wiretaps communication information, and a sensing eavesdropper (SenEve) that passively eavesdrops on the legiti-

收稿日期: 2025-05-29; 修回日期: 2025-06-25

通信作者: 钟州, zhongzhoundsc@gmail.com

基金项目: 国家科技重大专项 (No. 2025ZD1303100); 国家自然科学基金资助项目 (No. 62301608)

Foundation Items: The National Science and Technology Major Project of China (No. 2025ZD1303100), The National Natural Science Foundation of China (No. 62301608)



mate user's echo signal for sensing. Focusing on the sensing eavesdropping issue, the expression of sensing secrecy rate was derived, and a weighted optimization model of communication and sensing secrecy rates was formulated. This model helped to find the upper bound of system performance that balanced the security of both aspects. To enhance the security of practical ISAC systems, the optimization problems were established to maximize sensing or communication secrecy rate under different constraints, yielding optimal secure precoding designs for different requirements. Simulation results indicate that the proposed precoding scheme improves the overall system security performance by approximately 30% on average compared with the schemes that only consider the security of communication or sensing.

Key words: ISAC, dual eavesdropping threat, secure precoding, secrecy rate, secure performance upper bound

0 引言

通信感知一体化 (integrated sensing and communication, ISAC) 系统可以同时实现高质量的通信和感知, 是 6G 移动通信系统的关键技术之一^[1], 受到广泛的关注和研究^[2-4]。同时, 由于 6G 安全、隐私、弹性的设计原则, 保障 ISAC 系统中感知和通信的安全至关重要。

由于无线信号的开放性, ISAC 系统天然存在安全缺陷^[5]。具体而言, 潜在窃听者能够通过 ISAC 信号获取用户信息, 包括通信内容和感知数据。为了应对这些挑战, 本文分别从通信和感知的视角出发, 将 ISAC 系统的安全问题划分为通信安全问题和感知安全问题。

ISAC 系统通信安全问题模型如图 1 所示, 基站 (base station, BS) 发射一体化的 ISAC 信号^[6], 由于电磁波传播的开放性, 潜在通信窃听者 (communication eavesdropper, ComEve) 可以截获传输给合法用户 (legitimate user, LU) 的机密信息, 从而导致信息泄露。此外, 当 ComEve 作为感知目标存在时, 一方面, 为了增强感知性能, 需要将信号能量集中于感知目标; 另一方面, 必须防止 ISAC 信号中的机密信息被感知目标窃听^[7], 这导致了感知性能和通信安全之间的矛盾。

ISAC 系统感知安全问题模型如图 2 所示, 通常认为感知信号是公开的, 这使感知窃听者 (sensing eavesdropper, SenEve) 可以通过接收

BS 发射的感知信号非法感知环境, 进而导致环境中合法感知目标和 LU 的个人隐私泄露^[8]。更进一步, SenEve 可以利用获得的感知信息推断 LU 的行为轨迹、判断其生理特征等, 造成严重的安全威胁。

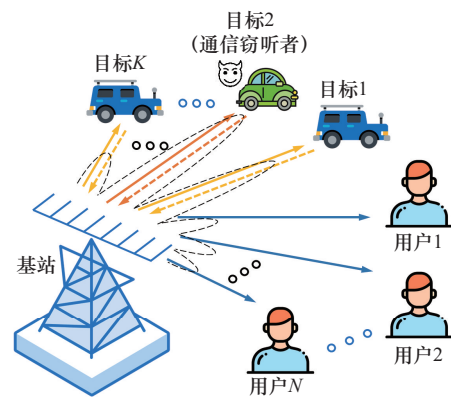


图1 ISAC 系统通信安全问题模型

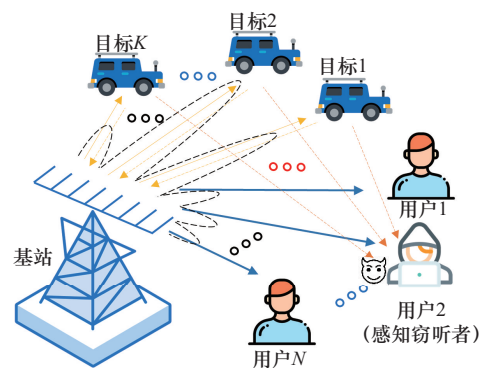


图2 ISAC 系统感知安全问题模型

在通信安全方面, Deligiannis 等^[9]考虑了 ISAC 系统中感知目标作为 ComEve 的情况, 利用人工噪声 (artificial noise, AN) 和波束成形恶化

ComEve 的接收信号质量来保护通信信息。然而,该方法要求 BS 已知完美的信道状态信息 (channel state information, CSI),但在实际场景中一般难以满足该条件。因此, Su 等^[10]考虑在无法获取完美 CSI 的情况下,分别针对已知和未知 ComEve 位置的情况设计最优预编码和 AN 方案,研究表明, ComEve 位置的先验信息影响设计方案的安全性能。在此基础上,其进一步设计了一种感知辅助通信安全的最优预编码和 AN 方案,利用 BS 感知能力获取 ComEve 位置进而辅助安全通信,实现了通信和感知的资源复用^[7]。此外,有部分研究利用波束扫描结合 AN 技术^[11]、定向调制技术^[12]等方法保护 ISAC 系统的通信信息安全。

在感知安全方面,针对潜在的 SenEve 非法获取 LU 的隐私信息 (包括 LU 的位置、速度、心跳脉搏等通过感知能够获取的数据) 这一问题, Zhu 等^[13]针对现有商业 Wi-Fi 信号提出了一种感知窃听攻击模型, SenEve 通过监测 CSI 变化判断房间内 LU 的状态,针对该问题提出了一种信号干扰策略保护 LU 隐私,但该方案会降低合法设备的感知性能。Qiao 等^[14]提出了利用第三方设备转发 ISAC 信号,在干扰感知窃听的同时提升通信性能,但需要配合的第三方设备增加了系统成本。Zou 等^[8]在 ISAC 系统中通过波束成形和 AN 技术保护用户隐私,但 AN 技术可能会消耗额外的功率。Luo 等^[15]通过调整发送端的预编码矩阵,利用与时间相关的加密序列实现物理加密,以保护多用户无线感知系统的隐私安全。此外,还有部分研究利用环境修改^[16-17]等方法保护 ISAC 系统中的用户隐私。

当前针对 ISAC 系统安全问题的研究虽已提出若干方案,但存在一定局限性。部分研究仅聚焦于通信安全,致力于防止通信信息被窃听;另一些研究仅关注感知安全,试图阻止非法感知行为。然而,在 ISAC 系统中,通信与感知紧密耦

合、相互影响,信息在两者之间共享与交互。仅考虑通信安全或感知安全,均无法全面地保障系统的安全性。例如,仅关注通信安全时,感知过程中的信息泄露风险未得到充分防范;仅聚焦感知安全时,通信链路中的信息窃听隐患也未得到有效解决,难以确保 ISAC 系统在面临 ComEve 和 SenEve 的双重窃听威胁时的安全。因此,必须打破传统单一安全防护模式,提出一种能同时兼顾通信和感知安全的解决方案。Ren 等^[18]在存在双窃听威胁的 ISAC 系统中,通过联合设计预编码矩阵和 AN 协方差矩阵,同时保护通信信息和用户隐私。该方案在满足通信用户最小接收信干噪比 (signal to interference plus noise ratio, SINR) SenEve 和 ComEve 接收 SINR 约束条件下,最大化 BS 的检测概率,同时兼顾通信和感知安全。

本文面向存在双窃听威胁的 ISAC 场景,在文献[18]研究的基础上,分析了通信保密速率和感知保密速率之间的折中关系,推导出双窃听威胁下 ISAC 系统安全性能上界。此外,构建了通信和感知性能约束下保密速率优化模型,分别设计了通信保密速率约束下感知保密速率最优和感知保密速率约束下通信保密速率最优的预编码方案。

1 系统模型

针对 6G 场景中 ISAC 系统的安全挑战,本文构建了一个存在双重窃听威胁的单站 ISAC 系统模型,存在双重窃听威胁的单站 ISAC 系统模型如图 3 所示。该模型包括合法用户 LU、配备多天线的 ISAC 基站 BS、通信窃听者 ComEve 以及感知窃听者 SenEve。其中,BS 通过直射链路与 LU 进行通信,同时利用 ISAC 信号中的感知信号感知 LU 的位置。ComEve 试图截获 BS 发送给 LU 的下行通信信息,而 SenEve 利用公开的感知信号非法感知 LU 的位置。系统中,BS 和 SenEve 均配备具有 M 根天线的均匀线阵天线,而 LU 和 ComEve



则配备单天线。鉴于 ISAC 基站进行感知的前提是基站与感知目标之间存在直射链路，且实际环境中存在大量散射体带来非直射的散射链路，因此模型中信道均采用莱斯信道模型进行建模。

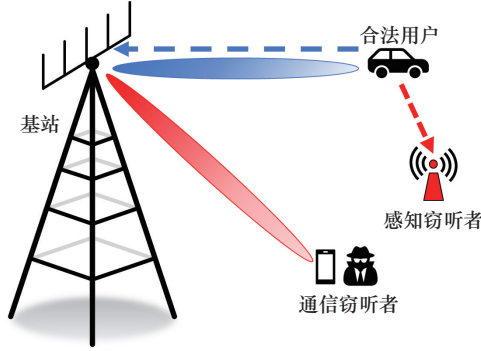


图3 存在双重窃听威胁的单站 ISAC 系统模型

令 BS 的基带发射信号表示为：

$$\mathbf{x}(t) = \mathbf{w}(s_c(t) + s_s(t)) \quad (1)$$

其中， $\mathbf{w} = [w_1, w_2, \dots, w_M]^T$ 为 BS 的预编码矩阵，且 $[\cdot]^T$ 表示矩阵转置； $s_c(t)$ 是发送给 LU 的机密通信信号； $s_s(t)$ 是用于感知 LU 方向、距离等信息的公开感知信号。假设 $s_c(t)$ 和 $s_s(t)$ 具有单位功率，即 $\{ |s_c|^2 \} = \{ |s_s|^2 \} = 1$ ， $\{\cdot\}$ 表示求期望。

1.1 感知接收信号模型

在感知过程中，接收信号的有效部分源自感知目标（即 LU）反射的回波信号，而非感知目标产生的杂波信号被视为噪声。假设 LU 的反射系数为 α ，那么，BS 发射的信号经 LU 反射后抵达 BS 和 SenEve 接收天线的信道模型可描述为：

$$\mathbf{h}_b = \sqrt{\frac{\beta_b}{\beta_b + 1}} \bar{\mathbf{h}}_b + \sqrt{\frac{1}{\beta_b + 1}} \tilde{\mathbf{h}}_b \quad (2)$$

$$\mathbf{h}_{se} = \sqrt{\frac{\beta_{se}}{\beta_{se} + 1}} \bar{\mathbf{h}}_{se} + \sqrt{\frac{1}{\beta_{se} + 1}} \tilde{\mathbf{h}}_{se} \quad (3)$$

其中， β_b 和 β_{se} 是 BS 和 SenEve 回波信道的莱斯因子； $\tilde{\mathbf{h}}_b$ 和 $\tilde{\mathbf{h}}_{se}$ 对应信道的非直射分量，由其他散射体带来的散射信道构成，可建模为服从复高斯分布 $\text{CN} \sim (0, \mathbf{I})$ 的随机变量矩阵， \mathbf{I} 是 $M \times M$ 的单位

矩阵。 $\bar{\mathbf{h}}_b$ 和 $\bar{\mathbf{h}}_{se}$ 对应信道的直射分量，它们由感知目标 LU 反射的回波信号形成，表示为：

$$\bar{\mathbf{h}}_b = \zeta_b \mathbf{a}(\theta_b) \mathbf{a}^H(\theta_b) \quad (4)$$

$$\bar{\mathbf{h}}_{se} = \zeta_{se} \mathbf{a}(\theta_{se}) \mathbf{a}^H(\theta_{se}) \quad (5)$$

其中，将感知目标的散射信息定义为 $\zeta_b = \alpha e^{j(-2\pi f_c \tau_b + \varphi_0)}$ 和 $\zeta_{se} = \alpha e^{j(-2\pi f_c \tau_{se} + \varphi_0)}$ ，其中包含由信号传输时延引起的相位偏移以及感知目标散射带来的幅频响应。其中， τ_b 和 τ_{se} 分别是感知目标反射后到达 BS 和 SenEve 接收天线的信号传播时延； θ_b 和 θ_{se} 分别是 BS 到 LU 方向的信号出射角和从 LU 到 SenEve 方向的信号入射角； φ_0 表示信号从发射端发射时的初始相位。均匀线阵的阵列导向矢量 $\mathbf{a}(\theta)$ 可表示为：

$$\mathbf{a}(\theta) = \left(1, e^{j\frac{2\pi d}{\lambda} \sin \theta}, \dots, e^{j\frac{2\pi d}{\lambda} (M-1) \sin \theta} \right)^T \quad (6)$$

其中， d 是天线阵元间距， $\lambda = c/f_c$ 是信号波长， c 是光速， f_c 是载波频率， M 是天线数量， θ 是信号出射角或入射角。并且，考虑接收信号中的噪声影响，BS 和 SenEve 接收机接收到的等效基带感知信号表示为：

$$\mathbf{r}_b(t) = \mathbf{h}_b \mathbf{x}(t - \tau_b) + \mathbf{z}_b(t) \quad (7)$$

$$\mathbf{r}_{se}(t) = \mathbf{h}_{se} \mathbf{x}(t - \tau_{se}) + \mathbf{z}_{se}(t) \quad (8)$$

其中， $\mathbf{z}_b(t) \sim \text{CN}(0, \sigma_b^2 \mathbf{I})$ 和 $\mathbf{z}_{se}(t) \sim \text{CN}(0, \sigma_{se}^2 \mathbf{I})$ 分别表示 BS 和 SenEve 接收信号中的噪声信号，元素服从复高斯分布。为了进一步处理信号，将接收信号下变频到基带，并根据奈奎斯特采样定理以速率 $f_s = B$ 对信号进行采样，其中， $B/2$ 是基带信号的带宽。得到的离散等效基带感知接收信号表示为：

$$\mathbf{r}_b(n) = \mathbf{h}_b \mathbf{x}(n - k_b) + \mathbf{z}_b(n) \quad (9)$$

$$\mathbf{r}_{se}(n) = \mathbf{h}_{se} \mathbf{x}(n - k_{se}) + \mathbf{z}_{se}(n) \quad (10)$$

其中， $n = 0, 1, \dots, N-1$ 且 $N = BT$ 是时间带宽积， T 是符号持续时间； $k_i \in (0, 1, \dots, N-1)$ ， $i \in \{b, se\}$ ， b 和 se 分别代表 BS 和 SenEve， k_b 和 k_{se} 分别是 BS 和 SenEve 接收信号中的归一化的时延量。最后，

根据接收信号模型定义BS和SenEve感知接收信噪比（signal-to-noise ratio, SNR）分别为：

$$\delta_b^2 = \frac{\|\mathbf{h}_b \mathbf{w}\|^2}{M\sigma_b^2} \quad (11)$$

$$\delta_{se}^2 = \frac{\|\mathbf{h}_{se} \mathbf{w}\|^2}{M\sigma_{se}^2} \quad (12)$$

1.2 通信接收信号模型

在通信方面，BS与LU和ComEve之间的信道模型可表示为：

$$\mathbf{h}_u = \sqrt{\frac{\beta_u}{\beta_u + 1}} \bar{\mathbf{h}}_u + \sqrt{\frac{1}{\beta_u + 1}} \tilde{\mathbf{h}}_u \quad (13)$$

$$\mathbf{h}_{ce} = \sqrt{\frac{\beta_{ce}}{\beta_{ce} + 1}} \bar{\mathbf{h}}_{ce} + \sqrt{\frac{1}{\beta_{ce} + 1}} \tilde{\mathbf{h}}_{ce} \quad (14)$$

其中， β_u 和 β_{ce} 分别代表BS与LU和ComEve之间信道的莱斯因子， $\tilde{\mathbf{h}}_u$ 和 $\tilde{\mathbf{h}}_{ce}$ 是服从复高斯分布 $CN(0, \mathbf{I})$ 的信道非直射分量。信道直射分量 $\bar{\mathbf{h}}_u$ 和 $\bar{\mathbf{h}}_{ce}$ 可表示为：

$$\bar{\mathbf{h}}_u = e^{j(-2\pi f_c \tau_u + \varphi_0)} \mathbf{a}^H(\theta_u) \quad (15)$$

$$\bar{\mathbf{h}}_{ce} = e^{j(-2\pi f_c \tau_{ce} + \varphi_0)} \mathbf{a}^H(\theta_{ce}) \quad (16)$$

其中， τ_u 和 τ_{ce} 分别表示BS到LU和BS到ComEve的信号传播时延。 θ_u 和 θ_{ce} 分别表示BS到LU和ComEve方向的出射角，此时，LU和ComEve接收机接收到的等效基带通信信号表示为：

$$y_u = \mathbf{h}_u \mathbf{x}(t) + z_u(t) \quad (17)$$

$$y_{ce} = \mathbf{h}_{ce} \mathbf{x}(t) + z_{ce}(t) \quad (18)$$

其中， $z_u(t) \sim CN(0, \sigma_u^2)$ 和 $z_{ce}(t) \sim CN(0, \sigma_{ce}^2)$ 分别表示LU接收信号中的服从复高斯分布的噪声信号。最后，根据接收信号模型定义LU和ComEve的通信接收SNR分别为：

$$\delta_u^2 = \frac{\|\mathbf{h}_u \mathbf{w}\|^2}{\sigma_u^2} \quad (19)$$

$$\delta_{ce}^2 = \frac{\|\mathbf{h}_{ce} \mathbf{w}\|^2}{\sigma_{ce}^2} \quad (20)$$

2 最优化预编码方案设计

2.1 感知保密速率上界

在现代通信领域中，感知过程与通信过程存在着相似性，本质均为信息的获取。将BS和SenEve对LU的感知过程类比为通信过程，可构建如下模型：将LU视作信源，通过反射回波这一特定方式，传递自身的位置、大小、速度等感知信息；而BS和SenEve则作为信宿，负责接收LU所发送的位置、大小、速度等信息。依据空间信息论^[19]的相关原理，本文将信号传播时延、信号入射角和散射信息定义为目标感知信息的关键要素。运用互信息的定义，可分别得到BS和SenEve的感知互信息，表示为：

$$I(\mathbf{r}_i; k_i, \theta_i, \zeta_i | \mathbf{x}) = I(\mathbf{r}_i; k_i | \mathbf{x}) + I(\mathbf{r}_i; \theta_i | k_i, \mathbf{x}) + I(\mathbf{r}_i; \zeta_i | k_i, \theta_i, \mathbf{x}) \quad (21)$$

其中， $I(\mathbf{r}_i; k_i, \theta_i, \zeta_i | \mathbf{x})$ ； $i \in \mathbf{b}, \text{se}$ ，表示BS和SenEve在已知发射信号 \mathbf{x} 的情况下接收信号与LU感知信息之间的感知互信息， \mathbf{r}_i 表示接收的感知回波信号，其中 $i \in \mathbf{b}, \text{se}$ ，表示由BS或SenEve接收的感知回波信号。假设LU在BS和SenEve的探测区域内独立且均匀分布，此时归一化的信号传播时延 k_i 、信号入射角度 θ_i 、散射系数 ζ_i 、BS发射信号 \mathbf{x} 之间相互独立。式(21)简化为

$$I(\mathbf{r}_i; k_i, \theta_i, \zeta_i | \mathbf{x}) = I(\mathbf{r}_i; k_i) + I(\mathbf{r}_i; \theta_i) + I(\mathbf{r}_i; \zeta_i) \quad (22)$$

在进行感知前，由于缺乏对探测区域内感知目标的任何先验信息，故假设感知目标在探测区域内遵循均匀分布规律。归一化时延和角度的先验概率密度函数（probability density function, PDF）由下式给出：

$$p(k_i) = \frac{1}{N}, i = \mathbf{b}, \text{se} \quad (23)$$

$$p(\theta_i) = \frac{1}{\Theta}, i = \mathbf{b}, \text{se} \quad (24)$$

其中， Θ 表示角度探测范围。由式(4)和式(5)可知，当载波频率较高时，时延的微小变化将导



致相位产生显著变化。此外，由目标雷达散射截面引起的幅频响应通常表现为非恒定复数特性。因此，将散射系数 ξ_i 建模为服从复高斯分布的复数。考虑 \mathbf{z}_b 和 \mathbf{z}_{se} 为服从独立同分布的复高斯白噪声矩阵，则 \mathbf{z}_b 和 \mathbf{z}_{se} 的先验 PDF 表达式为：

$$p(\mathbf{z}_i) = \prod_{m=1}^M \frac{1}{\pi\sigma_i^2} \exp\left\{-\frac{\|z_i(n)\|^2}{\sigma_i^2}\right\} = \left(\frac{1}{\pi\sigma_i^2}\right)^M \exp\left\{-\frac{1}{\sigma_i^2} \sum_{m=1}^M \|z_i(n)\|^2\right\}, i = b, se \quad (25)$$

其中， $\prod(\cdot)$ 为累乘运算， σ_b 表示 BS 处的接收噪声， σ_{se} 表示 SenEve 处的接收噪声。根据文献[19-21]中关于雷达系统的感知互信息的定义，感知互信息中的距离互信息和方向互信息可以表示为：

$$I(\mathbf{r}_i; k_i) = h(k_i) - h(k_i|\mathbf{r}_i) = \ln(N) - E_{r_i} \left[-\int_0^{N-1} p(k_i|\mathbf{r}_i) \ln(p(k_i|\mathbf{r}_i)) dk_i \right] \quad (26)$$

$$I(\mathbf{r}_i; \theta_i) = h(\theta_i) - h(\theta_i|\mathbf{r}_i) = \ln(\Theta) - E_{r_i} \left[-\int_{-\theta/2}^{\theta/2} p(\theta_i|\mathbf{r}_i) \ln(p(\theta_i|\mathbf{r}_i)) d\theta_i \right] \quad (27)$$

上述距离互信息和方向互信息的表达式可通过近似的方法获得闭式解，具体闭式解形式参考附录 A，详细推导过程参考文献[19]。此外，当散射系数服从复高斯分布时，感知互信息中的散射互信息表示为：

$$I(\mathbf{r}_i; \xi_i) = h(\mathbf{r}_i) - h(\mathbf{r}_i|\xi_i) = \ln\left(\left|\mathbf{h}_i \mathbf{w} \mathbf{w}^H \mathbf{h}_i^H + \sigma_i^2 \mathbf{I}\right|\right) - \ln\left(\left|\sigma_i^2 \mathbf{I}\right|\right) = \ln(1 + M\delta_i^2) \quad (28)$$

根据文献[19]中关于熵误差的定义，在进行感知参数估计时的熵误差可表示为：

$$\sigma_{EE}^2 = \frac{2^{2h(g_i|\mathbf{r}_i)}}{2\pi e}, g \in k, \theta; i \in b, se \quad (29)$$

其中， $h(g_i|\mathbf{r}_i)$ 表示系统在已知接收信号 \mathbf{r}_i 的情况下关于感知参数 g_i 的不确定度，值越大代表系统性能越差，感知精度越低； $i \in b, se$ ，表示对应

参数是在 BS 和 SenEve 处获得/处理的。然后，根据上述关于感知互信息的结论，可以推导出熵误差与感知互信息之间的关系式，表示为：

$$\sigma_{EE}^2 = \frac{1}{2\pi e} \frac{2^{2h(g_i)}}{2^{2I(g_i|\mathbf{r}_i)}}, g \in k, \theta, i \in b, se \quad (30)$$

其中， $i \in b, se$ ，表示对应参数是在 BS 和 SenEve 处获得/处理的。在无线通信领域，借鉴通信保密速率的相关概念，定义感知保密速率为合法方与窃听方所获感知的互信息之差。鉴于感知参数的相互独立性，每个参数可被视为独立信源。据此，将感知保密速率分为距离、角度和散射 3 类，以评估不同感知信息的保密性，可表示为：

$$SR_g^r = I(\mathbf{r}_b; g_b) - I(\mathbf{r}_{se}; g_{se}), g \in k, \theta, \xi \quad (31)$$

其中， SR_g^r 是感知参数 $g \in k, \theta, \xi$ 分别取不同的参数时对应的感知保密速率。鉴于保密容量是保密速率可达到的理论上限，对此构建了一个优化问题，旨在最大化 ISAC 系统的感知保密速率，以此来表征感知保密容量。

$$CS_g^r = \max_{\mathbf{w}} [SR_g^r] \quad (32)$$

s. t. C1: $\text{tr}(\mathbf{w}^H \mathbf{w}) \leq P_0, \text{rank}(\mathbf{w} \mathbf{w}^H) = 1$

其中， CS_g^r 表示不同感知参数 g 对应的感知保密容量，约束 C1 表示 BS 的发射功率约束和预编码矩阵的秩 1 约束， P_0 是 ISAC 系统的最大发射功率。通过求解该问题可获得 ISAC 系统中不同感知参数的感知保密容量和感知保密速率最大的预编码矩阵设计。

2.2 感知保密速率上界

根据香农信息论，通信互信息可表示为接收信号与发射通信信号之间的互信息，在高斯信号下的闭式解表示为：

$$I(s_c; y_u) = \text{lb}\left(1 + \delta_u^2\right) \quad (33)$$

$$I(s_c; y_{ce}) = \text{lb}\left(1 + \delta_{ce}^2\right) \quad (34)$$

通信保密速率定义为合法用户接收通信互信

息与窃听方接收互信息之差^[10], 具体表达式为:

$$SR^c = I(s_c; y_u) - I(s_c; y_{ce}) \quad (35)$$

通信保密容量作为通信保密速率的可达上界, 可通过构建 ISAC 系统中最大化通信保密速率的优化问题来表征。

$$\begin{aligned} CS^c &= \max_w [SR^c] \\ \text{s. t. C1: } &\text{tr}(\mathbf{w}\mathbf{w}^H) \leq P_0, \text{rank}(\mathbf{w}\mathbf{w}^H) = 1 \end{aligned} \quad (36)$$

其中, CS^c 表示通信保密容量, 求解该问题可获得 ISAC 系统中通信保密速率最大的预编码矩阵。

2.3 通感安全性能折中

在 ISAC 系统中, 由于存在双窃听威胁, 需要同时确保通信和感知信息的安全性。为了设计出安全性能最优的预编码矩阵, 本文构建了以下优化问题:

$$\begin{aligned} \max_w & [SR_k^r, SR_\theta^r, SR_\zeta^r, SR^c] \\ \text{s. t. C1: } &\text{tr}(\mathbf{w}\mathbf{w}^H) \leq P_0, \text{rank}(\mathbf{w}\mathbf{w}^H) = 1 \end{aligned} \quad (37)$$

显然, 式 (37) 所示的优化问题是一个多目标优化问题。在系统条件确定的情况下, SR_k^r 、 SR_θ^r 、 SR_ζ^r 和 SR^c 是关于预编码矩阵 \mathbf{w} 的函数。通常, 多目标优化问题不存在一个解能够同时最大化所有目标函数, 而是存在一组解, 这些解在各个目标函数之间达到了某种平衡, 这组解被称为 Pareto 最优解集。为了获得 Pareto 最优解集, 引入权重因子 v_k^r , v_θ^r , v_ζ^r 和 v^c 分别表示距离、方向、散射保密速率和通信保密速率在整个系统安全性能中的权重, 且满足 $v_k^r + v_\theta^r + v_\zeta^r + v^c = 1$ 。因此, 优化问题式 (37) 可以进一步表示为:

$$\begin{aligned} \max_w & [v_k^r SR_k^r + v_\theta^r SR_\theta^r + v_\zeta^r SR_\zeta^r + v^c SR^c] \\ \text{s. t. C1: } &\text{tr}(\mathbf{w}\mathbf{w}^H) \leq P_0, \text{rank}(\mathbf{w}\mathbf{w}^H) = 1 \end{aligned} \quad (38)$$

这里, 采用 4 个权重因子分别表示距离、方向、散射保密速率和通信保密速率的权重。原因在于, 在感知参数估计中, 每个参数可以等效为一个独立的信源, 参数之间相互独立。从信息论的角度来看, 它们与通信信源等价, 因此需要独立

分配权重因子以确保公平性。通过求解不同权重组合下的问题式 (38), 可以获得不同的 Pareto 最优解。这些解构成了给定 ISAC 系统参数下的最优安全性能边界, 并且反映了 ISAC 系统中通信安全和感知安全之间的权衡关系。

在实际应用中, 采用层次分析法 (analytic hierarchy process, AHP) 进行权重分配。首先, 以 ISAC 系统整体安全性能优化为目标层, 距离、方向、散射和通信保密速率为准则层, 方案层为预编码矩阵设计; 然后, 根据专家意见对准则层各指标重要程度进行两两比较, 综合系统设计需求构建判断矩阵, 采用 1~9 标度法确定矩阵元素值; 随后, 利用特征值法计算判断矩阵的最大特征值和对应的特征向量, 经过归一化处理得到权重向量; 最后, 计算一致性指标 (consistency index, CI) 和一致性比率 (consistency ratio, CR), 若 CR 小于或等于 0.1, 则认为判断矩阵的一致性是可接受的, 否则需要重新调整判断矩阵, 直至满足一致性要求。通过 AHP 获得给定 ISAC 系统的设计目标和性能要求下的权重分配结果, 使系统在通信与感知保密性能之间达到预期的平衡。

2.4 实际系统中安全最优预编码设计

在实际的 ISAC 系统中, 具体的性能指标通常是关注的重点。在提升系统安全性能的同时, 确保正常的通信和感知功能不受影响是至关重要的。为了设计出性能指标约束下的最优预编码矩阵, 本文构建了两种优化问题, 分别是感知保密速率最大化问题和通信保密速率最大化问题。

$$\begin{aligned} \max_w & [SR_\zeta^r] \\ \text{s. t. C1: } &\text{tr}(\mathbf{w}\mathbf{w}^H) \leq P_0, \text{rank}(\mathbf{w}\mathbf{w}^H) = 1 \\ &\text{C2: } SR^c \geq \Gamma^c \\ &\text{C3: } SR_g^r \geq \Gamma_g^r, \forall g \neq \zeta, g = k, \theta, \zeta \\ &\text{C4: } I(s_c; y_u) \geq \Upsilon^c \\ &\text{C5: } \sigma_{EE}^2(g_b) \leq \Upsilon_g^r, \forall g = k, \theta, \zeta \end{aligned} \quad (39)$$



$$\begin{aligned}
& \max_{\mathbf{w}} [\text{SR}^c] \\
\text{s. t. C1: } & \text{tr}(\mathbf{w}\mathbf{w}^H) \leq P_0, \text{rank}(\mathbf{w}\mathbf{w}^H) = 1 \\
& \text{C2: } \text{SR}_g^r \geq \Gamma_g^r, \forall g = k, \theta, \zeta \\
& \text{C3: } I(s_c; y_u) \geq \gamma^c \\
& \text{C4: } \sigma_{\text{EE}}^2(g_b) \leq \gamma_g^r, \forall g = k, \theta, \zeta
\end{aligned} \quad (40)$$

其中, SR_ζ^r , $\forall \zeta = k, \theta, \zeta$ 表示优化目标分别是距离、方向、散射保密速率的情况; 式 (39) C2 约束表示通信保密速率约束, 要求通信保密速率必须大于最小允许值 Γ^c ; 式 (39) C3 和式 (40) C2 约束表示不同感知参数对应的感知保密速率约束, 要求感知保密速率必须大于最小允许值 Γ_g^r ; 式 (39) C4 和式 (40) C3 约束表示通信速率约束, 要求合法用户的下行通信速率必须大于阈值 γ^c ; 式 (39) C5 和式 (40) C4 约束表示感知精度约束, 要求合法感知接收机的参数估计精度必须小于阈值 γ_g^r , $g = k, \theta, \zeta$ 表示待估计的参数。

经分析, 目标函数 SR^c 和 SR_ζ^r 呈非凸非线性特征; 式 (39) 和式 (40) C1 约束中 $\text{tr}(\mathbf{w}\mathbf{w}^H) \leq P_0$ 为凸二次约束, 而 $\text{rank}(\mathbf{w}\mathbf{w}^H) = 1$ 为非凸矩阵秩约束; 式 (39) C2~C5 和式 (40) C2~C4 约束亦为复杂的非凸非线性约束。鉴于此, 显然难以通过常规凸优化算法进行求解, 故选用 MATLAB 的 `fmincon` 非线性优化求解器求解问题。尽管 `fmincon` 能高效地处理非线性优化问题, 但易陷入局部最优。为提升求解质量, 采用均匀分布初始点策略以逼近全局最优。针对 `fmincon` 不支持复数变量的局限, 将波束成形向量 \mathbf{w} 转换为:

$$\mathbf{w} = \mathbf{u} + \mathbf{v}i \quad (41)$$

其中, \mathbf{u} 和 \mathbf{v} 分别为 \mathbf{w} 的实部和虚部。因为 \mathbf{w} 的取值需满足式 (39) 和式 (40) 的 C1 约束, 表示其取值范围为半径为 P_0 的 M 维球体。为实现全局优化, 首先生成 L 组均匀分布于该球体内的 \mathbf{u} 和 \mathbf{v} 初始值, 将其输入 `fmincon` 进行多轮求解, 得

到 L 个局部最优解。最终, 选取使目标函数最优的解作为全局最优解输出。均匀初值内点法如算法 1 所示。

算法 1 均匀初值内点法

- (1) 输入 $M, P_0, L, f(\mathbf{w})$
- (2) 初始化循环次数 $i = 0$;
- (3) 循环;
- (4) 生成大小为 $M \times 1$ 的标准正态分布矩阵 $[\mathbf{u}^{(i)}, \mathbf{v}^{(i)}]$;
- (5) 计算模长 $\kappa^{(i)} = \sqrt{(\mathbf{u}^{(i)})^H \mathbf{u}^{(i)} + (\mathbf{v}^{(i)})^H \mathbf{v}^{(i)}}$, 如果 $\kappa^{(i)} = 0$, 则重新生成矩阵 $[\mathbf{u}^{(i)}, \mathbf{v}^{(i)}]$;
- (6) 归一化方向向量 $\mathbf{u}_0^{(i)} = \mathbf{u}^{(i)} / \kappa^{(i)}$, $\mathbf{v}_0^{(i)} = \mathbf{v}^{(i)} / \kappa^{(i)}$, 生成均匀分布的随机数 $\eta^{(i)}$;
- (7) 生成初始预编码矩阵 $\mathbf{w}_0^{(i)} = \sqrt{0.5 \cdot (P_0 \eta^{(i)})^{1/M}} \cdot (\mathbf{u}_0^{(i)} + \mathbf{v}_0^{(i)}i)$;
- (8) 调用 `fmincon` 求解器以初值 $\mathbf{w}_0^{(i)}$ 求解优化函数 $[\mathbf{w}^{(i)}, f(\mathbf{w}^{(i)})] = \text{fmincon}(\mathbf{w}_0^{(i)}, f(\mathbf{w}))$;
- (9) 直到 $i = L$;
- (10) 寻找 L 次循环中目标函数最小的解 $[\mathbf{w}, f(\mathbf{w})] = \min\{f(\mathbf{w}^{(1)}), f(\mathbf{w}^{(2)}), \dots, f(\mathbf{w}^{(L)})\}$;
- (11) 输出 $[\mathbf{w}, f(\mathbf{w})]$

采用上述算法能够获得全局次优解, 当 L 取值较大时, 可近似认为获得了全局最优解。算法 1 在结构上可分为初始点生成和优化求解两个部分。在初始点生成阶段, 每次生成初始点须生成两个 $M \times 1$ 的标准正态分布向量 (\mathbf{u}, \mathbf{v}) , 进行归一化并计算半径, 其时间复杂度为 $O(M)$ 。在优化求解阶段, 每次调用 `fmincon` 函数的时间复杂度取决于内点法的迭代次数及每步迭代的运算量。内点法每步迭代的复杂度约为 $O(M^3)$, 单次优化的复杂度约为 $O(M^3 \cdot T)$, 其中, T 为平均迭代次

数。整体而言，总时间复杂度为初始点生成和优化求解两部分复杂度之和，即 $O\left(L \cdot \left(M + M^3 \cdot T\right)\right)$ 。

3 仿真分析

本文通过数值仿真验证所提的兼顾通信安全与感知安全的 ISAC 系统设计的有效性。依据中国通信标准化协会向国家标准信息公共服务平台提交的行业标准《5G 数字蜂窝移动通信网 6 GHz 以下频段基站设备技术要求（第一阶段）》^[22]中 1-C 型 5G 基站本地覆盖技术指标，选取测量信道 G-FR1-A2-6 作为噪声功率参考，载波频段为 n79，带宽为 100 MHz。 R_{bu} 表示 BS 到 LU 之间的直线距离， R_{use} 表示 LU 到 SenEve 之间的直线距离， R_{bce} 表示 BS 到 ConEve 之间的直线距离。仿真参数见表 1，除非另有说明，否则所有仿真均基于此参数配置进行。

表 1 仿真参数

参数	值	参数	值
M	8	P_0	24 dBm
f_c	3.5 GHz	d	0.5λ
$B/2$	100 MHz	$\sigma_b^2, \sigma_u^2, \sigma_{se}^2, \sigma_{ce}^2$	-64.1 dBm
R_{bu}, R_{use}, R_{bce}	50 m	$\theta_u, \theta_{se}, \theta_{ce}$	0°
N	256	θ	π
γ^c	3 bit/符号	$\gamma_k^s, \gamma_\theta^s, \gamma_\zeta^s$	0.01
Γ^c	1 bit/符号	$\Gamma_k^s, \Gamma_\theta^s, \Gamma_\zeta^s$	1 bit/符号

为揭示接收信噪比与通信、距离、方向、散射互信息之间的内在联系，通过数值计算仿真得到互信息随信噪比变化的曲线，互信息随接收信噪比变化曲线如图 4 所示（数据来源于 MATLAB 仿真结果）。从图 4 可见，通信、距离、方向、散射互信息均随接收信噪比的提升而呈上升趋势。根本原因在于接收信号中有效信号功率的增强，使接收信号与信源的条件熵相应减小，而信源本身的熵保持稳定，进而推动互信息上升。

进一步分析发现，通信互信息和散射互信息具有相同增长趋势，但拐点存在差异；距离互信

息和方向互信息增长趋势一致，拐点却不尽相同。究其根源，通信信息与散射信息的信源遵循高斯分布，而距离信息与方向信息的信源呈均匀分布。此外，通信信息和散射信息与接收信号之间呈线性关系，距离信息与方向信息与接收信号之间呈指数关系。正是信源分布的差异以及与接收信号关系的不同，导致了它们增长趋势的区别。拐点的差异则归因于同一类型分布中概率密度函数的不一致。最终，各互信息基本处于相同数量级，这表明各个信源之间相互独立，因此在进行权重分配时应给予同等重视。

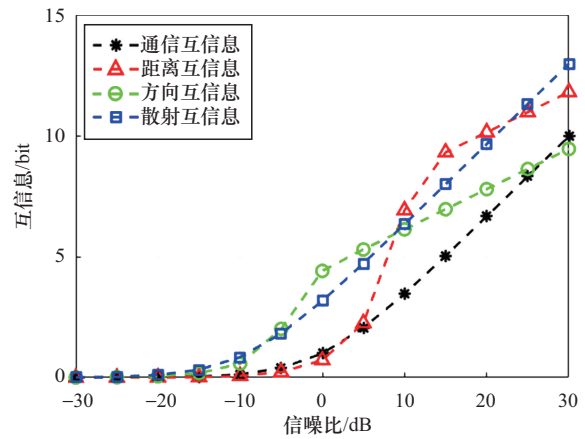


图 4 互信息随接收信噪比变化曲线

为探究 ISAC 系统的安全性能极限，在忽略通信与感知性能约束的条件下，分别求解问题式 (32) 和式 (36)，得到各类信息的最大保密速率。仿真实验结果表明，不同信息的最大保密速率与发射功率正相关，ISAC 系统中保密速率随发射功率变化曲线如图 5 所示。观察发现，通信保密速率最大化时，感知保密速率几乎为 0，反之亦然。这表明单独针对通信或感知设计安全方案，无法保障系统的整体安全，须兼顾两者的安全需求。

进一步分析图 5 (b) ~ (d)，当某一感知保密速率达到最大值时，其他感知保密速率并非为 0，但相较于其对应的最大保密速率，仍存在较

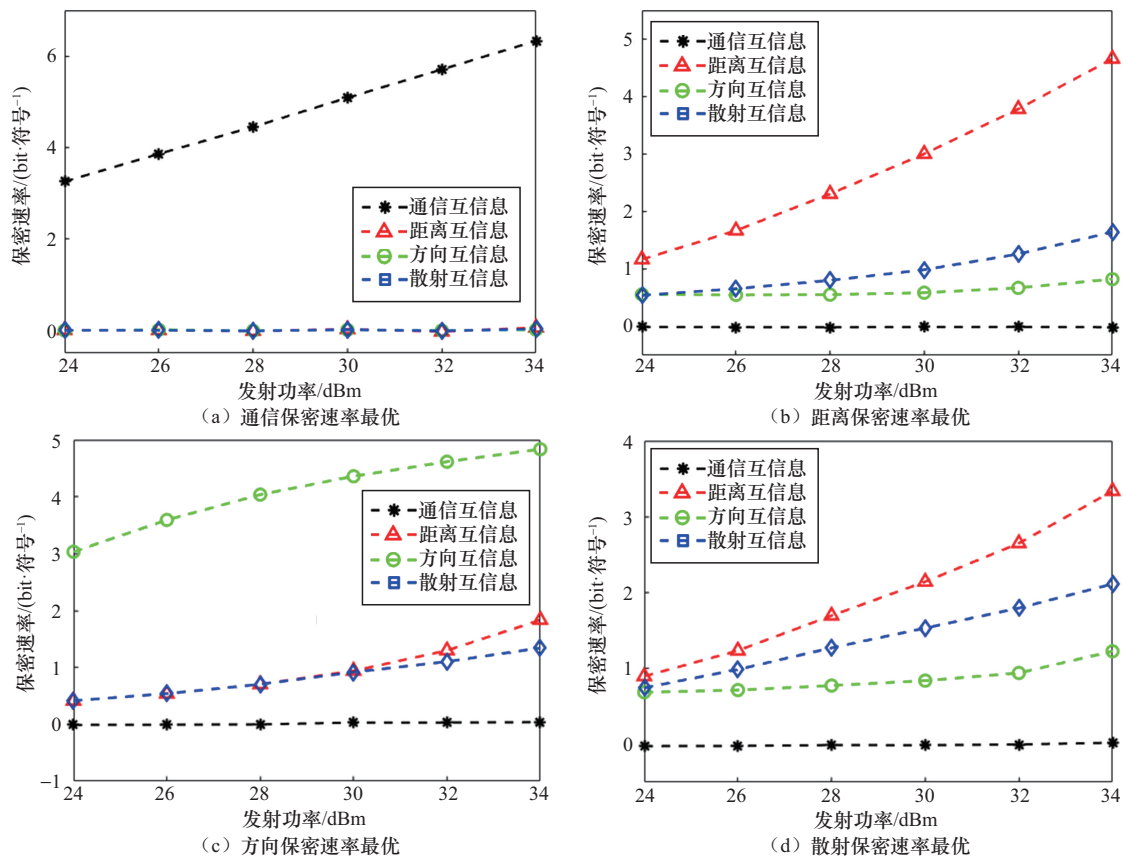


图5 ISAC系统中保密速率随发射功率变化曲线

大差距。原因在于不同感知信息均从同一回波信号中提取，因此，某一感知信息保密速率的提升会在一定程度上带动其他感知信息保密速率的提升；然而，由于各类感知信息相互独立，它们无法同时实现保密速率的最大化。综上，仿真实验证实单纯考虑通信安全或感知安全无法确保系统的整体安全，且通信与感知、不同感知信息间均存在安全性能权衡。因此，分析ISAC系统中通信和感知的安全性能权衡关系十分必要。

为确定ISAC系统通信与感知安全性能折中关系，在不同权重因子下求解问题式(38)，得到通信保密速率与感知保密速率的性能折中曲线，ISAC系统中通信和感知保密速率性能折中关系如图6所示。图6(a)~(c)分别展示了不同感知信息与通信之间的安全性能折中关系。其中，图6(a)展示了当 $v_{\theta}^r = v_{\xi}^r = 0$ 时，令 $v_{\theta}^r = v_{\xi}^r = 0$

并从0到1等间隔取值，求解问题式(38)得到最优预编码矩阵 \mathbf{w} 及相应保密速率之间关系曲线，图6(b)和图6(c)同理。结果表明，通信保密速率与感知保密速率呈此消彼长关系，但不同感知信息(距离、方向、散射)保密速率与通信保密速率的折中特性各异。例如，在图6(a)中，增加距离感知保密速率权重会使通信保密速率降低，同时角度和散射感知保密速率略有提升，但平均增幅低于距离感知保密速率，这与之前的研究结论相符，表明不同感知信息的保密速率虽存在共同提升的趋势，但无法同时达到最优，一种感知信息的保密速率最优会导致其他感知信息保密速率的次优。这说明不同感知信息之间既存在合作共赢，也存在资源竞争。

由于权重因子为四维变量，难以通过图像直观展示通信保密速率与距离、方向、散射感知、

保密速率四者之间的性能折中关系。但根据现有结果可以推断,通过求解不同权重因子下的问题式(38),可得到ISAC系统整体安全性能最优的Pareto解集。ISAC系统的安全性能上界可被视为四维空间中的球体,球体内为系统可达的安全性能范围,球面上的点集则构成通过求解问题式(38)得到的Pareto解集。

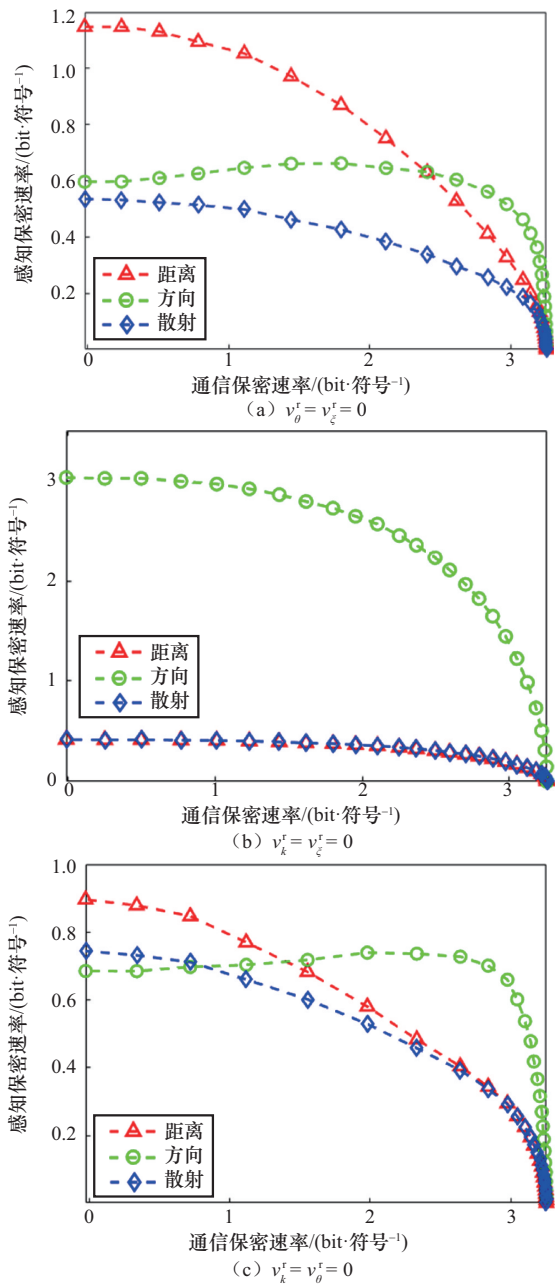


图6 ISAC系统中通信和感知保密速率性能折中关系

最后,通过仿真试验对本文所提的实际系统中安全最优预编码设计方案的有效性进行了充分验证。为了全面地衡量系统的整体安全性能,本研究引入了综合保密速率这一指标,定义为通信保密速率与感知保密速率之和。最优预编码方案下综合保密速率随发射功率变化曲线如图7所示。在基准方案的选取上,选取在通信和感知性能约束下,单纯考虑通信保密速率最优的预编码方案作为基准方案1,单纯考虑感知保密速率最优的预编码方案作为基准方案2,以此来凸显联合考虑通信和感知安全性能在ISAC系统整体安全性能方面的优势。

图7(a)~(d)分别展示了本文所提的实际ISAC系统中安全最优预编码方案在最大化不同感知信息(距离、方向、散射)保密速率和通信保密速率时,综合保密速率与基准方案的综合保密速率随发射功率变化的曲线。从图7中可以清晰地看出,本文所提的联合考虑通信和感知安全的最优预编码方案相较于基准方案,在系统的综合保密速率上具有显著优势。无论在何种情况下追求保密速率最优,本文所提方案的综合保密速率均高于基准方案。以图7(a)为例,所提方案在最大化距离保密速率的同时,充分考虑了方向、散射和通信保密速率,并对其对应的保密速率设置了大于设定门限的约束。这种设计既确保了整体安全性能的提升,又避免了某一信息的保密速率小于0的情况,从而全面地保护了通信和感知信息的安全性。

通过进一步的数值分析可知,本文所提的安全方案相较于基准方案1,系统的综合保密速率提升幅度在8.68%~85.57%,平均提升34.11%;相较于基准方案2,系统的综合保密速率提升幅度在5.76%~100.16%,平均提升30.75%。这一提升效果与优化目标选择和发射功率密切相关。从图7中可以看出,在发射功率较低时,系统的综合保密速率提升最显著,而随着发射功率的逐渐

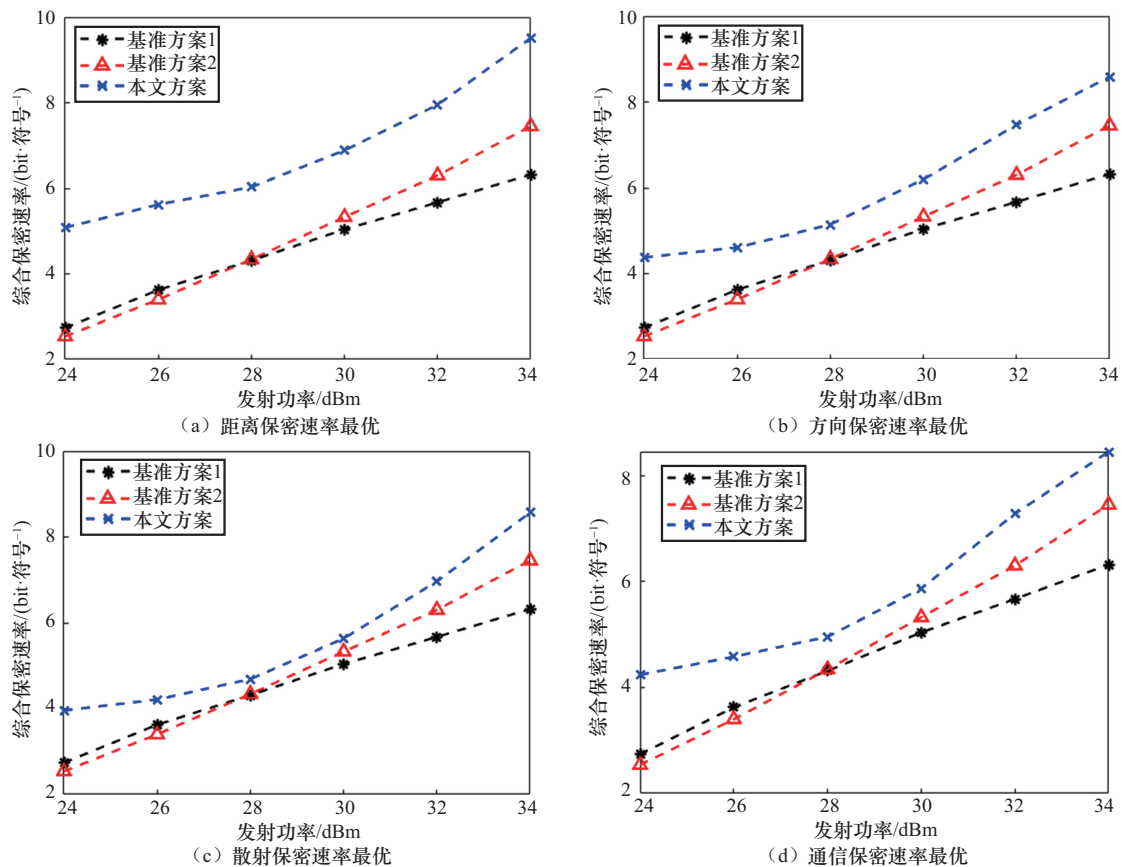


图7 最优预编码方案下综合保密速率随发射功率变化曲线

增大,提升幅度会逐渐减小并趋于收敛。原因在于,当发射功率较低时,受到发射功率的限制,本文所提方案能够合理地分配有限的功率,集中于提升系统的整体安全性能;而基准方案则会将功率主要用于提升单一信息的安全性能,从而导致在系统综合保密速率方面,本文所提方案具有更显著的优势。综上所述,通过仿真实验的验证,本文所提的实际系统中的安全最优预编码设计相较于基准方案,在系统整体安全性能上展现出明显的优势。

4 结束语

针对存在双窃听威胁的ISAC系统,利用信息论推导出感知保密速率的表达式,进而获得ISAC系统中感知保密速率的可达上界。鉴于ISAC系统中通信与感知相互耦合的特性,单独

分析通信安全或感知安全均存在局限性。因此,综合考虑通信与感知的安全性能,为获取二者之间的性能折中曲线及保密速率上界,构建了通信保密速率和感知保密速率之间的加权优化问题模型。通过求解不同权重下的加权优化问题,得出联合优化通信和感知保密速率的Pareto解集,进而确立了ISAC系统中的安全性能的理论上界。

为解决实际ISAC系统中安全性能最优的预编码方案的设计问题,基于实际性能需求构建相应优化问题。通过求解优化问题,分别得出在通信安全性能约束下感知安全性能最优以及在感知安全性能约束下通信安全性能最优的预编码设计方案。仿真结果显示,本文所提的联合考虑的安全预编码方案相较于传统单一考虑的安全预编码方案,综合保密速率平均提升了32.43%。特别是在发射功率较低的情形下,性

能提升更为显著。此外，本文为便于性能上界的推导，仅针对ISAC系统中单一用户情况予以分析。后续研究将着眼于拓展场景至多用户，深入钻研多用户场景中同步保障通信和感知安全的方案设计问题。

附录A

距离互信息的近似闭式解表示为：

$$I(r_i; k_i) = p_k \ln \frac{N\delta_i}{\sqrt{6e}} + (1-p_k) \ln \frac{e^{0.5(\delta_i^2+1)}}{\delta_i \sqrt{2\pi}} + H(p_k) \quad (\text{A1})$$

方向互信息的近似闭式解表示为：

$$I(r_i; \theta_i) = p_\theta \ln \frac{|\Theta| M \cos \theta_0 \sqrt{\pi M \delta_i^2}}{2\sqrt{3e}} + (1-p_\theta) \ln \frac{e^{M\delta_i^2+0.5}}{\sqrt{2\pi} \cdot (2M\delta_i^2)} + H(p_\theta) \quad (\text{A2})$$

其中， p_k 和 p_θ 分别定义了距离和角度的可分辨率，它们是基于感知接收信号中信号自相关函数与信号和噪声的互相关函数得到的关于感知参数的估计值位于实际值附近的归一化概率，表示为：

$$p_k = \frac{e^{0.5\delta_i^2+1}}{N\delta_i^2 \sqrt{\pi/3} + e^{0.5\delta_i^2+1}} \quad (\text{A3})$$

$$p_\theta = \frac{2\sqrt{3} e^{M\delta_i^2 + \frac{1}{2} + \frac{2M-1}{M+1}}}{|\Theta| 2M^2 \pi \delta_i^2 \cos \theta_i + 2\sqrt{3} e^{M\delta_i^2 + \frac{1}{2} + \frac{2M-1}{M+1}}} \quad (\text{A4})$$

并且， $H(p)$ 定义为表示源信号的不确定性变量，表示为：

$$H(p) = p \ln p - (1-p) \ln (1-p) \quad (\text{A5})$$

参考文献：

- [1] ITU-R M. 2160-0(11/2023). Framework and overall objectives of the future development of IMT for 2030 and beyond[S].
- [2] 熊一枫, 刘凡, 袁伟杰, 等. 通信感知一体化的信息理论极限[J]. 中国科学:信息科学, 2023, 53(11): 2057-2086.
Xiong Y F, Liu F, Yuan W J, et al. Information-theoretic limits of integrated sensing and communications[J]. Sci Sin Inform, 2023, 53(11): 2057-2086.
- [3] 徐金雷, 赵俊渥, 卢华兵, 等. 面向6G的多维扩展通感一体化研究综述[J]. 电子与信息学报, 2024, 46(5): 1672-1683.
Xu J L, Zhao J S, Lu H B, et al. An overview on multi-dimensional expanded integrated sensing and communication for 6G[J]. Journal of Electronics & Information Technology, 2024, 46(5): 1672-1683.
- [4] 彭木根, 刘喜庆, 刘子乐, 等. 6G通信感知一体化理论与技术[J]. 控制与决策, 2023, 38(01): 22-38.
Peng M G, Liu X Q, Liu Z L, et al. Principles and techniques in communication and sensing integrated 6G systems[J]. Control and Decision, 2023, 38(01): 22-38.
- [5] Khalid W, Rehman M A U, Van C T, et al. Reconfigurable intelligent surface for physical layer security in 6G-IoT: designs, issues, and advances[J]. IEEE Internet of Things Journal, 2024, 11(2): 3599-3613.
- [6] Liu F, Zhou L, Masouros C, et al. Toward dual-functional radar-communication systems: optimal waveform design[J]. IEEE Transactions on Signal Processing, 2018, 66(16): 4264-4279.
- [7] Su N, Liu F, Masouros C. Sensing-assisted eavesdropper estimation: an ISAC breakthrough in physical layer security[J]. IEEE Transactions on Wireless Communications, 2024, 23(4): 3162-3174.
- [8] Zou J, Masouros C, Liu F, et al. Securing the sensing functionality in ISAC networks: an artificial noise design[J]. IEEE Transactions on Vehicular Technology, 2024, 73(11): 17800-17805.
- [9] Deligiannis A, Daniyan A, Lambotaran S, et al. Secrecy rate optimizations for MIMO communication radar[J]. IEEE Transactions on Aerospace and Electronic Systems, 2018, 54(5): 2481-2492.
- [10] Su N, Liu F, Masouros C. Secure radar-communication systems with malicious targets: integrating radar, communications and jamming functionalities[J]. IEEE Transactions on Wireless Communications, 2019, 20(1): 83-95.
- [11] Yu X, Ng D W K, Schmeink A, et al. Robust and secure resource allocation for ISAC systems: a novel optimization framework for variable-length snapshots[J]. IEEE Transactions on Communications, 2022, 70(12): 8196-8214.
- [12] Su N, Liu F, Wei Z, et al. Secure dual-functional radar-communication transmission: exploiting interference for resilience against target eavesdropping[J]. IEEE Transactions on Wireless Communications, 2022, 21(9): 7238-7252.
- [13] Zhu Y, Xiao Z, Chen Y, et al. Et Tu Alexa? When commodity Wi-Fi devices turn into adversarial motion sensors[C]//Proceedings of the 2020 Network and Distributed System Security



Symposium. 2020:1 - 15.

- [14] Qiao Y, Zhang O, Zhou W, et al. PhyCloak: obfuscating sensing from communication signals[C]//Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16). Santa Clara, USA: USENIX, 2016: 685-699.
- [15] Luo J, Cao H, Jiang H, et al. MIMOCrypt: multi-user privacy-preserving Wi-Fi sensing via MIMO encryption[C]// Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2024: 2812-2830.
- [16] Paul S, Simon M, Stefan R, et al. IRShield: a countermeasure against adversarial physical-layer wireless sensing[C]// Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2022: 1705-1721.
- [17] Ruan L, Zhu H. Leveraging RIS to assist communication and against CSI-based passive sensing[J]. IEEE Wireless Communications Letters, 2024, 13(6): 1750-1754.
- [18] Ren Z, Xu J, Qiu L, et al. Secure cell-free integrated sensing and communication in the presence of information and sensing eavesdroppers[J]. IEEE Journal on Selected Areas in Communications, 2024, 24(11): 3217-3231.
- [19] 徐大专, 张小飞. 空间信息论[M]. 北京: 科学出版社, 2021.
Xu D Z, Zhang X F. Space informatics theory[M]. Beijing: Science Press, 2021.
- [20] Xu S, Xu D, Luo H. Information theory of detection in radar systems[C]//Proceedings of the 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT). Piscataway: IEEE Press, 2017: 249-254.
- [21] Xu D, Yan X, Xu S, et al. Spatial information theory of sensor array and its application in performance evaluation[J]. IET Communications, 2019, 13(15): 2304-2312.
- [22] YD/T 3929-2021 5G 数字蜂窝移动通信网6GHz 以下频段基站设备技术要求(第一阶段)[S].
YD/T 3929-2021 Technical requirements for base station equipment in 5G digital cellular mobile communication networks (Sub-6 GHz Band) (Phase 1)[S].

[作者简介]



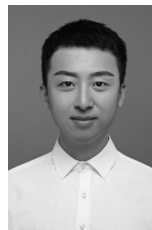
焦世恒 (2001-), 男, 信息工程大学信息技术研究所硕士生, 主要研究方向为通信感知一体化和物理层安全等。



钟州 (1982-), 男, 博士, 信息工程大学信息技术研究所副教授、硕士生导师, 主要研究方向为智能超表面、物理层安全、阵列信号处理等。



马克明 (1985-), 男, 信息工程大学信息技术研究所副研究员, 主要研究方向为智能超表面、物理层安全、阵列信号处理等。



胡晓言 (1992-), 男, 博士, 信息工程大学信息技术研究所助理研究员, 主要研究方向为物理层安全及信息安全。



华浩江 (1994-), 男, 博士, 紫金山实验室助理研究员, 主要研究方向为通信感知一体化、无线物理层安全、信息超材料等。