中国科学: 信息科学 2023 年 第 53 卷 第 11 期: 2266–2282
SCIENTIA SINICA Informationis
论文

多维域低零功率通信

安建平, 丁海川*, 王帅

北京理工大学网络空间安全学院, 北京 100081
* 通信作者. E-mail: hcding@bit.edu.cn

收稿日期: 2023–02–13; 修回日期: 2023–04–05; 接受日期: 2023–05–17; 网络出版日期: 2023–11–09

国家重点研发计划 (批准号: 2022YFC3331103)、国家自然科学基金 (批准号: 62201045) 和中国科协青托项目 (批准号: 2021QNRC001) 资助

摘要 无线信道的开放性使得无线通信链路极易受到窃听和攻击. 随着硬件设备的发展和信号处理技术的进步, 无线通信链路面临的安全威胁日益严峻, 亟需一种更为有效的防护机制保障无线通信链路的安全. 为此, 本文从能量博弈的角度提出了基于信号能量弥散的多维域低零功率通信体制, 通过隐藏通信信号和行为来避免恶意用户对无线通信链路监听和攻击. 该体制以直接序列扩频技术为基础, 以通信行为的隐匿为目标, 通过将信号能量在时、频、空、码和极化等多维参数空间进行弥散, 增加侦听方的能量收集难度, 提升信号的隐蔽性. 本文以侦听方有关多维域信号参数的先验信息为基础定义信号的隐蔽性, 并结合概率论、信息论和信号检测理论建立多维域低零功率通信系统的数学模型, 分析了系统的可达性能极限, 揭示了侦听方先验知识对隐蔽通信速率的影响, 为后续研究工作的开展奠定了理论基础. 结果显示通过信号能量的多维域弥散合法用户间的通信速率能够突破传统 1/2 次幂的变化规律, 实现高效隐蔽的信号传输.

关键词 低零功率通信, 扩频通信, 先验信息, 性能分析

1 引言

随着无线通信技术的广泛应用, 其所带来的安全问题也日益凸显. 无线信道的开放特性使得无线通信链路极易受到窃听和攻击 [1~3]. 同时, 硬件设备和信号处理技术的发展进一步加剧了无线通信链路所面临的安全威胁. 为满足高层次的无线安全通信需求, 本文在低截获概率通信的基础上, 从能量博弈的角度提出了基于信号能量弥散的多维域低零功率通信体制, 通过保证通信信号和行为的隐蔽性来避免恶意用户对无线通信链路的监听和攻击. 多维域低零功率通信与物理层安全技术均能保证合法用户的信息在无线信道上的安全传输. 然而, 多维域低零功率通信侧重于通信信号的隐蔽, 物理层安全技术则更注重传输信息的隐匿. 鉴于直接序列扩频信号良好的抗侦测、抗截获能力, 多维域低零功率通信以直接序列扩频技术为基础, 以通信行为的隐匿为目标, 通过将信号能量在时、频、空、码和极

引用格式: 安建平, 丁海川, 王帅. 多维域低零功率通信. 中国科学: 信息科学, 2023, 53: 2266–2282, doi: 10.1360/SSI-2023-0033
An J P, Ding H C, Wang S. Low-to-no-power covert communication based on energy dispersion (in Chinese). Sci Sin Inform, 2023, 53: 2266–2282, doi: 10.1360/SSI-2023-0033

化等多维参数空间进行弥散, 增加侦听方的能量收集难度, 提升信号的隐蔽性. 与低截获概率通信相比, 多维域低零功率通信信号不仅需要保证信号在常规侦测手段下的隐蔽性, 更需要能够应对长年累月近乎无尽算力的信号侦收. 另一方面, 现有隐蔽通信的相关工作多集中于理论层面, 主要通过信道编码方案的设计来确保信号的隐蔽性. 相比之下, 多维域低零功率通信从能量博弈的角度出发, 通过信号能量弥散的方式增加侦听方的能量收集难度, 从而提升通信信号的隐蔽性.

理解系统的性能极限及其随不同信号参数的变化规律是通信系统设计与应用的基础. 通信信号隐蔽性的刻画是多维域低零功率通信系统性能分析的关键. 自 2013 年起, 学者们提出了以错误检测概率为基础和以 Kullback-Leibler 散度 (KL 散度) 为基础的两种常用通信信号隐蔽性度量, 并以此为指引围绕隐蔽性约束下的通信系统性能极限开展了大量的研究工作. Bash 等 [4] 率先建立了隐蔽通信系统的数学模型, 并结合信号检测概率与 KL 散度间的关系给出了隐蔽通信系统最大无差错通信速率随侦听方侦测时长的幂次衰减规律. Bash 等 [5] 随后将这一结果进一步拓展至侦听方未知信号发送时刻的情况, 通过分析证明了信号发送时刻的不确定性能够带来隐蔽通信速率的提升. 依托 Bash 等所提出的隐蔽通信系统分析框架, 文献 [6] 运用随机几何理论对多址干扰下的隐蔽通信速率展开了讨论, 分别得出了干扰受限和噪声受限场景下隐蔽通信速率随干扰节点分布和传输功率的变化规律. 在有限码长的情况下, 文献 [7] 研究了隐蔽通信速率随侦听信道质量信息和通信信道质量信息准确程度的变化规律, 并根据上述结果得出了隐蔽性约束下的最大发送功率和码长. 为满足战场的实时态势感知需求, 文献 [8] 通过优化码长、发送功率和传输概率实现了通信信号隐蔽性和信息传输时效性间的折中. 类似地, 文献 [9] 提出了一种基于概率的信号传输方案以提升隐蔽通信系统的性能. 文献 [10] 探究了多侦听节点随机分布的情形下有限码长隐蔽通信系统的性能. 结果显示系统的平均有效隐蔽通信速率仅会在侦听节点密度较低的情况下随码长的增加而增大. 文献 [11] 研究了搭载智能反射表面的无人机辅助下的隐蔽通信, 在侦听方位置不确定的前提下, 分析了侦听方的信号侦测性能, 并对信号的发射功率、智能反射表面的相移以及无人机的水平位置进行优化, 在满足隐蔽性约束的前提下最大化合法用户间的隐蔽传输速率. 文献 [4,5,8] 的研究结果表明侦听方所侦收到的信号能量对通信信号的隐蔽性有着决定性的影响. 因此, 利用信号能量的多维域弥散降低侦听方的能量侦收效率能够有效地提升通信信号的隐蔽性. 虽然现有工作初步刻画了隐蔽性约束下的通信系统性能, 但其结果难以准确刻画基于能量弥散的多维域低零功率通信系统的性能. 一方面, 现有的理论分析结果仅停留在符号的层面, 无法直接适用于以直接序列扩频为基础的低零功率通信系统. 另一方面, 现有的分析框架缺乏对于侦听方先验知识的考虑, 难以有效刻画信号能量多维域弥散和侦听方有关多维域信号参数的先验知识对隐蔽通信速率的影响. 虽然文献 [12,13] 围绕侦听方先验知识对隐蔽通信性能的影响进行了讨论, 但是这两项工作主要从侦听方对接收信号认知的角度出发, 并未考虑先验知识对信号能量侦收的影响, 无法直接应用于多维域低零功率通信系统的性能分析.

鉴于现有工作的不足, 本文以直接序列扩频信号的特点为基础, 从侦听方的先验知识入手, 结合概率论、信息论和信号检测理论建立了基于能量弥散的多维域低零功率通信系统的性能分析框架. 首先, 本文就通信信号能量多维域弥散的过程展开了讨论, 并以此建立了多维域低零功率通信系统的信号模型. 考虑到侦测方式对信号传输隐蔽性的影响, 本文随后以 KL 散度为指引就侦听方的信号侦测方式展开了讨论, 并结合其有关多维域信号参数的先验知识给出了通信信号隐蔽性的数学度量. 最后, 本文根据上述结果分析了多维域低零功率通信系统的可达速率, 研究了信号能量多维域弥散和侦听方先验知识对通信系统性能的影响. 本文主要贡献总结如下.

• 提出了基于信号能量多维域弥散的低零功率通信体制, 通过将信号能量在时、频、空、码和极化等不同的维域进行弥散, 增加信号被侦测的难度, 提升通信信号的隐蔽性.

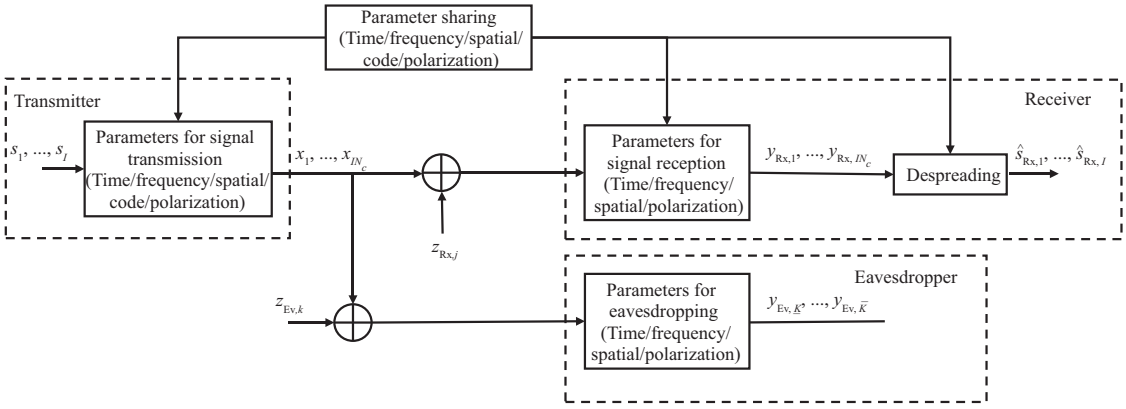

图 1　多维域隐蔽低零功率通信系统示意图

Figure 1　System model for covert communication based on energy dispersion

• 建立了多维域低零功率通信系统的数学模型, 并以 KL 散度为指引就侦听方的信号侦测方式展开了分析.

• 结合侦听方的信号侦测方式及其关于信号参数的先验知识给出了通信信号隐蔽性的数学度量, 分析了多维域低零功率通信系统的可达速率.

• 通过理论分析验证了通信系统能够通过发送信号能量的多维域弥散突破传统 1/2 次幂的变化规律, 实现高效且隐蔽的信号传输.

接下来, 第 2 节就多维域低零功率通信的基本概念展开了讨论, 并建立了多维域低零功率通信系统的数学模型; 第 3 节以 KL 散度为指引讨论了侦听方应当采用的信号侦测方式; 第 4 节在前几节内容的基础上给出了通信信号隐蔽性的数学度量, 分析了多维域低零功率通信系统的可达速率及侦听方先验知识对隐蔽通信速率的影响; 第 5 节通过仿真结果验证了理论分析的有效性; 第 6 节对本文的主要结果进行了梳理和总结.

2　基本概念与系统模型

在多维域低零功率通信系统中, 发送方以符号为单位通过时、频、空、码和极化等参数的选取完成信号能量在高维参数空间的弥散. 合法用户间的通信速率取决于接收方的能量收集效率, 而信号的抗侦测能力取决于侦听方的能量收集难度. 多维域低零功率通信系统通过信号能量在时、频、空、极化等维度的弥散提高了接收机接收到有用信号能量的难度, 运用直接序列扩频技术增加了接收机有效利用侦收信号能量的难度. 因此, 接收方和侦听方对信号时、频、空、码和极化等发送参数的估计直接影响了自身的通信速率和信号侦收性能. 考虑到发送信号的低零功率特性, 接收方和侦听方的发送参数估计效果取决于其所掌握的信号参数相关的先验知识. 正确的先验知识能够有效地辅助信号的参数估计, 而错误的先验知识将会导致错误的参数估计结果, 从而制约了能量收集效率. 根据上述讨论, 我们以各方有关信号参数的先验知识为基础建立了如图 1 所示的多维域低零功率通信系统的数学模型.

图 1 中, 发送方根据事先和接收方约定好的信号参数通过直接序列扩频和调制等步骤将基带号 $s_1, \ldots, s_I$ 变换为 $x_1, \ldots, x_{IN_c}$ 进行发送, 其中, I 是发送符号的个数, N_c 是信号的扩频比, $\boldsymbol{x}_i = \boldsymbol{c}_i s_i$. s_i 服从均值为 0 方差为 P 的循环对称复高斯 (Gauss) 分布, P 是信号的发送功率. $\boldsymbol{c}_i$ 是 N_c 维的向量, 代表了发送第 i 个符号时所使用的扩频序列. 本文所涉及的扩频码字均具有相同的长度. 第 i 个符号

所对应的信号片段 $x_{(i-1)N_c+1},\ldots,x_{iN_c}$ 在第 $m_{\mathrm{Tx},i}$ 个信道上发送, 其中, $m\in\mathcal{M}$, $\mathcal{M}$ 为系统中可用信道序号所组成的集合. 接收方按照约定的参数进行信号接收, 得到叠加噪声后的信号

$$y_{\mathrm{Rx},j}=h_{\mathrm{Rx},j}x_j+z_{\mathrm{Rx},j},\ 1\leqslant j\leqslant IN_c, \tag{1}$$

其中, $h_{\mathrm{Rx},j}$ 代表信号经过信道传播后所经历的幅度和相位变化, $z_{\mathrm{Rx},j}\sim\mathcal{CN}\left(0,\eta_{\mathrm{Rx}}W_{\mathrm{Rx}}\right)$ 是加性高斯白噪声, η_{Rx} 是接收方处的噪声功率谱密度, W_{Rx} 是发送信号的带宽. 如图 1 所示, 本文考虑了数字域的信号模型. 因此, 本文将在接下来的讨论中通过采样时刻的序号来刻画信号的发送时段和侦听方的侦收时段. 不失一般性, 设信号在序号为 1 的采样时刻开始发送, 发送时长为 IN_c 个采样点. 同样的, 侦听方处的接收信号可以被表示为

$$y_{\mathrm{Ev},k}=h_{\mathrm{Ev},k}x_{\mathrm{Ev},k}+z_{\mathrm{Ev},k},\ \underline{K}\leqslant k\leqslant\overline{K}, \tag{2}$$

其中, $h_{\mathrm{Ev},k}$ 代表信号经过发送方至侦听方间的信道传播后所产生的幅度和相位变化, $z_{\mathrm{Ev},k}$ 代表了均值为 0 方差为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}$ 的加性高斯白噪声, η_{Ev} 是侦听方处的噪声功率谱密度, W_{Ev} 是侦听方的侦收机带宽, $\underline{K}$ 是侦听方开始进行信号侦听的时刻, $\overline{K}$ 是信号侦听结束的时刻. 在接下来的讨论中, 假设发送方已知 $h_{\mathrm{Rx},j}$ 和 $h_{\mathrm{Ev},k}$ 的取值, 接收方和侦听方分别已知 $h_{\mathrm{Rx},j}$ 和 $h_{\mathrm{Ev},k}$ 的取值, 并且通信信道和侦听信道状态在整个侦听过程中保持不变, 即 $h_{\mathrm{Rx},j}=h_{\mathrm{Rx}}$, $h_{\mathrm{Ev},k}=h_{\mathrm{Ev}}$. 实际中, 接收方可以利用发送信号中所插入的导频信号进行信道估计来获取 $h_{\mathrm{Rx},j}$. 另外, 为了保证信号传输的隐蔽性, 本文沿用现有研究工作的思路, 考虑了侦听方的信号侦测性能极限, 故而假设侦听方能够获取准确的信道状态 $h_{\mathrm{Ev},k}$. 与现有的工作不同, 本文通过 $\underline{K}$ 和 $\overline{K}$ 的引入在系统模型中明确考虑了侦听方侦收时段与发送方信号发送时段的不同. 当 $1\leqslant k\leqslant IN_c$ 时, $x_{\mathrm{Ev},k}=x_k$, 否则 $x_{\mathrm{Ev},k}=0$. 侦收方的侦收带宽能够同时覆盖 M_{Ev} 个信道. 记侦听方所侦听的信道序号的集合为 $\mathcal{M}_{\mathrm{Ev}}$, $\mathcal{M}_{\mathrm{Ev}}\subset\mathcal{M}$. 为了达到最佳的通信性能, 发送方需要在保证侦听方无法从 $[y_{\mathrm{Ev},k}]_{\underline{K}\leqslant k\leqslant\overline{K}}$ 中侦测到有用信号的前提下最大化通信速率. 根据本节开头的讨论可知, 侦听方关于信号参数的先验知识决定了 $[y_{\mathrm{Ev},k}]_{\underline{K}\leqslant k\leqslant\overline{K}}$ 中所含信号能量的多寡和侦听方从 $[y_{\mathrm{Ev},k}]_{1\leqslant k\leqslant K}$ 收集信号能量的能力, 从而决定了通信信号被侦测的可能性. 为了便于后续的讨论, 在接下来的分析中仅考虑发送信号能量在时域、频域和码域的弥散, 本文后续的分析方法可以直接拓展至更高维的情况. 将侦听方关于信号参数的先验知识建模为 $(\mathcal{T}_{\mathrm{Ev}},\mathcal{F}_{\mathrm{Ev}},\mathcal{C}_{\mathrm{Ev}})$, 其中, $\mathcal{T}_{\mathrm{Ev}}$ 是可能的信号发送时段的集合, $\mathcal{F}_{\mathrm{Ev}}$ 是可能的信号发送信道的集合, $\mathcal{C}_{\mathrm{Ev}}$ 是可能的扩频码的集合. 为了尽可能多地侦收信号能量, 侦听方应当在其认为有信号传输的时间段内持续地进行信号侦听. 因此, $\underline{K}$ 和 $\overline{K}$ 的取值分别由 $\mathcal{T}_{\mathrm{Ev}}$ 中各时段起始时间的最小值和终止时间的最大值所决定. 侦听方监听的信道所组成的集合 $\mathcal{M}_{\mathrm{Ev}}$ 需满足 $\mathcal{M}_{\mathrm{Ev}}\subset\mathcal{F}_{\mathrm{Ev}}$.

侦听方的信号侦测性能不仅取决于 $[y_{\mathrm{Ev},k}]_{\underline{K}\leqslant k\leqslant\overline{K}}$ 中所含信号能量的多寡, 还取决于侦听方如何利用 $[y_{\mathrm{Ev},k}]_{\underline{K}\leqslant k\leqslant\overline{K}}$ 中所蕴含的信号能量. 接下来, 将以 KL 散度为指引就侦听方的信号侦测方式展开讨论, 并在此基础上给出通信信号隐蔽性的定义, 分析多维域低零功率通信系统的可达性能极限.

3 侦听方式选择

信号侦测是一个二元假设检验问题, 检测器的性能极限取决于接收信号和纯噪声的相似程度. 根据文献 [4] 可知, 侦听方需要根据有信号传输时的接收信号分布来构造最优检测器. 由于侦听方不知道发送方所采用的扩频序列, 其难以直接进行最优检测器的构造. 因此, 侦听方需要寻找一种既能剥离扩频序列的影响又能保证信号检测性能不受损失的侦听方式. 文献 [4] 中的讨论显示最优检测器的

性能可以通过有信号传输和无信号传输所对应的概率分布间的 KL 散度来刻画. KL 散度越大, 最优检测器能够获得越小的错误检测概率. 这一结论也和直观相吻合. KL 散度实质上刻画了两个概率分布间的相似程度 [14]. 有无信号传输所对应的概率分布越相似, 侦听方就越难以准确分辨是否有信号传输. 以下定理从 KL 散度的角度说明利用正确的扩频序列对 $[y_{\mathrm{Ev},k}]_{\underline{K}\leqslant k\leqslant\overline{K}}$ 做相干累积不会对信号侦测性能产生影响.

定理1 当 $\underline{K}\leqslant 1$, $\overline{K}\geqslant IN_c$, 且发送符号服从高斯分布时, 采用 $\boldsymbol{c}_i$ 对 $[y_{\mathrm{Ev},k}]_{(i-1)N_c+1\leqslant k\leqslant iN_c}$ 进行相干累积可得

$$\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},c}\|\,\mathbb{P}_{\boldsymbol{s},c}\right)=\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},nc}\|\,\mathbb{P}_{\boldsymbol{y},nc}\right),$$

其中, $\mathbb{P}_{\boldsymbol{z},c}$ 是 $\left(\overline{K}-\underline{K}+1\right)/N_c$ 个均值为 0 方差为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c$ 的循环对称复高斯变量的联合分布, $\mathbb{P}_{\boldsymbol{s},c}$ 是有信号传输时相干累积结果的联合概率分布, $\mathbb{P}_{\boldsymbol{z},nc}$ 是 $\left(\overline{K}-\underline{K}+1\right)$ 个均值为 0 方差为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}$ 的独立循环对称复高斯随机变量的联合分布, $\mathbb{P}_{\boldsymbol{y},nc}$ 是有信号传输时 $[y_{\mathrm{Ev},k}]_{\underline{K}\leqslant k\leqslant\overline{K}}$ 的分布, $\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},c}\|\,\mathbb{P}_{\boldsymbol{s},c}\right)$ 是 $\mathbb{P}_{\boldsymbol{z},c}$ 和 $\mathbb{P}_{\boldsymbol{s},c}$ 间的 KL 散度, $\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},nc}\|\,\mathbb{P}_{\boldsymbol{y},nc}\right)$ 是 $\mathbb{P}_{\boldsymbol{z},nc}$ 和 $\mathbb{P}_{\boldsymbol{y},nc}$ 间的 KL 散度 [14].

证明 在发送方进行信号传输的情况下, 侦听方利用扩频序列 $\boldsymbol{c}_i$ 对 $[y_{\mathrm{Ev},k}]_{(i-1)N_c+1\leqslant k\leqslant iN_c}$, $1\leqslant i\leqslant I$ 进行相干累积可得

$$\hat{s}_{\mathrm{Ev},i}=\begin{cases}h_{\mathrm{Ev}}s_i+z_i\ m_{\mathrm{Tx},i}\in\mathcal{M}_{\mathrm{Ev}},\ 1\leqslant i\leqslant I,\\ z_i, \qquad\qquad\qquad\qquad\qquad\text{其他},\end{cases}\tag{3}$$

其中, z_i 为均值为 0 方差为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c$ 的循环对称复高斯变量. 结合 KL 散度的定义可将 $\mathcal{D}(\mathbb{P}_{\boldsymbol{z},c}\|\mathbb{P}_{\boldsymbol{s},c})$ 改写为

$$\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},c}\|\,\mathbb{P}_{\boldsymbol{s},c}\right)=I_m\mathcal{D}\left(\mathbb{P}_{z,c}\|\,\mathbb{P}_{s,c}\right),\tag{4}$$

其中, $\mathbb{P}_{z,c}$ 代表一个均值为 0 方差为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c$ 的循环对称复高斯变量的分布, $\mathbb{P}_{s,c}$ 是一个均值为 0 方差为 $|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c$ 的循环对称复高斯变量的分布, P 是符号 s_i 的发送功率, I_m 是满足 $m_{\mathrm{Tx},i}\in\mathcal{M}_{\mathrm{Ev}},1\leqslant i\leqslant I$ 的序号 i 的个数. 根据定义可得

$$\begin{aligned}\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},c}\|\,\mathbb{P}_{\boldsymbol{s},c}\right)=&I_m\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{1}{\pi\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}\mathrm{e}^{-\frac{u_{\mathrm{Re}}^2+u_{\mathrm{Im}}^2}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}}\ln\left\{\frac{|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}\mathrm{e}^{-\frac{u_{\mathrm{Re}}^2+u_{\mathrm{Im}}^2}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}}\right.\\&\left.\times\,\mathrm{e}^{\frac{u_{\mathrm{Re}}^2+u_{\mathrm{Im}}^2}{|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}}\right\}\mathrm{d}u_{\mathrm{Re}}\mathrm{d}u_{\mathrm{Im}}\\=&I_m\ln\frac{|h_{\mathrm{Ev}}|^2P+\eta_{Ev}W_{Ev}/N_c}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}-I_m\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{1}{\pi\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}\mathrm{e}^{-\frac{u_{\mathrm{Re}}^2+u_{\mathrm{Im}}^2}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}}\\&\times\frac{\left(u_{\mathrm{Re}}^2+u_{\mathrm{Im}}^2\right)|h_{\mathrm{Ev}}|^2P}{(|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c)\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}\mathrm{d}u_{\mathrm{Re}}\mathrm{d}u_{\mathrm{Im}}\\=&I_m\ln\left(1+\frac{|h_{\mathrm{Ev}}|^2P}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}\right)-\frac{I_m|h_{\mathrm{Ev}}|^2P}{|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}.\end{aligned}\tag{5}$$

另一方面, $\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},nc}\|\,\mathbb{P}_{\boldsymbol{y},nc}\right)$ 可以根据 KL 散度的定义改写为

$$\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},nc}\|\,\mathbb{P}_{\boldsymbol{y},nc}\right)=I_m\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},N_c}\|\,\mathbb{P}_{\boldsymbol{y},N_c}\right),\tag{6}$$

其中, $\mathbb{P}_{\boldsymbol{z},N_c}$ 是 N_c 个独立的均值为 0 方差为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}$ 的循环对称复高斯随机变量的联合分布, $\mathbb{P}_{\boldsymbol{y},N_c}$ 是有信号传输时单个符号所对应的 N_c 个采样点的联合分布, I_m 已在式 (4) 中进行了定义. 受到符号取值的影响, 同一个符号对应的采样点的幅值和相位具有一定的相关性. 因此, 式 (6) 中的 $\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},nc}\|\,\mathbb{P}_{\boldsymbol{y},nc}\right)$ 无法直接分解成单个采样点所对应的 KL 散度之和. 根据 KL 散度的定义, 可得

$$\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},N_c}\|\,\mathbb{P}_{\boldsymbol{y},N_c}\right)=\int\frac{1}{\left(\pi\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^{N_c}}\mathrm{e}^{-\frac{\boldsymbol{u}^{\mathrm{H}}\boldsymbol{u}}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}}\ln\frac{\frac{1}{\left(\pi\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^{N_c}}\mathrm{e}^{-\frac{\boldsymbol{u}^{\mathrm{H}}\boldsymbol{u}}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}}}{f_{\boldsymbol{y},N_c}\left(\boldsymbol{u}\right)}\mathrm{d}\boldsymbol{u},\tag{7}$$

其中, $f_{\boldsymbol{y},N_c}\left(\boldsymbol{u}\right)$ 是有信号发送时单个符号所对应的采样点的联合概率密度函数, $\boldsymbol{u}^{\mathrm{H}}$ 是向量 $\boldsymbol{u}$ 的共轭转置. 此处, 我们以 $\left[y_{\mathrm{Ev},k}\right]_{1\leqslant k\leqslant N_c}$ 为例来进行 $f_{\boldsymbol{y},N_c}\left(\boldsymbol{u}\right)$ 的推导. 根据第 2 节的信号模型可知

$$\left[y_{\mathrm{Ev},k}\right]_{1\leqslant k\leqslant N_c}=h_{\mathrm{Ev}}\boldsymbol{c}_1s_1+\boldsymbol{z}_1,\tag{8}$$

其中, $\boldsymbol{z}_1$ 是一个由 N_c 个均值为 0 方差为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}$ 的独立循环对称复高斯随机变量所组成的向量. 根据 $\left[y_{\mathrm{Ev,k}}\right]_{1\leqslant k\leqslant N_c}$ 的实部和虚部的独立性, $f_{\boldsymbol{y},N_c}\left(\boldsymbol{u}\right)=f_{\boldsymbol{y}_{\mathrm{Re}},N_c}\left(\boldsymbol{u}_{\mathrm{Re}}\right)f_{\boldsymbol{y}_{\mathrm{Im}},N_c}\left(\boldsymbol{u}_{\mathrm{Im}}\right)$, 其中, $f_{\boldsymbol{y}_{\mathrm{Re}},N_c}\left(\boldsymbol{u}_{\mathrm{Re}}\right)$ 是 $\left[y_{\mathrm{Ev,k}}\right]_{1\leqslant k\leqslant N_c}$ 的实部的概率密度函数, $f_{\boldsymbol{y}_{\mathrm{Im}},N_c}\left(\boldsymbol{u}_{\mathrm{Im}}\right)$ 是 $\left[y_{\mathrm{Ev,k}}\right]_{1\leqslant k\leqslant N_c}$ 的虚部的概率密度函数. 由式 (8) 可得 $f_{\boldsymbol{y},N_c}\left(\boldsymbol{u}\right)$ 的表达式为

$$\begin{aligned}f_{\boldsymbol{y}_{\mathrm{Re}},N_c}\left(\boldsymbol{u}_{\mathrm{Re}}\right)&=\int_{-\infty}^{\infty}f_{\boldsymbol{y}_{\mathrm{Re}},N_c}\left(\boldsymbol{u}_{\mathrm{Re}}\left|s_{1,\mathrm{Re}}\right.\right)\frac{1}{\sqrt{\pi|h_{\mathrm{Ev}}|^2P}}\mathrm{e}^{-\frac{s_{1,\mathrm{Re}}^2}{|h_{\mathrm{Ev}}|^2P}}\mathrm{d}s_{1,\mathrm{Re}}\\&=\int_{-\infty}^{\infty}\frac{1}{\left(\pi\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^{N_c/2}}\mathrm{e}^{-\frac{\left(\boldsymbol{u}_{\mathrm{Re}}-\boldsymbol{c}_1s_{1,\mathrm{Re}}\right)^{\mathrm{T}}\left(\boldsymbol{u}_{\mathrm{Re}}-\boldsymbol{c}_1s_{1,\mathrm{Re}}\right)}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}}\frac{1}{\sqrt{\pi|h_{\mathrm{Ev}}|^2P}}\mathrm{e}^{-\frac{s_{1,\mathrm{Re}}^2}{|h_{\mathrm{Ev}}|^2P}}\mathrm{d}s_{1,\mathrm{Re}},\end{aligned}\tag{9}$$

其中, $s_{1,\mathrm{Re}}$ 是发送符号 s_1 的实部. 由于 $\boldsymbol{c}_1^{\mathrm{T}}\boldsymbol{c}_1=N_c$, $\boldsymbol{c}_1^{\mathrm{T}}$ 是向量 $\boldsymbol{c}_1$ 的转置, $f_{\boldsymbol{y}_{\mathrm{Re}},N_c}\left(\boldsymbol{u}_{\mathrm{Re}}\right)$ 可以化为

$$\begin{aligned}f_{\boldsymbol{y}_{\mathrm{Re}},N_c}\left(\boldsymbol{u}_{\mathrm{Re}}\right)&=\int_{-\infty}^{\infty}\frac{1}{\left(\pi\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^{N_c/2}}\frac{1}{\sqrt{\pi\left|h_{\mathrm{Ev}}\right|^2P}}\mathrm{e}^{-\frac{\boldsymbol{u}_{\mathrm{Re}}^{\mathrm{T}}\boldsymbol{u}_{\mathrm{Re}}-2\boldsymbol{u}_{\mathrm{Re}}^{\mathrm{T}}\boldsymbol{c}_1s_{1,\mathrm{Re}}+N_cs_{1,\mathrm{Re}}^2}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}-\frac{s_{1,\mathrm{Re}}^2}{|h_{\mathrm{Ev}}|^2P}}\mathrm{d}s_{1,\mathrm{Re}}\\&=\int_{-\infty}^{\infty}\frac{1}{\left(\pi\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^{N_c/2}}\frac{1}{\sqrt{\pi\left|h_{\mathrm{Ev}}\right|^2P}}\mathrm{e}^{-\frac{P\boldsymbol{u}_{\mathrm{Re}}^{\mathrm{T}}\boldsymbol{u}_{\mathrm{Re}}-2|h_{\mathrm{Ev}}|^2P\boldsymbol{u}_{\mathrm{Re}}^{\mathrm{T}}\boldsymbol{c}_1s_{1,\mathrm{Re}}+(N_c|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}})s_{1,\mathrm{Re}}^2}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}|h_{\mathrm{Ev}}|^2P}}\mathrm{d}s_{1,\mathrm{Re}}\\&=\int_{-\infty}^{\infty}\frac{1}{\left(\pi\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^{N_c/2}}\frac{1}{\sqrt{\pi\left|h_{\mathrm{Ev}}\right|^2P}}\mathrm{e}^{-\frac{\boldsymbol{u}_{\mathrm{Re}}^{\mathrm{T}}\boldsymbol{u}_{\mathrm{Re}}}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}+\frac{N_c|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}|h_{\mathrm{Ev}}|^2P}\left(\frac{|h_{\mathrm{Ev}}|^2P\boldsymbol{u}_{\mathrm{Re}}^{\mathrm{T}}\boldsymbol{c}_1}{N_c|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}\right)^2}\\&\quad\times\mathrm{e}^{-\frac{N_c|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}|h_{\mathrm{Ev}}|^2P}\left(s_{1,\mathrm{Re}}-\frac{|h_{\mathrm{Ev}}|^2P\boldsymbol{u}_{\mathrm{Re}}^{\mathrm{T}}\boldsymbol{c}_1}{N_c|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}\right)^2}\mathrm{d}s_{1,\mathrm{Re}}\\&=\frac{1}{\left(\pi\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^{N_c/2}}\sqrt{\frac{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}{N_c\left|h_{\mathrm{Ev}}\right|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}}\mathrm{e}^{-\frac{\boldsymbol{u}_{\mathrm{Re}}^{\mathrm{T}}\boldsymbol{u}_{\mathrm{Re}}}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}+\frac{|h_{\mathrm{Ev}}|^2P\left(\boldsymbol{u}_{\mathrm{Re}}^{\mathrm{T}}\boldsymbol{c}_1\right)^2}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\left(N_c|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)}}.\end{aligned}\tag{10}$$

经过类似的推导过程可以得到 $f_{\boldsymbol{y}_{\mathrm{Im}},N_c}\left(\boldsymbol{u}_{\mathrm{Im}}\right)$ 的表达式. 在此基础上, 我们可以得到 $f_{\boldsymbol{y},N_c}\left(\boldsymbol{u}\right)$ 的表达式为

$$f_{\boldsymbol{y},N_c}\left(\boldsymbol{u}\right)=\frac{1}{\left(\pi\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^{N_c}}\frac{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}{N_c\left|h_{\mathrm{Ev}}\right|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}\mathrm{e}^{-\frac{\boldsymbol{u}^{\mathrm{H}}\boldsymbol{u}}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}+\frac{|h_{\mathrm{Ev}}|^2P\boldsymbol{u}^{\mathrm{H}}\boldsymbol{c}_1\boldsymbol{c}_1^{\mathrm{T}}\boldsymbol{u}}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\left(N_c|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)}}.\tag{11}$$

式 (11) 中应用了 $u^{\mathrm{H}}c_1c_1^{\mathrm{T}}u=\left(u_{\mathrm{Re}}^{\mathrm{T}}c_1\right)^2+\left(u_{\mathrm{Im}}^{\mathrm{T}}c_1\right)^2$. 将式 (11) 代入式 (7) 可得

$$\begin{aligned}\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},N_c}\|\,\mathbb{P}_{\boldsymbol{y},N_c}\right)&=\ln\left(1+\frac{N_c\left|h_{\mathrm{Ev}}\right|^2P}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}\right)-\frac{\left|h_{\mathrm{Ev}}\right|^2P\mathrm{E}\left[\boldsymbol{u}^{\mathrm{H}}\boldsymbol{c}_1\boldsymbol{c}_1^{\mathrm{T}}\boldsymbol{u}\right]}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}(N_c\left|h_{\mathrm{Ev}}\right|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}})}\\&=\ln\left(1+\frac{N_c\left|h_{\mathrm{Ev}}\right|^2P}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}\right)-\frac{\left|h_{\mathrm{Ev}}\right|^2PN_c}{N_c\left|h_{\mathrm{Ev}}\right|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}},\end{aligned}\tag{12}$$

其中, 第 1 个等式中的 $\mathrm{E}[\boldsymbol{u}^{\mathrm{H}}\boldsymbol{c}_1\boldsymbol{c}_1^{\mathrm{T}}\boldsymbol{u}]$ 代表了对 $\boldsymbol{u}$ 的分布求期望, 第 2 个等式用到了 $\mathrm{E}[\boldsymbol{u}\boldsymbol{u}^{\mathrm{H}}]=\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\boldsymbol{E}$ 和 $\boldsymbol{c}_{\mathrm{I}}^{\mathrm{T}}\boldsymbol{c}_1=N_c$ 两个结果, $\boldsymbol{E}$ 为单位矩阵. 对比式 (5), (6) 和 (12) 可得到 $\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},c}\|\,\mathbb{P}_{\boldsymbol{s},c}\right)=\mathcal{D}\left(\mathbb{P}_{\boldsymbol{z},nc}\|\,\mathbb{P}_{\boldsymbol{y},nc}\right)$.

当侦听方准确掌握信号的发送功率 P 和信道状态 h_{Ev} 且发送符号分布已知时, 侦听方能够根据直接序列扩频信号的特性得到有信号和无信号发送时相干累积结果的概率分布, 从而构造面向相干累积结果的最优信号检测器. 由定理 1 和前文的分析可知, 此时通过相干累积结果构造的检测器能够逼近最优的信号检测性能. 因此, 本文将在后续的分析中考虑如下的信号侦测方式:

• 尝试用 $\mathcal{C}_{\mathrm{Ev}}$ 中的各个序列对 $[y_{\mathrm{Ev},k}]_{\underline{K}\leqslant k\leqslant\overline{K}}$ 做相干累积, 并构造基于相干累积结果的信号检测器进行信号侦测.

• 若基于相干累积的结果没有侦测到信号传输, 侦听方尝试通过非相干累积的方式进行信号检测.

接下来, 本文将基于上述信号侦测方式探讨多维域低零功率通信系统的可达速率.

4 多维域低零功率通信系统的可达速率

多维域低零功率通信需要同时保证通信信号在接收方处的可靠接收和信号传输对侦听方的隐蔽性. 如图 1 所示, 接收方利用事先共享的参数信息对接收信号进行解扩, 解扩后的信号可以表示为

$$\hat{s}_{\mathrm{Rx},i}=h_{\mathrm{Rx}}s_i+z_i,\ \forall 1\leqslant i\leqslant I,\tag{13}$$

其中, z_i 是均值为 0 方差为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c$ 的循环对称复高斯变量. 由式 (13) 可知, 合法用户间的通信信道是加性高斯白噪声信道. 根据信道编码定理可知, 在给定发送功率 P 的情况下, 合法用户间的可达通信速率为 $I\log_2(1+\left|h_{\mathrm{Rx}}\right|^2PN_c/\eta_{\mathrm{Rx}}W_{\mathrm{Rx}})$ [14], 其中仅有通信信号的发送功率 P 受到隐蔽性约束的影响. 为了得到多维域低零功率通信的可达速率, 本文围绕满足通信信号隐蔽性的最大发送功率 P^* 展开讨论.

因为信号侦测是一个二元假设检验问题, 所以我们采用相干累积和非相干累积时通信信号被侦测的概率来刻画通信信号的隐蔽性, 即隐蔽的信号传输需满足以下条件:

$$\begin{aligned}&\mathbb{P}_{D,c}\left(\mathcal{T}_{\mathrm{Ev}},\mathcal{M}_{\mathrm{Ev}},\boldsymbol{c}_{\mathrm{Ev}}\right)\leqslant\varepsilon,\ \forall\boldsymbol{c}_{\mathrm{Ev}}\in\mathcal{C}_{\mathrm{Ev}},\ \mathcal{M}_{Ev}\subset\mathcal{F}_{\mathrm{Ev}},\\&\mathbb{P}_{D,nc}\left(\mathcal{T}_{\mathrm{Ev}},\mathcal{M}_{\mathrm{Ev}}\right)\leqslant\varepsilon,\end{aligned}\tag{14}$$

其中, $\mathbb{P}_{D,c}\left(\mathcal{T}_{\mathrm{Ev}},\mathcal{M}_{\mathrm{Ev}},\boldsymbol{c}_{\mathrm{Ev}}\right)$ 是利用扩频码字 $\boldsymbol{c}_{\mathrm{Ev}}\in\mathcal{C}_{\mathrm{Ev}}$ 进行相干累积时的信号检测概率, $\mathbb{P}_{D,nc}(\mathcal{T}_{\mathrm{Ev}},\mathcal{M}_{\mathrm{Ev}})$ 是侦听方直接对信号进行非相干累积时的信号检测概率. 接下来, 基于式 (14) 分别就相干累积和非相干累积的情况下发送信号功率需满足的条件展开讨论.

4.1 相干累积下的发送功率约束

根据文献 [15], 当发送符号服从高斯分布时, 对于相干累积结果来说能量检测和似然比检测具有相同的信号检测性能. 因此, 我们考虑用能量检测的方式来刻画通信信号被侦测的概率, 即侦听方判断

有信号传输的条件为

$$\frac{1}{I_W}\sum_{i=1}^{I_W}\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2 \geqslant V_{\mathrm{Ev},j}, \tag{15}$$

其中, $I_W=\left(\overline{K}-\underline{K}+1\right)/N_c$, $V_{\mathrm{Ev},j}$ 是侦听方采用 $\mathcal{C}_{\mathrm{Ev}}$ 中的第 j 个扩频序列进行相干累积时所对应的检测门限, $\hat{s}_{\mathrm{Ev},j}\left[i\right]$ 是相干累积的结果. 根据扩频序列的性质可得

$$\hat{s}_{\mathrm{Ev},j}\left[i\right]=\begin{cases}h_{\mathrm{Ev}}s_i+z_i, & m_{\mathrm{Tx},i}\in\mathcal{M}_{\mathrm{Ev}},\boldsymbol{c}_{\mathrm{Ev,j}}=\boldsymbol{c}_i,\\ z_i, & \text{其他},\end{cases}\quad (\underline{K}-1)/N_c+1\leqslant i\leqslant\overline{K}/N_c, \tag{16}$$

其中, $\boldsymbol{c}_{\mathrm{Ev},j}$ 是集合 $\mathcal{C}_{\mathrm{Ev}}$ 中的第 j 个码字. 记满足 $1\leqslant i\leqslant I$ 且 $m_{\mathrm{Tx},i}\in\mathcal{M}_{\mathrm{Ev}},\boldsymbol{c}_{\mathrm{Ev,j}}=\boldsymbol{c}_i$ 的序号 i 所构成的集合为 $\Pi_{j,1}$, 不满足该条件的序号所构成的集合为 $\Pi_{j,2}$, $\Pi_{j,1}\cup\Pi_{j,2}=\left\{(\underline{K}-1)/N_c+1,\ldots,\overline{K}/N_c\right\}$. 利用 $\Pi_{j,1}$ 和 $\Pi_{j,2}$, 可以将 $\mathbb{P}_{D,c}\left(\mathcal{T}_{\mathrm{Ev}},\mathcal{M}_{\mathrm{Ev}},\boldsymbol{c}_{\mathrm{Ev},j}\right)$ 改写为

$$\mathbb{P}_{D,c}\left(\mathcal{T}_{\mathrm{Ev}},\mathcal{M}_{\mathrm{Ev}},\boldsymbol{c}_{\mathrm{Ev},j}\right)=\mathrm{P}\left(\frac{1}{I_W}\left(\sum_{i\in\Pi_{j,1}}\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2+\sum_{i\in\Pi_{j,2}}\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2\right)\geqslant V_{\mathrm{Ev},j}\right). \tag{17}$$

根据 Berry-Esseen 定理可知, $\mathbb{P}_{D,c}\left(\mathcal{T}_{\mathrm{Ev}},\mathcal{M}_{\mathrm{Ev}},\boldsymbol{c}_{\mathrm{Ev},j}\right)$ 可以被近似为 [16]

$$\mathbb{P}_{D,c}\left(\mathcal{T}_{\mathrm{Ev}},\mathcal{M}_{\mathrm{Ev}},\boldsymbol{c}_{\mathrm{Ev},j}\right)=Q\left(\frac{V_{\mathrm{Ev},j}I_W-\mathrm{E}\left[\Psi\right]}{\sqrt{\mathrm{var}\left[\Psi\right]}}\right), \tag{18}$$

其中, $\Psi=\sum_{i\in\Pi_{j,1}}\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2+\sum_{i\in\Pi_{j,2}}\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2$, $\mathrm{E}\left[\Psi\right]$ 是 Ψ 的期望, $\mathrm{var}\left[\Psi\right]$ 是 Ψ 的方差, $Q\left(x\right)=\frac{1}{\sqrt{2\pi}}\int_x^{\infty}\mathrm{e}^{-t^2/2}\mathrm{d}t$ [17]. 因为 $\hat{s}_{\mathrm{Ev},j}\left[i\right]$ 是独立的随机变量, Ψ 的期望和方差可以表示为

$$\begin{aligned}\mathrm{E}\left[\Psi\right]&=\sum_{i\in\Pi_{j,1}}\mathrm{E}\left[\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2\right]+\sum_{i\in\Pi_{j,2}}\mathrm{E}\left[\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2\right],\\ \mathrm{var}\left[\Psi\right]&=\sum_{i\in\Pi_{j,1}}\mathrm{var}\left[\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2\right]+\sum_{i\in\Pi_{j,2}}\mathrm{var}\left[\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2\right].\end{aligned} \tag{19}$$

从式 (16) 可知, 当 $i\in\Pi_{j,1}$ 时, $\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2$ 服从均值为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c+\left|h_{\mathrm{Ev}}\right|^2P$ 的指数分布. 当 $i\in\Pi_{j,12}$ 时, $\left|\hat{s}_{\mathrm{Ev},j}\left[i\right]\right|^2$ 服从均值为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c$ 的指数分布. 根据式 (19) 可得 $\mathrm{E}\left[\Psi\right]$ 和 $\mathrm{var}\left[\Psi\right]$ 的表达式为

$$\begin{aligned}\mathrm{E}\left[\Psi\right]&=\left|\Pi_{j,1}\right|\left(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c+\left|h_{\mathrm{Ev}}\right|^2P\right)+\left|\Pi_{j,2}\right|\left(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right),\\ \mathrm{var}\left[\Psi\right]&=\left|\Pi_{j,1}\right|\left(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c+\left|h_{\mathrm{Ev}}\right|^2P\right)^2+\left|\Pi_{j,2}\right|\left(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)^2.\end{aligned} \tag{20}$$

综合式 (14), (18) 和 (20) 的结果可得发送信号的功率 P 需满足以下约束:

$$Q\left(\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)-\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2P}{\sqrt{\left|\Pi_{j,1}\right|\left(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c+\left|h_{\mathrm{Ev}}\right|^2P\right)^2+\left|\Pi_{j,2}\right|\left(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)^2}}\right)\leqslant\varepsilon. \tag{21}$$

由于形式过于复杂, 难以直接从式 (21) 中得到满足隐蔽性约束的最大发送功率 P^* 的表达式. 因此, 本文尝试寻求 P^* 的上界 P_{U}^* 和下界 P_{L}^* 来探究隐蔽性约束及侦听方先验知识对 P^* 的影响. 为了保

证信号的隐蔽性, 通常要求 $\varepsilon \leqslant 1/2$. 根据 Q 函数的定义可知, 此时式 (21) 中 Q 函数自变量的分子应当大于等于 0. 因此, 可以得到 P 需满足的第 1 个条件,

$$P \leqslant \frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)}{\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2}. \tag{22}$$

在式 (22) 成立的情况下, 我们可以通过放缩 Q 函数中变量的分母得到式 (21) 成立的充分条件为

$$Q\left(\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)-\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2P}{\sqrt{I_W}\left(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c+\left|h_{\mathrm{Ev}}\right|^2P\right)}\right)\leqslant\varepsilon,\ P\leqslant\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)}{\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2}. \tag{23}$$

对式 (23) 化简可得

$$\begin{aligned}P\leqslant&\min\left\{\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)-Q^{-1}\left(\varepsilon\right)\sqrt{I_W}\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}{Q^{-1}\left(\varepsilon\right)\sqrt{I_W}\left|h_{\mathrm{Ev}}\right|^2+\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2},\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)}{\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2}\right\}\\=&\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)-Q^{-1}\left(\varepsilon\right)\sqrt{I_W}\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}{Q^{-1}\left(\varepsilon\right)\sqrt{I_W}\left|h_{\mathrm{Ev}}\right|^2+\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2}.\end{aligned} \tag{24}$$

类似地, 可以得到式 (21) 成立的必要条件为

$$Q\left(\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)-\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2P}{\sqrt{I_W}\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}\right)\leqslant\varepsilon,\ P\leqslant\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)}{\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2}. \tag{25}$$

将式 (25) 化简可得

$$P\leqslant\min\left\{\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)-Q^{-1}\left(\varepsilon\right)\sqrt{I_W}\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}{\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2},\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)}{\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2}\right\} \tag{26}$$

$$=\frac{I_W\left(V_{\mathrm{Ev},j}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\right)-Q^{-1}\left(\varepsilon\right)\sqrt{I_W}\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}{\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2}. \tag{27}$$

为确保信号侦测效率, 侦听方的门限 $V_{\mathrm{Ev},j}$ 的取值应当满足

$$Q\left(\frac{\sqrt{I_W}\left(V_{\mathrm{Ev},j}-N_c\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)}{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}\right)\leqslant\alpha, \tag{28}$$

其中, α 是侦听方能够接受的虚警概率上限 [18]. 对比式 (21) 和 (28), α 的取值应当满足 $\alpha\leqslant\varepsilon$. 从式 (21) 可知, $V_{\mathrm{Ev},j}$ 设置得太高会导致过高的漏检概率. 因此, 根据式 (28) 将 $V_{\mathrm{Ev},j}$ 设置为

$$V_{\mathrm{Ev},j}=\frac{\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c}{\sqrt{I_W}}Q^{-1}\left(\alpha\right)+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c. \tag{29}$$

将式 (29) 代入式 (24) 可得当 P 满足以下条件时式 (21) 一定成立.

$$P\leqslant\frac{\sqrt{I_W}\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\left(Q^{-1}\left(\alpha\right)-Q^{-1}\left(\varepsilon\right)\right)}{Q^{-1}\left(\varepsilon\right)\sqrt{I_W}\left|h_{\mathrm{Ev}}\right|^2+\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2}. \tag{30}$$

根据式 (30) 可知 P_{L}^* 的表达式为

$$P_{\mathrm{L}}^*=\frac{\sqrt{I_W}\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}/N_c\left(Q^{-1}\left(\alpha\right)-Q^{-1}\left(\varepsilon\right)\right)}{Q^{-1}\left(\varepsilon\right)\sqrt{I_W}\left|h_{\mathrm{Ev}}\right|^2+\left|\Pi_{j,1}\right|\left|h_{\mathrm{Ev}}\right|^2}. \tag{31}$$

将式 (29) 代入式 (26) 可得当式 (21) 成立时 P 需满足

$$P \leqslant \frac{\sqrt{I_W}\eta_{\mathrm{Ev}} W_{\mathrm{Ev}}/N_c \left(Q^{-1}(\alpha) - Q^{-1}(\varepsilon)\right)}{|\Pi_{j,1}|\,|h_{\mathrm{Ev}}|^2}. \tag{32}$$

同样地, 根据式 (32) 可知 P_{U}^* 的表达式为

$$P_{\mathrm{U}}^* = \frac{\sqrt{I_W}\eta_{\mathrm{Ev}} W_{\mathrm{Ev}}/N_c \left(Q^{-1}(\alpha) - Q^{-1}(\varepsilon)\right)}{|\Pi_{j,1}|\,|h_{\mathrm{Ev}}|^2}. \tag{33}$$

结合式 (31) 和 (33) 可得

$$\begin{aligned} P^* = \min\left\{ \frac{\eta_{\mathrm{Ev}} W_{\mathrm{Ev}}/N_c \left(Q^{-1}(\alpha) - Q^{-1}(\varepsilon)\right)}{|h_{\mathrm{Ev}}|^2}\beta, P_{\max} \right\}, \\ \frac{1}{Q^{-1}(\varepsilon) + |\Pi_{j,1}|/\sqrt{I_W}} \leqslant \beta \leqslant \frac{1}{|\Pi_{j,1}|/\sqrt{I_W}}, \end{aligned} \tag{34}$$

其中, $P_{\max}$ 是发送方的最大发送功率.

4.2 非相干累积下的发送信号功率约束

在非相干累积的情况下, 侦听方判定存在信号传输的条件为

$$\frac{1}{\mathcal{K}} \sum_{k=\underline{K}}^{\overline{K}} |y_{\mathrm{Ev},k}|^2 \geqslant \mathcal{V}_{\mathrm{Ev}}, \tag{35}$$

其中, $\mathcal{K} = \overline{K} - \underline{K} + 1$, $\mathcal{V}_{\mathrm{Ev}}$ 是非相干累积下的信号检测门限. 由直接序列扩频信号的特性可知, 同一符号对应的 N_c 个采样点的取值具有相关性. 因此, 我们无法直接采用 4.1 小节的思路得出检测概率的表达式. 考虑到符号间的独立性, 本文将每连续 N_c 个采样点分为一组, 得到 $\mathbb{P}_{D,nc}(\mathcal{T}_{\mathrm{Ev}}, \mathcal{M}_{\mathrm{Ev}})$ 表达式为

$$\mathbb{P}_{D,nc}(\mathcal{T}_{\mathrm{Ev}}, \mathcal{M}_{\mathrm{Ev}}) = \mathbb{P}\left(\frac{1}{\mathcal{K}} \left(\sum_{i\in\Pi_{nc,1}} \sum_{k=(i-1)N_c+1}^{iN_c} |y_{\mathrm{Ev},k}|^2 + \sum_{i\in\Pi_{nc,2}} \sum_{k=(i-1)N_c+1}^{iN_c} |y_{\mathrm{Ev},k}|^2 \right) \geqslant \mathcal{V}_{\mathrm{Ev}} \right), \tag{36}$$

其中, $\Pi_{nc,1} = \Pi_{\mathcal{M}_{\mathrm{Ev}}} \cap \{1,\ldots,I\}$, $\Pi_{\mathcal{M}_{\mathrm{Ev}}}$ 是满足 $m_{\mathrm{Tx},i} \in \mathcal{M}_{\mathrm{Ev}}$ 的序号 i 所构成的集合, $\Pi_{nc,2}$ 与 $\Pi_{nc,1}$ 不相交且满足 $\Pi_{nc,1} \cup \Pi_{nc,2} = \left\{(\underline{K}-1)/N_c + 1, \ldots, \overline{K}/N_c\right\}$. 令 $\psi_i = \sum_{k=(i-1)N_c+1}^{iN_c} |y_{\mathrm{Ev},k}|^2$. 由定义可知, ψ_i, $i \in \left\{(\underline{K}-1)/N_c + 1, \ldots, \overline{K}/N_c\right\}$ 是相互独立的随机变量. 因此, 根据 Berry-Esseen 定理可以将 $\mathbb{P}_{D,nc}(\mathcal{T}_{\mathrm{Ev}}, \mathcal{M}_{\mathrm{Ev}})$ 表示为

$$\mathbb{P}_{D,nc}(\mathcal{T}_{\mathrm{Ev}}, \mathcal{M}_{\mathrm{Ev}}) = Q\left(\frac{\mathcal{K}\mathcal{V}_{\mathrm{Ev}} - \sum_{i=1}^{\mathcal{K}/N_c} \mathrm{E}[\psi_i]}{\sqrt{\sum_{i=1}^{\mathcal{K}/N_c} \mathrm{var}[\psi_i]}} \right), \tag{37}$$

其中, $\mathrm{E}[\psi_i]$ 和 $\mathrm{var}[\psi_i]$ 代表了 ψ_i 的均值和方差. 当 $i \in \Pi_{nc,2}$ 时, ψ_i 是 N_c 个独立同分布的指数随机变量之和. 此时, ψ_i 的均值和方差分别为 $N_c\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}$ 和 $N_c(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}})^2$. 当 $i \in \Pi_{nc,1}$ 时, ψ_i 是 N_c 个相关的随机变量之和. 此时, ψ_i 的均值和方差分别为

$$\mathrm{E}[\psi_i] = N_c\left(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}} + |h_{\mathrm{Ev}}|^2 P\right),$$

$$\begin{aligned}\mathrm{var}\left[\psi_i\right] &= \mathrm{E}\left[\left(\sum_{k=(i-1)N_c+1}^{iN_c}\left|y_{\mathrm{Ev},k}\right|^2\right)^2\right] - \left(\mathrm{E}\left[\sum_{k=(i-1)N_c+1}^{iN_c}\left|y_{\mathrm{Ev},k}\right|^2\right]\right)^2 \\ &= \underbrace{\mathrm{E}\left[\left(\sum_{k=(i-1)N_c+1}^{iN_c}\left|y_{\mathrm{Ev},k}\right|^2\right)^2\right]}_{\Phi_i} - N_c^2\Big(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}} + \left|h_{\mathrm{Ev}}\right|^2 P\Big)^2. \end{aligned} \tag{38}$$

从定义出发, 可以将 Φ_i 改写为

$$\begin{aligned}\Phi_i &= \mathrm{E}\left[\sum_{k=(i-1)N_c+1}^{iN_c}\sum_{l=(i-1)N_c+1}^{iN_c}\left|y_{\mathrm{Ev},l}\right|^2\left|y_{\mathrm{Ev},k}\right|^2\right] \\ &= \mathrm{E}\left[\sum_{k=(i-1)N_c+1}^{iN_c}\left|y_{\mathrm{Ev},k}\right|^4\right] + \mathrm{E}\left[\sum_{k=(i-1)N_c+1}^{iN_c}\sum_{l=(i-1)N_c+1}^{iN_c}\left|y_{\mathrm{Ev},l}\right|^2\left|y_{\mathrm{Ev},k}\right|^2 1\left(k\neq l\right)\right], \end{aligned} \tag{39}$$

其中, 当 $k\neq l$ 时 $1\left(k\neq l\right)=1$, 当 $k=l$ 时 $1\left(k\neq l\right)=0$. 记 $y_{\mathrm{Ev},k}$ 的实部为 $\mathrm{Re}\left\{y_{\mathrm{Ev},k}\right\}$, $y_{\mathrm{Ev},k}$ 的虚部为 $\mathrm{Im}\left\{y_{\mathrm{Ev},k}\right\}$. 由此可得

$$\begin{aligned}\mathrm{E}\left[\sum_{k=(i-1)N_c+1}^{iN_c}\left|y_{\mathrm{Ev},k}\right|^4\right] &= \mathrm{E}\left[\sum_{k=(i-1)N_c+1}^{iN_c}\left(\mathrm{Re}^2\left\{y_{\mathrm{Ev},k}\right\} + \mathrm{Im}^2\left\{y_{\mathrm{Ev},k}\right\}\right)^2\right] \\ &= \sum_{k=(i-1)N_c+1}^{iN_c}\mathrm{E}[\mathrm{Re}^4\{y_{\mathrm{Ev},k}\}] + 2\mathrm{E}[\mathrm{Re}^2\{y_{\mathrm{Ev},k}\}\mathrm{Im}^2\{y_{\mathrm{Ev},k}\}] + \mathrm{E}[\mathrm{Im}^4\{y_{\mathrm{Ev},k}\}]. \end{aligned} \tag{40}$$

在 $i\in\Pi_{nc,1}$ 的情况下, $y_{\mathrm{Ev},k}=h_{\mathrm{Ev}}s_ic_k+z_{\mathrm{Ev},k}$, s_i 是发送的符号, c_k 是第 k 个采样点所对应的码片的取值, $z_{\mathrm{Ev},k}$ 是均值为 0, 方差为 $\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}$ 的循环对称复高斯随机变量. 由此可得

$$\begin{aligned}&\mathrm{E}\left[\mathrm{Re}^4\left\{y_{\mathrm{Ev},k}\right\}\right] = \mathrm{E}\left[\mathrm{Im}^4\left\{y_{\mathrm{Ev},k}\right\}\right] = \frac{3}{4}\Big(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}} + \left|h_{\mathrm{Ev}}\right|^2P\Big)^2, \\ &\mathrm{E}\left[\mathrm{Re}^2\left\{y_{\mathrm{Ev},k}\right\}\mathrm{Im}^2\left\{y_{\mathrm{Ev},k}\right\}\right] = \mathrm{E}\left[\mathrm{Re}^2\left\{y_{\mathrm{Ev},k}\right\}\right]\mathrm{E}\left[\mathrm{Im}^2\left\{y_{\mathrm{Ev},k}\right\}\right] = \frac{1}{4}\Big(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}} + \left|h_{\mathrm{Ev}}\right|^2P\Big)^2. \end{aligned} \tag{41}$$

将式 (41) 代入式 (40) 可得

$$\mathrm{E}\left[\sum_{k=(i-1)N_c+1}^{iN_c}\left|y_{\mathrm{Ev},k}\right|^4\right] = 2N_c\Big(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}} + \left|h_{\mathrm{Ev}}\right|^2P\Big)^2. \tag{42}$$

采用和式 (40) 相同的思路, 可以将式 (39) 中第 2 个等式右边的第 2 项改写为

$$\begin{aligned}&\mathrm{E}\left[\sum_{k=(i-1)N_c+1}^{iN_c}\sum_{l=(i-1)N_c+1}^{iN_c}\left|y_{\mathrm{Ev},l}\right|^2\left|y_{\mathrm{Ev},k}\right|^2 1\left(k\neq l\right)\right] \\ &= \sum_{k=(i-1)N_c+1}^{iN_c}\sum_{l=(i-1)N_c+1}^{iN_c}\mathrm{E}\left[\mathrm{Re}^2\left\{y_{\mathrm{Ev},k}\right\}\mathrm{Re}^2\left\{y_{\mathrm{Ev},l}\right\}\right]1\left(k\neq l\right)\end{aligned}$$

$$
\begin{aligned}
&+\sum_{k=(i-1)N_c+1}^{iN_c}\sum_{l=(i-1)N_c+1}^{iN_c}\mathrm{E}\left[\mathrm{Im}^2\left\{y_{\mathrm{Ev},k}\right\}\mathrm{Im}^2\left\{y_{\mathrm{Ev},l}\right\}\right]1\left(k\neq l\right)\\
&+\sum_{k=(i-1)N_c+1}^{iN_c}\sum_{l=(i-1)N_c+1}^{iN_c}\mathrm{E}\left[\mathrm{Re}^2\left\{y_{\mathrm{Ev},k}\right\}\right]\mathrm{E}\left[\mathrm{Im}^2\left\{y_{\mathrm{Ev},l}\right\}\right]\left(k\neq l\right)\\
&+\sum_{k=(i-1)N_c+1}^{iN_c}\sum_{l=(i-1)N_c+1}^{iN_c}\mathrm{E}\left[\mathrm{Re}^2\left\{y_{\mathrm{Ev},l}\right\}\right]\mathrm{E}\left[\mathrm{Im}^2\left\{y_{\mathrm{Ev},k}\right\}\right]1\left(k\neq l\right).
\end{aligned}\tag{43}
$$

根据 $y_{\mathrm{Ev},k}$ 的表达式可得

$$
\begin{aligned}
&\mathrm{E}\left[\mathrm{Re}^2\left\{y_{\mathrm{Ev},k}\right\}\mathrm{Re}^2\left\{y_{\mathrm{Ev},l}\right\}\right]\\
&\quad=\mathrm{E}\left[\left(\mathrm{Re}\left\{h_{\mathrm{Ev}}s_ic_k\right\}+\mathrm{Re}\left\{z_{\mathrm{Ev},k}\right\}\right)^2\left(\mathrm{Re}\left\{h_{\mathrm{Ev}}s_ic_l\right\}+\mathrm{Re}\left\{z_{\mathrm{Ev},l}\right\}\right)^2\right]\\
&\quad=\mathrm{E}\left[\mathrm{Re}^4\left\{h_{\mathrm{Ev}}s_i\right\}\right]+\mathrm{E}\left[\mathrm{Re}^2\left\{h_{\mathrm{Ev}}s_i\right\}\right]\mathrm{E}\left[\mathrm{Re}^2\left\{z_{\mathrm{Ev},l}\right\}\right]+\mathrm{E}\left[\mathrm{Re}^2\left\{h_{\mathrm{Ev}}s_i\right\}\right]\mathrm{E}\left[\mathrm{Re}^2\left\{z_{\mathrm{Ev},k}\right\}\right]\\
&\qquad+\mathrm{E}\left[\mathrm{Re}^2\left\{z_{\mathrm{Ev},k}\right\}\right]\mathrm{E}\left[\mathrm{Re}^2\left\{z_{\mathrm{Ev},l}\right\}\right]\\
&\quad=\frac{3}{4}|h_{\mathrm{Ev}}|^4P^2+\frac{1}{2}\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}|h_{\mathrm{Ev}}|^2P+\frac{1}{4}(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}})^2.
\end{aligned}\tag{44}
$$

利用式 (44) 可以将式 (43) 改写为

$$
\begin{aligned}
&\mathrm{E}\left[\sum_{k=(i-1)N_c+1}^{iN_c}\sum_{l=(i-1)N_c+1}^{iN_c}|y_{\mathrm{Ev},l}|^2|y_{\mathrm{Ev},k}|^2 1\left(k\neq l\right)\right]\\
&\qquad=N_c\left(N_c-1\right)\left(2|h_{\mathrm{Ev}}|^4P^2+2\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}|h_{\mathrm{Ev}}|^2P+\left(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^2\right).
\end{aligned}\tag{45}
$$

将式 (39), (42) 和 (45) 代入式 (38) 可得 $\mathrm{var}\left[\psi_i\right]$ 的表达式为

$$
\mathrm{var}\left[\psi_i\right]=N_c\left(N_c-1\right)|h_{\mathrm{Ev}}|^4P^2+N_c\Big(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}+|h_{\mathrm{Ev}}|^2P\Big)^2.\tag{46}
$$

根据式 (37), (38) 和 (46) 可得非相干累积下的隐蔽性约束,

$$
Q\left(\frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)-|\Pi_{nc,1}|\,N_c|h_{\mathrm{Ev}}|^2P}{\sqrt{|\Pi_1|\left(N_c|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^2+\left(\mathcal{K}-|\Pi_1|\right)\left(\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)^2}}\right)\leqslant\varepsilon.\tag{47}
$$

沿用 4.1 小节的思路, 本文不直接通过式 (47) 进行非相干累积下最大发射功率 P_{nc}^* 的求解, 而是通过放缩式 (47) 中 Q 函数的分母获得式 (47) 成立的充分条件和必要条件, 并以此为基础求解 P_{nc}^* 的下界 $P_{nc,\mathrm{L}}^*$ 和上界 $P_{nc,\mathrm{U}}^*$.

式 (47) 成立的充分条件为

$$
Q\left(\frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)-|\Pi_{nc,1}|\,N_c|h_{\mathrm{Ev}}|^2P}{\sqrt{\mathcal{K}}(N_c|h_{\mathrm{Ev}}|^2P+\eta_{\mathrm{Ev}}W_{\mathrm{Ev}})}\right)\leqslant\varepsilon,\ P\leqslant\frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)}{|\Pi_{nc,1}|\,N_c|h_{\mathrm{Ev}}|^2}.\tag{48}
$$

由式 (48) 可知, 为保证隐蔽性约束 (47) 的成立, 信号的发送功率 P 需满足

$$
P\leqslant\min\left\{\frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)-Q^{-1}\left(\varepsilon\right)\sqrt{\mathcal{K}}\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}}{Q^{-1}\left(\varepsilon\right)\sqrt{\mathcal{K}}N_c|h_{\mathrm{Ev}}|^2+|\Pi_{nc,1}|\,N_c|h_{\mathrm{Ev}}|^2},\frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}}-\eta_{\mathrm{Ev}}W_{\mathrm{Ev}}\right)}{|\Pi_{nc,1}|\,N_c|h_{\mathrm{Ev}}|^2}\right\}
$$

$$= \frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}} - \eta_{\mathrm{Ev}} W_{\mathrm{Ev}}\right) - Q^{-1}(\varepsilon)\sqrt{\mathcal{K}}\eta_{\mathrm{Ev}} W_{\mathrm{Ev}}}{Q^{-1}(\varepsilon)\sqrt{\mathcal{K}} N_c |h_{\mathrm{Ev}}|^2 + |\Pi_{nc,1}| N_c |h_{\mathrm{Ev}}|^2}. \tag{49}$$

另一方面, 可以得到式 (47) 成立的必要条件为

$$Q\left(\frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}} - \eta_{\mathrm{Ev}} W_{\mathrm{Ev}}\right) - |\Pi_{nc,1}| N_c |h_{\mathrm{Ev}}|^2 P}{\sqrt{\mathcal{K}}\eta_{\mathrm{Ev}} W_{\mathrm{Ev}}}\right) \leqslant \varepsilon,\ P \leqslant \frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}} - \eta_{\mathrm{Ev}} W_{\mathrm{Ev}}\right)}{|\Pi_{nc,1}| N_c |h_{\mathrm{Ev}}|^2}. \tag{50}$$

将式 (50) 化简可得

$$\begin{aligned} P &\leqslant \min\left\{\frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}} - \eta_{\mathrm{Ev}} W_{\mathrm{Ev}}\right) - Q^{-1}(\varepsilon)\sqrt{\mathcal{K}}\eta_{\mathrm{Ev}} W_{\mathrm{Ev}}}{|\Pi_{nc,1}| N_c |h_{\mathrm{Ev}}|^2}, \frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}} - \eta_{\mathrm{Ev}} W_{\mathrm{Ev}}\right)}{|\Pi_{nc,1}| N_c |h_{\mathrm{Ev}}|^2}\right\} \\ &= \frac{\mathcal{K}\left(\mathcal{V}_{\mathrm{Ev}} - \eta_{\mathrm{Ev}} W_{\mathrm{Ev}}\right) - Q^{-1}(\varepsilon)\sqrt{\mathcal{K}}\eta_{\mathrm{Ev}} W_{\mathrm{Ev}}}{|\Pi_{nc,1}| N_c |h_{\mathrm{Ev}}|^2}. \end{aligned} \tag{51}$$

与 4.1 小节类似, 通过虚警概率 α 将非相干累积时的检测门限设为

$$\mathcal{V}_{\mathrm{Ev}} = \frac{1}{\sqrt{\mathcal{K}}} Q^{-1}(\alpha)\eta_{\mathrm{Ev}} W_{\mathrm{Ev}} + \eta_{\mathrm{Ev}} W_{\mathrm{Ev}}. \tag{52}$$

将式 (52) 代入式 (49) 和 (51) 可以分别得到 $P^*_{nc,\mathrm{L}}$ 和 $P^*_{nc,\mathrm{U}}$ 的表达式

$$\begin{aligned} P^*_{nc,\mathrm{L}} &= \frac{\sqrt{\mathcal{K}}\eta_{\mathrm{Ev}} W_{\mathrm{Ev}}\left(Q^{-1}(\alpha) - Q^{-1}(\varepsilon)\right)}{Q^{-1}(\varepsilon)\sqrt{\mathcal{K}} N_c |h_{\mathrm{Ev}}|^2 + |\Pi_{nc,1}| N_c |h_{\mathrm{Ev}}|^2}, \\ P^*_{nc,\mathrm{U}} &= \frac{\sqrt{\mathcal{K}}\eta_{\mathrm{Ev}} W_{\mathrm{Ev}}\left(Q^{-1}(\alpha) - Q^{-1}(\varepsilon)\right)}{|\Pi_{nc,1}| N_c |h_{\mathrm{Ev}}|^2}. \end{aligned} \tag{53}$$

根据式 (53), 我们可以得到 P^*_{nc} 的表达式

$$\begin{aligned} P^*_{nc} &= \min\left\{\frac{\eta_{\mathrm{Ev}} W_{\mathrm{Ev}}\left(Q^{-1}(\alpha) - Q^{-1}(\varepsilon)\right)}{|h_{\mathrm{Ev}}|^2}\beta_{nc}, P_{\max}\right\}, \\ &\frac{1}{Q^{-1}(\varepsilon) + |\Pi_{nc,1}| N_c \Big/ \sqrt{\mathcal{K}}} \leqslant \beta_{nc} \leqslant \frac{1}{|\Pi_{nc,1}| N_c \Big/ \sqrt{\mathcal{K}}}. \end{aligned} \tag{54}$$

接下来, 结合 4.1 和 4.2 小节中的结果, 就多维域低零功率通信系统的可达速率展开讨论.

4.3 可达速率分析

根据式 (34) 和本节第 1 段的讨论可得多维域低零功率通信系统的最大可达速率:

$$\begin{aligned} &\mathcal{R} = I\log_2\left(1 + \min\left\{\frac{|h_{\mathrm{Rx}}|^2 \eta_{\mathrm{Ev}} W_{\mathrm{Ev}}}{|h_{\mathrm{Ev}}|^2 \eta_{\mathrm{Rx}} W_{\mathrm{Rx}}}\left(Q^{-1}(\alpha) - Q^{-1}(\varepsilon)\right)\min\{\tilde{\beta}, N_c\beta_{nc}\}, \frac{|h_{\mathrm{Rx}}|^2 N_c P_{\max}}{\eta_{\mathrm{Rx}} W_{\mathrm{Rx}}}\right\}\right), \\ &\frac{1}{Q^{-1}(\varepsilon) + \Lambda/\sqrt{I}} \leqslant \tilde{\beta} \leqslant \frac{1}{\Lambda/\sqrt{I}},\ \Lambda = \max_{j\in\{1,\ldots,|\mathcal{C}_{\mathrm{Ev}}|\}} |\Pi_{j,1}|, \\ &\frac{1}{Q^{-1}(\varepsilon) + |\Pi_{nc,1}| N_c/\sqrt{\mathcal{K}}} \leqslant \beta_{nc} \leqslant \frac{1}{|\Pi_{nc,1}| N_c/\sqrt{\mathcal{K}}}. \end{aligned} \tag{55}$$

由式 (55) 可知, 多维域低零功率通信系统的可达速率受到了通信信道和侦听信道质量的制约, 建立通信信道质量相对于侦听信道质量的优势有助于系统通信速率的提升. 因此, 低零功率通信系统

的设计不应局限于信号发送功率的降低, 还应该尝试建立通信信道相对于侦听信道的信道质量优势. 此外, 式 (55) 清晰地呈现了侦听方有关信号参数的先验知识对通信速率的影响. 若 Λ 与发送符号个数 I_W 呈线性关系, 即 $\Lambda=\vartheta I_W$ ($\vartheta\in(0,1]$), 则 $\vartheta I_W\leqslant|\Pi_{nc,1}|\leqslant\vartheta\left|\mathcal{C}_{\rm Ev}\right|I_W$, $|\mathcal{C}_{\rm Ev}|$ 是集合 $\mathcal{C}_{\rm Ev}$ 中扩频序列的个数. 不失一般性, 令 $|\Pi_{nc,1}|=\vartheta_1 I_W$, $\vartheta\leqslant\vartheta_1\leqslant\vartheta\left|\mathcal{C}_{\rm Ev}\right|$. 根据 $\mathcal{K}=I_W N_c$ 可得此时 $\tilde{\beta}$ 和 $N_c\beta_{nc}$ 的取值

$$\tilde{\beta}\approx\frac{1}{\vartheta\sqrt{I_W}},\ N_c\beta_{nc}\approx\frac{\sqrt{N_c}}{\vartheta_1\sqrt{I_W}}. \tag{56}$$

因此, 多维域低零功率通信系统的可达速率 $\mathcal{R}$ 可以根据式 (56) 近似为

$$\mathcal{R}\approx\begin{cases}\sqrt{I_W}\frac{1}{\vartheta\ln 2}\frac{|h_{\rm Rx}|^2\eta_{\rm Ev}W_{\rm Ev}}{|h_{\rm Ev}|^2\eta_{\rm Rx}W_{\rm Rx}}\left(Q^{-1}(\alpha)-Q^{-1}(\varepsilon)\right), & \sqrt{N_c}\vartheta\geqslant\vartheta_1,\\ \sqrt{I_W}\frac{\sqrt{N_c}}{\vartheta_1\ln 2}\frac{|h_{\rm Rx}|^2\eta_{\rm Ev}W_{\rm Ev}}{|h_{\rm Ev}|^2\eta_{\rm Rx}W_{\rm Rx}}\left(Q^{-1}(\alpha)-Q^{-1}(\varepsilon)\right), & \sqrt{N_c}\vartheta<\vartheta_1.\end{cases} \tag{57}$$

式 (57) 显示, 当 Λ 与发送符号个数 I_W 呈线性关系, 即相干累积的结果中包含足够多的发送符号时, 系统的最大可达速率 $\mathcal{R}$ 随发送符号数量的增长呈 1/2 次幂的变化规律. 由式 (16) 可知, 当 $\Lambda=I_W$ 时, 相干累积后的结果具有与文献 [4] 相同的信号模型. 此时, 式 (57) 中 1/2 次幂的变化规律与文献 [4] 中的结论相吻合. 另一方面, 式 (57) 还体现了信号能量在码域的弥散对基于相干累积的信号侦测方式和基于非相干累积的信号侦测方式性能的影响. 当 $\sqrt{N_c}\vartheta\geqslant\vartheta_1$ 时, 侦听方能够通过单一扩频序列侦收到足够多的发送符号. 此时, 通过相干累积的结果进行信号侦收将获得比直接对接收信号进行非相干累积更好的信号侦测结果, 因而当 $\sqrt{N_c}\vartheta\geqslant\vartheta_1$ 时系统的可达速率主要受相干累积下的隐蔽性约束所限. 当 $\sqrt{N_c}\vartheta<\vartheta_1$ 时, 侦听方难以通过单一扩频序列收集到足够多的发送符号. 此时, 直接对接收信号进行非相干累积将会获得更好的信号侦测结果, 故而当 $\sqrt{N_c}\vartheta<\vartheta_1$ 时系统的可达速率主要受非相干累积下的隐蔽性约束的制约. 上述结果不仅证明了在同等条件下采用相干累积结果进行信号侦收将会获得更好的侦测效果, 还表明了信号能量在码域的弥散能够恶化相干侦收的效果, 提升低零功率通信系统的性能.

当 $\Lambda=o\left(\sqrt{I_W}\right)$, $|\Pi_{nc,1}|=o\left(\sqrt{I_W}\right)$ 时,

$$\begin{aligned}&\mathcal{R}\approx I_W\log_2\left(1+\min\left\{\frac{|h_{\rm Rx}|^2\eta_{\rm Ev}W_{\rm Ev}}{|h_{\rm Ev}|^2\eta_{\rm Rx}W_{\rm Rx}}\left(Q^{-1}(\alpha)-Q^{-1}(\varepsilon)\right)\min\{\tilde{\beta},N_c\beta_{nc}\},\frac{|h_{\rm Rx}|^2N_cP_{\max}}{\eta_{\rm Rx}W_{\rm Rx}}\right\}\right),\\ &\tilde{\beta}\geqslant\frac{1}{Q^{-1}(\varepsilon)},\ \beta_{nc}\geqslant\frac{1}{Q^{-1}(\varepsilon)},\end{aligned} \tag{58}$$

其中, $\Lambda=o(I_W)$ 表示 $\lim_{I_W\to\infty}\Lambda/I_W=0$ [19]. 式 (58) 中对数函数的取值随着 I_W 的增长维持不变, 此时系统的可达速率 $\mathcal{R}$ 随着 I_W 的增长呈线性变化. 式 (58) 中的结果表明, 当侦听方处的接收信号中未能包含足够多的发送符号时, 合法用户间的可达速率能够突破 1/2 次幂的变化规律. 因此, 当侦听方难以获得关于信号参数的有效先验信息时, 发送方可以通过将发送信号能量在高维参数空间进行弥散来确保侦听方难以捕获到足够多的发送符号, 从而实现高效且隐蔽的信号传输.

5 仿真实验与讨论

本节将通过仿真结果来检验第 4 节中理论分析的有效性. 在仿真过程中, 每个发送符号经过长度为 128 的伪随机序列扩频之后, 随机地从可用信道集合 $\mathcal{M}$ 中选择一个信道进行发送. $\mathcal{M}$ 中的各信道

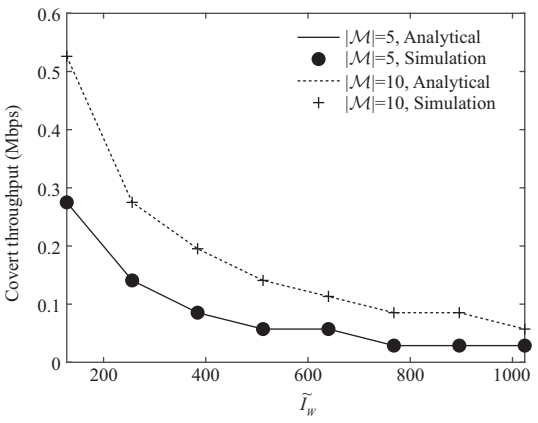

图 2　隐蔽通信速率随被侦听符号个数的变化规律

Figure 2　Covert throughput under various numbers of transmitted symbols received at the eavesdropper

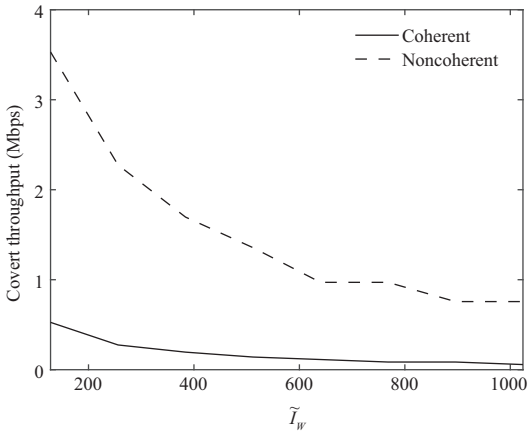

图 3　侦听方采用相干累积和非相干累积下的隐蔽通信速率

Figure 3　Covert throughput under coherent and noncoherent detection

具有相同的带宽. 每次仿真开始时, 侦听方从可用信道集合 $\mathcal{M}$ 中随机选择一个信道进行侦听, 并根据第 4 节中所述的信号侦测方式判断信道上有无信号进行传输. 侦听方每秒连续侦测 1 M 采样点所对应的时长. 受信号能量时域弥散的影响, 侦听方每秒仅能侦听到 $\tilde{I}_W$ 个发送符号. 侦听方根据虚警概率 $\alpha = 0.05$ 来设定信号侦测的门限. 发送方需要合理设置信号的发送功率, 使得发送信号被侦测的概率不高于 0.1.

图 2 展示了合法用户间隐蔽通信速率随被侦收符号数 $\tilde{I}_W$ 的变化规律. 图中侦听方能够选取正确的扩频序列对接收信号进行相干累积, 即侦听方采用第 4.1 小节所示的相干累积的方式进行信号侦收. 在图 2 的仿真实验中, 发送信道和侦听信道具有相同的信道状态, 并且侦听方和接收方处的噪声功率相同. 图中所示的仿真结果由 10000 次实验取平均而得到. 从图 2 可见, 随着 $\tilde{I}_W$ 的增加, 合法用户间的隐蔽通信速率不断下降. 从第 4.1 小节的分析可知, 被侦收到的符号数越多, 合法用户需要采用越低的发送功率来满足隐蔽性约束, 从而使得隐蔽通信速率逐渐下降. 因此, 图 2 验证了第 4.1 小节理论分析结果. 另一方面, 图 2 显示可用信道数量 $|\mathcal{M}|$ 的增加有利于隐蔽通信速率的提升. 产生这一现象的主要原因是可用信道数量 $|\mathcal{M}|$ 的增加提升了信号能量在频域的弥散程度, 从而增加了侦听方进行信号能量侦收的难度. 在此情况下, 即使合法用户采用更高的发送功率, 仍然能够保证发送信号的隐蔽性. 故而, 当可用信道数量 $|\mathcal{M}|$ 增加时, 合法用户间的隐蔽通信速率也得到了相应的提升.

图 3 展示了侦听方所采用的信号侦测方式对隐蔽通信速率的影响. 除 $|\mathcal{M}| = 10$ 外, 图 3 采用了与图 2 相同的仿真参数. 由于图 3 中侦听方能够选用正确的扩频序列进行相干累积, 所以侦收方本质上利用了相同的采样序列进行相干累积和非相干累积. 根据 4.3 小节的讨论可知, 同等条件下侦听方采用相干累积进行信号侦测将会获得比非相干累积更好的侦测效果. 因此, 当侦听方采用相干累积时, 发送方需要采用更低的发射功率来保证通信信号的隐蔽性. 图 3 中的结果进一步验证了文中理论分析的有效性.

6　结论

本文面向无线安全通信的需求从能量博弈的角度提出了以直接序列扩频技术为基础的多维域低

零功率通信体制. 以 KL 散度为指引, 本文就侦听方应当采用的信号侦测方式展开了讨论, 并结合侦听方关于信号参数的先验知识刻画了多维域低零功率通信系统的可达速率. 通过理论分析的结果, 我们可以得到以下结论.

• 建立通信信道质量相对于侦听信道质量的优势有助于多维域低零功率通信速率的提升.

• 当侦听方所收集到的符号数量与实际发送的符号数量呈线性关系时, 多维域低零功率通信系统的可达速率呈现出和现有工作中类似的 1/2 次幂的变化规律.

• 合法用户能够通过将发送信号能量在高维参数空间进行弥散来降低发送符号被侦听方截获的可能性, 从而突破 1/2 次幂的变化规律.

本文通过理论建模与分析验证了多维域弥散对信号隐蔽性能的提升, 相关成果能够为多维域低零功率通信相关的实践创新提供理论指导.

参考文献

1 Lu K, Liu H, Zeng L, et al. Applications and prospects of artificial intelligence in covert satellite communication: a review. Sci China Inf Sci, 2023, 66: 121301

2 Qiu B, Cheng W C. Multi-beam symbol-level secure transmission against hybrid eavesdropping. Sci Sin Inform, 2022, 52: 217–238 [邱彬, 程文驰. 混合窃听环境下多波束符号级安全传输方法. 中国科学: 信息科学, 2022, 52: 217–238]

3 Ma K N, Xu Y F, Shao S, et al. On the optimization problem in fading Gaussian MIMO wiretap channels. Sci Sin Inform, 2022, 52: 239–252 [马康宁, 徐寅飞, 邵硕, 等. 衰落高斯 MIMO 窃听信道下安全发送方案及其优化问题. 中国科学: 信息科学, 2022, 52: 239–252]

4 Bash B A, Goeckel D, Towsley D. Limits of reliable communication with low probability of detection on AWGN channels. IEEE J Sel Areas Commun, 2013, 31: 1921–1930

5 Bash B A, Goeckel D, Towsley D. LPD communication when the warden does not know when. In: Proceedings of IEEE International Symposium on Information Theory, Honolulu, 2014. 606–610

6 He B, Yan S, Zhou X, et al. Covert wireless communication with a Poisson field of interferers. IEEE Trans Wireless Commun, 2018, 17: 6005–6017

7 Shahzad K, Zhou X. Covert wireless communications under quasi-static fading with channel uncertainty. IEEE Trans Inform Forensic Secur, 2020, 16: 1104–1116

8 Yang W, Lu X, Yan S, et al. Age of information for short-packet covert communication. IEEE Wireless Commun Lett, 2021, 10: 1890–1894

9 Xu R, Guo D, Zhang B, et al. Finite blocklength covert communications with random selection of channel use. IEEE Wireless Commun Lett, 2021, 10: 2085–2089

10 Ma R, Yang W, Tao L, et al. Covert communications with randomly distributed wardens in the finite blocklength regime. IEEE Trans Veh Technol, 2021, 71: 533–544

11 Wang C, Chen X, An J, et al. Covert communication assisted by UAV-IRS. IEEE Trans Commun, 2023, 71: 357–369

12 Bash B A, Goeckel D, Towsley D, et al. Hiding information in noise: fundamental limits of covert wireless communication. IEEE Commun Mag, 2015, 53: 26–31

13 Yan S, Zhou X, Hu J, et al. Low probability of detection communication: opportunities and challenges. IEEE Wireless Commun, 2019, 26: 19–25

14 Cover T M, Thomas J A. Elements of Information Theory. 2nd ed. New Jersey: John Wiley & Sons, 2006

15 Kay S M. Fundamentals of Statistical Signal Processing (Volume II: Detection Theory). New Jersey: Prentice Hall, 1998

16 Feller W. An Introduction to Probability Theory and Its Applications (Volume II). 2nd ed. New York: John Wiley & Sons, 1971

17 Olver F W J, Lozier D W, Boisvert R F, et al. NIST Handbook of Mathematical Functions. New York: Cambridge University Press, 2010

18 Sobron I, Diniz P S R, Martins W A, et al. Energy detection technique for adaptive spectrum sensing. IEEE Trans Commun, 2015, 63: 617–627

19 Cormen T H, Leiserson C E, Rivest R L, et al. Introduction to Algorithms. 3rd ed. London: Massachusetts Institute of Technology Press, 2009

Low-to-no-power covert communication based on energy dispersion

Jianping AN, Haichuan DING* & Shuai WANG

School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081*, China*
* Corresponding author. E-mail: hcding@bit.edu.cn

Abstract With advances in computing and signal processing technologies, wireless communication systems are facing severe security threats, necessitating effective countermeasures. Unlike traditional secure communication schemes, covert communication should hide not only information content but also data transmission activity from adversaries. To this end, we propose an energy dispersion-based covert communication scheme to ensure that communication signal detection by adversaries has close-to-zero probability. The proposed scheme spreads the energy of transmitted signals throughout the whole parameter space to limit the signal detection capability of adversaries and improve the covertness of signal transmission. By defining the covertness of transmitted signals with respect to the adversaries' prior knowledge of parameter spaces, we study the modeling of energy dispersion-based covert communication systems and analyze their fundamental performance limitations. With these analytical results, we further investigate the impacts of adversaries' prior knowledge on the achievable throughput of covert communications. These results demonstrate that the dispersion of signal energy can degrade the performance of coherent signal detection so that the achievable throughput of the covert communication system does not necessarily follow the power-law decrease observed in existing work on the low probability of detection communications. This work lays the theoretical foundation for covert communication based on energy dispersion.

Keywords covert communications, spread-spectrum communications, prior knowledge, performance analysis