中国科学: 信息科学 2024 年 第 54 卷 第 8 期: 1940–1969
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
论文

基于扩维域能量弥散的隐蔽通信

安建平[1], 倪子涵[1], 王帅[1*], 潘高峰[1], 尹浩[2]

1. 北京理工大学网络空间安全学院, 北京 100081
2. 军事科学院, 北京 100091
* 通信作者. E-mail: swang@bit.edu.cn

收稿日期: 2024–01–09; 修回日期: 2024–02–27; 接受日期: 2024–03–18; 网络出版日期: 2024–08–08

国家重点研发计划项目 (批准号: 2021YFC3320200) 资助

摘要 无线通信技术是现今蓬勃发展的数据时代不可或缺的重要信息传输手段之一, 而无线数据的安全性更是构建数据时代的磐石. 在某些特殊应用场景中, 发送方不但要保障信息内容的安全, 甚至要做到无线信号传输的行为不被侦收发现. 面对严峻的无线电侦收威胁, 传统的隐蔽通信手段是基于某一个或两个维域进行能量弥散以降低被侦测概率, 如基于扩频的码分多址接入技术将能量弥散到频域, 短时猝发技术将能量弥散在时域的多个离散时段, 短时猝发与跳频结合的技术将能量弥散在时、频两域. 本文首先回归无线传输过程中信号能量弥散的物理本质, 将隐蔽通信模型从能量在单维域弥散扩展至时 – 频 – 空的多维域能量弥散. 即利用此模型并借助无线电传播理论以及数字信号处理方法等工具对无线信号能量在时 – 频 – 空 3 个维域的能量弥散进行建模, 设计了侦听方面向时 – 频 – 空维域的能量检测器. 接下来, 在此多维域能量检测模型下, 推导了侦听方收集能量的表达式, 侦听方使用平均噪声能量作为门限的检测概率上下边界表达式, 以及在纽曼 – 皮尔逊 (Neyman-Pearson) 能量检测器下的检测概率上下边界表达式. 然后, 结合理论推导分析、归纳并证明了扩维域能量弥散以实现隐蔽通信思路的正确性. 然后, 结合仿真结果, 从博弈的角度讨论了在多维域能量检测模型下发送方隐蔽性存在的条件以及侦听方接收机的改进策略. 最后, 针对实际工程, 揭示了无线隐蔽通信系统隐蔽性与可靠性这一内生矛盾及相互作用机理, 进而给出了实现无线隐蔽传输的原理及技术途径.

关键词 隐蔽通信, 多维域能量弥散, 无线电传播理论, 无线电侦收, 纽曼 – 皮尔逊检验

1 引言

近年来, 随着无线通信技术的飞速发展, 人们对信息安全的要求也逐步提高. 要想让传输的信号不被第三方窃听, 就必须牺牲通信质量以获得信号的隐蔽性能. 在民用通信应用场景中, 人们往往关注其传输的信息内容是否被第三方窃取, 而对于其发送信号是否被第三方发现和截获关注较少. 因此,

引用格式: 安建平, 倪子涵, 王帅, 等. 基于扩维域能量弥散的隐蔽通信. 中国科学: 信息科学, 2024, 54: 1940–1969, doi: 10.1360/SSI-2024-0012
An J P, Ni Z H, Wang S, et al. Covert communications based on energy dispersion in extended dimensions (in Chinese). Sci Sin Inform, 2024, 54: 1940–1969, doi: 10.1360/SSI-2024-0012

© 2024《中国科学》杂志社

传统的信息安全往往从隐写术、编码、网络协议等角度入手以实现信息传输的安全 [1]. 但在一些特殊的运用场景中, 进行通信的双方不仅需要保护信息内容本身, 还需要保证信号在空间中传播行为的隐蔽性, 即不被第三方发现无线信号传播的存在.

目前, 安全通信的研究方向主要有: 物理层安全通信、低截获概率通信、低检测概率通信等, 其中, 作为低检测概率通信中一类典型技术流派, 隐蔽通信技术追求无线通信信号行为级的隐蔽, 即不让第三方察觉到其通信行为的存在, 被认为是实现安全通信重要技术途径之一. 在经典的隐蔽通信理论研究模型中, Alice 作为发送方向接收方 Bob 发送信息, 同时, Willie 为监听方侦听并判断 Alice-Bob 间通信行为是否存在 [2]. 很久以来, 实现无线通信行为隐蔽的常见技术方式之一就是扩频通信. 1941 年, George Antheil 和 Hedy Lamarr 基于自动钢琴的原理首次实现了扩频传输以躲避第三方的侦测. 扩频通信技术可以将信号的功率谱密度展宽压低并隐匿于噪声功率谱密度之下从而使得通信行为不被察觉 [3]. 长期以来人们一直使用扩频的手段进行通信以躲避敌方侦听, 但是关于隐蔽通信的理论研究却十分稀少. 直到 2013 年, Bash 等 [4] 在经典 Alice-Bob-Willie 的三点囚徒模型的基础上, 使用信息论的研究思路, 假设侦听方使用最佳检测器, 证明了在 n 次使用信道的情况下最多可以可靠隐蔽传输 $o(n)$ bit 的信息. Bash 等首次使用检验理论和 Kullback-Leibler 散度 (KL 散度) 对隐蔽通信系统的框架进行描述, 从此隐蔽通信相关的研究如雨后春笋般涌现. 在文献 [5] 中, Bash 等指出噪声为隐蔽通信提供了基本条件. 2016 年 Bash 等 [6] 提出侦听方对发送方发送信号时间的不确定性也为传输信号的隐蔽提供了条件. 此后, 学者们纷纷运用信息论的研究方法, 探索各种场景下隐蔽通信信道的可达容量, 成果频现. 在 Bash 提出的平方根定律的基础之上, Goeckel 等 [7] 证明了当 Willie 不能统计其信道噪声分布时, Alice 可以隐蔽地传输不超过 $\mathcal{O}(n)$ bit 的信息. Che 等 [8] 计算了二进制对称信道下的隐蔽通信容量, 随后 Wang 等 [9] 在此基础上给出了离散无记忆信道下的隐蔽通信容量. Bloch [10] 证明了当 Bob 信道条件优于 Willie 信道条件时, Alice 可以在不使用密钥的情况下 n 次可靠地传输 $\sqrt{n}$ bit 的信息. 文献 [11] 计算了传统信道反转功率控制 (channel inversion power control, CIPC) 方案和截断 CIPC 方案下的最优检测阈值和最小总错误概率的表达式, 并且在两种 CIPC 约束下实现了有效隐蔽吞吐量的最大化. 文献 [12] 证明了在确定预先发送信息数的情况下, 等功率分配是可以最大化互信息量的最优功率分配方案. 在不确定预先发送信息数的情况下, 文献 [12] 也提出了一种基于幂级数的功率分配方案以满足隐蔽约束条件.

在 Bash 等学者所提出的隐蔽通信的大框架下, 寄生信号、可重构智能表面 (reconfigurable intelligent surface, RIS) 辅助、随机接入等实现信号行为级隐蔽的方法也相继为学者所研究. 文献 [13] 尝试将秘密信息嵌入到广播信号中并研究了其隐蔽性能. 文献 [14] 研究了块衰落信道中时隙 ALOHA 随机接入的隐蔽通信系统的吞吐量. 文献 [15] 研究了非正交多址接入下的下行链路隐蔽通信的功率分配. 文献 [16] 中, 作者创造性地提出信息年龄 (age of information, AoI) 来衡量隐蔽通信系统传输信息的新鲜度, 随后文献 [17] 便计算了隐蔽 AoI 的新指标以描述短数据包通信的隐蔽性和及时性. 文献 [18] 利用优化的手段调整合适的传输时间和传输功率以最大化隐蔽通信系统的传输信息量. 在文献 [19] 中作者提出了一种新的基于 RIS 辅助的多入多出隐蔽通信系统, 解决了 RIS 连续和离散相位下通信系统最小信噪比最大化问题, 并优化了系统性能. 文献 [20] 在星地通信系统中使用 RIS 辅助并优化了最小隐蔽通信速率以提高信号质量.

以上关于隐蔽通信的研究均借助经典 Alice-Bob-Willie 三点模型以外的其他方或通信网络作为掩体辅助进行隐蔽通信. 然而, 在一些战时特殊场景中, 没有任何公共设施和信号可以当作掩体. 因此, 对于在无掩体设施/信号辅助等更一般的情况来说, 对基于经典 Alice-Bob-Willie 三点模型的隐蔽通信研究是更具有现实指导意见和参考价值的. 目前, 现有的基于经典 Alice-Bob-Willie 三点模型的隐蔽

通信的研究均只在频域扩展频谱以弥散能量或在时域进行分时发送以实现能量的弥散. 文献 [21] 提出一种使用随机跳频技术以躲避侦收方的新方案. 文献 [22, 23] 提出了使用时间跳变脉冲调制进行通信的思路. 文献 [6] 从数学手段证明了发送时间的不确定性可以提高通信的隐蔽性. 为了达到最优的隐蔽通信性, Alice-Bob 应该突破单一维域能量弥散的束缚, 采用多个维域联合进行能量弥散的隐蔽性能优化设计思想. 文献 [24] 在三点隐蔽通信模型的框架上提出了将信号能量弥散在时、频、空等多个维域以实现低零功率谱通信的策略. 文献 [25] 以侦听方的先验知识为基础, 系统性研究了通信信号隐蔽性度量的理论和方法, 得出了多维域隐蔽通信系统的性能边界. 对于 Willie 来说时 – 频 – 空 3 个维域是 3 个独立的维域, 只有 Willie 在 3 个维域的侦收窗口与 Alice 发送信号的 3 个维域窗口均有较高重叠度且搜集到足够多的信号能量时, 才能做出 Alice 与 Bob 正在进行通信与否的正确判断. 而文献 [24] 基于三点模型提出了将信号的能量弥散在时、频、空等多个维域, 从而实现低零功率通信的策略, 但在其模型中仍然假设 Willie 能够较为完美地接收 Alice 的信息符号并利用接收到的符号统计接收功率或接收能量.

然而, 在现实通信场景中, Willie 对 Alice 信号的侦收受到多重因素的影响. 例如, Willie 接收机开机时段与 Alice 发送时段重叠程度, Willie 频谱采集范围与 Alice 信号频谱重叠程度, Willie 所处位置的信号能量密度大小均会对 Willie 判断的准确性产生影响. 因此, 对 Willie 能量侦收的研究也不应局限在单维域上, 应扩展到时 – 频 – 空多维域的联合侦收, 甚至是时 – 频 – 空 – 码 4 个维域的联合侦收. 本文中, 在 Alice-Bob-Willie 的经典三点模型的基础上, 建立了扩维域信号弥散侦收模型, 并从博弈的角度讨论了 Alice 和 Willie 发送和侦收信号时的博弈思路, 提出了针对 Alice 和 Willie 的系统改进思路. 本文主要贡献总结如下.

• 突破传统单一维域能量弥散和侦收的束缚, 提出了扩维域联合能量弥散和侦收的思想, 并建立了扩维域能量弥散和侦收的系统模型.

• 分析了在时 – 频 – 空能量检测模型下, Willie 检测器时 – 频 – 空窗口与 Alice 信号的时 – 频 – 空窗口错位时, Willie 检测到的能量变化.

• 计算了当 Willie 将检测门限设置为噪声能量平均值时的检测概率表达式及其上下限, 并探究了此时 Alice 实现满足一定隐蔽条件下进行较低误码率通信的可能性.

• 计算了当 Willie 使用纽曼 – 皮尔逊 (Neyman-Pearson) 检验控制虚警概率 α 为某一定值时的 Willie 的检测概率表达式及其上下限, 并得出了虚警概率与检测概率不能同时优化的结论.

• 推导了当 Alice 分别采取从仅时域能量弥散到时、频、空、码四域能量弥散策略时 Willie 的能量全侦收概率, 并用 Willie 的能量全侦收概率作为 Alice 隐蔽性能的表征从而推演出了扩维域能量弥散隐蔽通信的指导原则.

• 揭示了无线通信系统隐蔽性和可靠性这一固有内生矛盾并辩证地指出了破解和平衡该矛盾的思路, 以及实现无线隐蔽通信原理和技术途径.

本文的第 2 节详细地介绍了时 – 频 – 空多维域能量弥散和侦收模型. 第 3 节本文对 Willie 的检测性能进行理论计算和分析, 主要包括 Willie 侦收到的信号能量以及 Willie 的检测概率以及其上下边界. 第 4 节本文给出了在 Willie 使用平均噪声能量作为检测门限时的 Alice 隐蔽传输条件. 通过第 3 和 4 节的理论推导, 第 5 节总结了多维域能量弥散通信模型中的博弈原则. 第 6 节结合理论推导, 分析、归纳并证明出了扩维域能量弥散隐蔽通信系统的设计指导原则. 第 7 节本文通过蒙特卡罗 (Monte Carlo) 仿真验证了扩维域能量弥散隐蔽通信设计思路的正确性, 并给出了更具体的改进方案. 针对在实际场景中无线隐蔽通信系统的设计与实现, 第 8 节首先阐述隐蔽性与可靠性这一对内在矛盾及相互作用机理, 然后给出实现无线隐蔽通信的原理及技术路线. 第 9 节对本文的主要结论进行了梳理和

总结.

2 系统模型

2.1 Alice-Bob-Willie 三点空间模型

本文考虑 Alice-Bob-Willie 经典三点隐蔽通信模型, 其中, Alice 企图使用幅移键控 (amplitude shift keying, ASK) 信号与 Bob 进行通信[1)], Willie 作为窃听方于某一时间段在空间中某一位置对某一段频率进行能量检测. Alice-Bob-Willie 的空间位置模型可以用图 1 来描述. 忽略 Alice 天线旁瓣的能量辐射, 假设 Alice 使用锥面波束[2)]与 Bob 进行通信, 波束角度为 θ_0, 波束覆盖范围以外的区域无法接收到任何信号能量, 设 Alice 与 Bob 之间的距离为 d_{AB}, Alice 天线的最大辐射方向始终指向 Bob, Bob 天线的最大辐射方向也始终指向 Alice. 以 Alice 为原点 O, Alice 与 Bob 的连线为 z 轴建立球坐标系, 设 Willie 与 Alice 的距离为 d_{AW}, Willie 与 Alice 的连线与 z 轴的夹角为 θ_{AW}, Bob 与 Alice 的距离为 d_{AB}. 需要注意的是, 由于 Alice 使用的是关于 z 轴旋转对称的锥面波束, 所以本文对 Willie, Bob 位置只使用距离 Alice 的距离和与 Alice 连线与 z 轴构成的夹角两个变量来描述.

2.2 功率空间衰减模型

Alice 的信号能量会弥散在空间的各个方位, 且能量弥散的具体分布与 Alice 天线的方向性函数有关. 假设 Willie 可以自行调整其天线的方向以使得其天线能在所在位置上以最大辐射方向上接收 Alice 发射信号的能量. 由于 Alice 的波束只在角度为 θ_0 的锥形空间内分布且锥形空间内各个方向的天线辐射强度相同, 所以辐射强度 U 在锥形空间内为常数, 那么 Alice 天线的方向性函数建模成

$$D_A(\theta,\varphi)=D_A(\theta)=\frac{2}{1-\cos\frac{\theta_0}{2}}, \tag{1}$$

其中, $0\leqslant\theta\leqslant\frac{\theta_0}{2}$, $0\leqslant\varphi<2\pi$.

根据文献 [26] 中的 Friss 公式, 当 Alice 给天线的馈线功率为 P_t 时, Alice 天线的方向性函数为 $D_A(\theta)$, Willie 在空间中任意一点处的天线接收到的功率为

$$P_{rW}=e_A\frac{P_tD_A(\theta_{AW})}{4\pi d_{AW}^2}\cdot e_WD_{W\max}\frac{\mathrm{c}^2}{4\pi f_c^2}, \tag{2}$$

其中, $e_A\in(0,1), e_W\in(0,1)$ 分别为 Alice, Willie 天线自身产生的能量损失系数, $D_{W\max}$ 为 Willie 天线的最大方向性系数, c 为真空中光速, f_c 为 Alice 发射信号的载波频率. 同理 Bob 在空间中任意一点处的天线接收到的功率为

$$P_{rB}=e_A\frac{P_tD_A(\theta_{AB})}{4\pi d_{AB}^2}\cdot e_BD_{B\max}\frac{\mathrm{c}^2}{4\pi f_c^2}, \tag{3}$$

其中, $D_{B\max}$ 为 Bob 天线的最大方向性系数.

1) 本文主要关注信号能量在时 – 频 – 空 3 个维域的弥散与侦收, 为了便于分析和计算选取 ASK 信号作为研究对象. 由于其他调制的信号可以看作两路正交的 ASK 信号叠加, 故本文的研究模型也可以推广至其他调制方式. 本小节所提出的模型适用于将能量弥散在时 – 频 – 空三维域的隐蔽通信系统的性能分析.

2) 若更改式 (1) 中的方向性函数表达式, 那么 Alice 天线旁瓣所辐射的能量也能被考虑进来. 但是由于 Willie 的位置对于 Alice 和 Bob 均是未知的, 若 Willie 在 Alice 天线的旁瓣辐射方向, Willie 极有可能几乎探测不到任何信号能量, 因此本文考虑空间上的最差情况, 将 Alice 的天线波束建模为锥面波束, 并假设 Willie 和 Bob 均在波束内部. 由于 Willie 到 Alice 的距离与 Bob 的有所不同, 故 Willie 和 Bob 接收的能量大小仍因其空间位置的不同而不同.

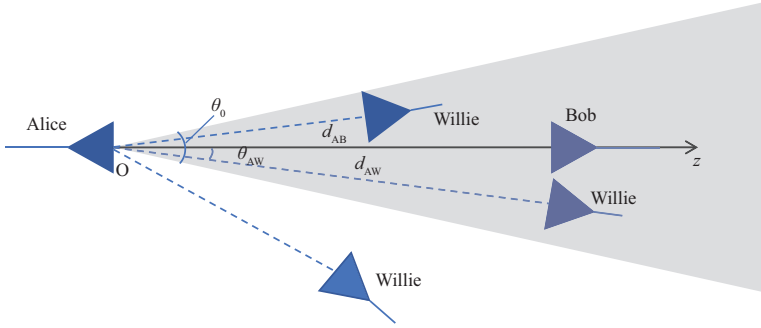

图 1　(网络版彩图) Alice-Bob-Willie 三点模型

Figure 1　(Color online) Alice-Bob-Willie three-point model

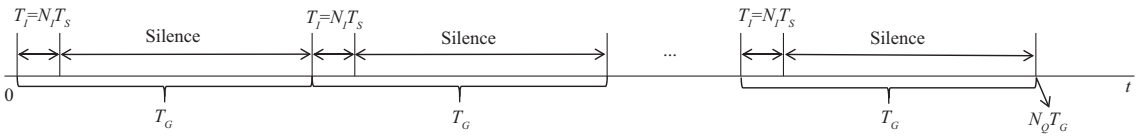

图 2　Alice 发射信号模型

Figure 2　Alice transmitting signal model

2.3　Alice 发射信号模型

假设 Alice 使用 ASK 的调制方式与 Bob 进行通信且为了防止被 Willie 发现, Alice 使用间隔发送信息的时域猝发 (时猝) 调制策略. 如图 2 所示, 假设 Alice 向 Bob 完整发送一次的秘密信息包含多个时猝加沉默的周期 T_G. Alice 在每个时猝加沉默周期 T_G 的前 T_I 秒使用 ASK 的调制方式进行时猝发送信息. 假设 Alice 的符号周期为 T_S, 每个时猝时间 T_I 包含 N_I 个码元符号, 即 $T_I = N_I T_S$. 为了简便, 假设每个时猝加沉默的周期 $T_G = N_G T_S$, 即假设时猝加沉默周期的持续时间 T_G 是码元周期的整数倍. 假设 Alice 向 Bob 完整发送秘密信息的总时长一共包含 N_Q 个 T_G.

这样, Alice 传输给发射天线前的信号可以表示为

$$s(t) = \sqrt{\frac{P_t}{P_{\text{ave}}}} \sum_{n=0}^{N_G N_Q} A_n g(t - nT_S) \cos(2\pi f_c t) G_{T_G}(t), \tag{4}$$

其中, $P_{\text{ave}} = \frac{M^2-1}{6}$ 为信号单个码元的平均功率, $g(t) = 1\ (0 \leqslant t < T_S)$ 为码元脉冲符号, P_t 为可控制的天线馈线功率, $A_n \in \{2i - M - 1 | i = 1, \ldots, M\}$ 为每个码元符号对应的 ASK 调制幅度, f_c 为载波频率, $G_{T_G}(t) = 1\ (kT_G \leqslant t \leqslant kT_G + T_I, k \in Z)$ 为时猝调制器.

2.4　Willie 能量检测模型

Alice 的信号传输到 Willie 后, 记信号第 1 个码元的起始时刻为 0 s. 假设 Willie 在 t_0 时刻打开接收机开始监测, 监测时长为 Δt s. 设时域限制函数 $G_{t_0,\Delta t}(t) = 1\ (t \in (t_0, t_0 + \Delta t))$. $G_{t_0,\Delta t}(t)$ 的作用就是 Willie 的接收时间区间在 Alice 信号的时域上的滑动截取, t_0 控制滑动窗口的位置, Δt 控制滑动窗口的大小. 由于 Alice 发送的是一个时猝信号, 故只要 Willie 的滑动窗口没有覆盖 Alice 时猝发送的周期, 那么 Willie 就无法接收到任何信号. Willie 的时域窗口模型可以由图 3 表示.

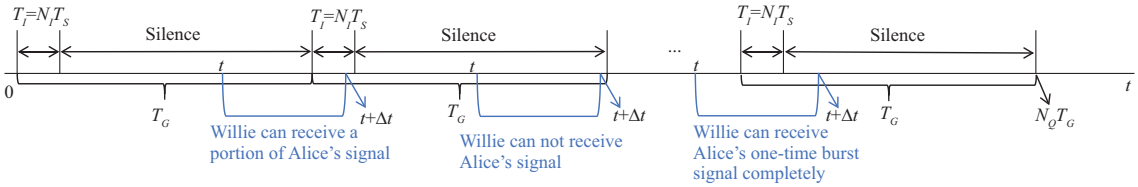

图 3 (网络版彩图) Willie 时域滑动检测窗口

Figure 3 (Color online) Willie time domain sliding detection window

这样, Willie 的天线接收到来自于 Alice 的信号可以表示为

$$r_1(t)=\sqrt{\frac{P_{rW}}{P_{\text{ave}}}}\sum_{n=0}^{N_G N_Q} A_n g(t-nT_S)\cos(2\pi f_c t)G_{T_G}(t)G_{t_0,\Delta t}(t). \tag{5}$$

Willie 还需要对自己想监测的频段进行截取, 截取频段相当于对信号 (5) 进行带通滤波. 假设在时间段 $(t_0, t_0+\Delta t)$ 的时间内, Willie 的监测频段为 $(f_W-\Delta f, f_W+\Delta f)$, 那么 Willie 最终接收到的信号只是信号 (5) 中的一个频段. 实际上, 滤波器的作用就是对 Willie 在时间段 $(t_0, t_0+\Delta t)$ 的信号进行特定频段提取. 滤波器相当于频域上的一个滑动窗口, 当窗口与 $(t_0, t_0+\Delta t)$ 时间段的信号频率有重叠时, Willie 就能采集到一部分 Alice 的能量. Willie 对频域的观测可以用图 4 来阐述.

因此, Willie 最终接收到的来自 Alice 的信号为

$$\begin{aligned} r_2(t)&=\sqrt{\frac{P_{rW}}{P_{\text{ave}}}}\sum_{n=0}^{N_G N_Q} A_n g(t-nT_S)\cos(2\pi f_c t)G_{T_G}(t)G_{t_0,\triangle t}(t)*\frac{2\sin(2\pi\triangle f t)\cos(2\pi f_W t)}{\pi t}\\ &=\sqrt{\frac{P_{rW}}{P_{\text{ave}}}}\sum_{n=0}^{N_G N_Q}\frac{2A_n}{\pi}\int_{\mathcal{T}_A\cap\mathcal{T}_W\cap\mathcal{T}_S}\frac{\cos(2\pi f_c\tau)\sin[2\pi\triangle f(t-\tau)]\cos[2\pi f_W(t-\tau)]}{t-\tau}\mathrm{d}\tau, \end{aligned} \tag{6}$$

其中, $\mathcal{T}_A=\{kT_G\leqslant\tau\leqslant kT_G+T_I\}$, $\mathcal{T}_W=\{t_0\leqslant\tau\leqslant t_0+\Delta t\}$, $\mathcal{T}_S=\{(n-1)T_S\leqslant\tau\leqslant nT_S\}$, $*$ 代表卷积运算.

故此, Willie 在位置 $(R_{AW}, \theta_{AW}, \varphi)$ 处, 在 $(t_0, t_0+\Delta t)$ 时间段, 观测 $(f_W-\Delta f, f_W+\Delta f)$ 的频谱获得的来自 Alice 信号的能量为

$$E_S=\int_{-\infty}^{+\infty} r_2^2(t)\mathrm{d}t. \tag{7}$$

在任何时刻 Willie 只要打开接收机都能接收到平稳随机高斯 (Gauss) 噪声, 由于 Willie 的检测频段为 $(f_W-\Delta f, f_W+\Delta f)$, 所以实际 Willie 接收到的是频率中心为 f_W, 带宽为 $2\Delta f$ 的窄带平稳高斯噪声.

设 Willie 处的噪声单边功率谱密度为 n_W. 可以得到 Willie 在位置 $(R_{AW}, \theta_{AW}, \varphi)$ 处, 在 $(t_0, t_0+\Delta t)$ 时间段, 观测 $(f_W-\Delta f, f_W+\Delta f)$ 的频谱获得的噪声能量为

$$E_N=\int_{t_0}^{t_0+\Delta t} n_{rW}^2(t)\mathrm{d}t, \tag{8}$$

其中, $n_{rW}(t)$ 为功率谱分布范围在 $(f_W-\Delta f, f_W+\Delta f)$ 的窄带高斯白噪声.

设 Willie 在位置 $(R_{AW}, \theta_{AW}, \varphi)$ 处, 在 $(t_0, t_0+\triangle t)$ 时间段, 观测 $(f_W-\Delta f, f_W+\triangle f)$ 的频谱获得的能量为 $E(t_0, \triangle t, f_W, \triangle f, R_{AW}, \theta_{AW})$. 根据统计理论 [27], Willie 的能量检测器可以建模为一个二

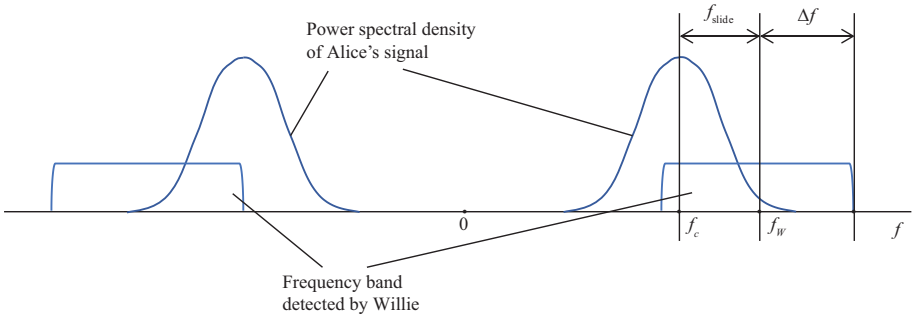

图 4 (网络版彩图) Willie 频域滑动检测窗口

Figure 4 (Color online) Willie frequency domain sliding detection window

元假设检验. 对于 Willie 有如下两种可能性:

$$\mathcal{H}_0: \text{Alice 正在发送信号},$$
$$\mathcal{H}_1: \text{Alice 没有发送信号}.$$

对于 Willie 来说其判决 Alice 是否在传输信息的根本条件是侦收能量的多寡, 故 Willie 的判决方式可以这样表征

$$\mathcal{D}_0: E\left(t_0, \triangle t, f_W, \triangle f, R_{AW}, \theta_{AW}\right) < E_{\text{th}},$$
$$\mathcal{D}_1: E\left(t_0, \triangle t, f_W, \triangle f, R_{AW}, \theta_{AW}\right) > E_{\text{th}},$$

其中, E_{th} 为检测门限.

因此, Willie 的检测概率可以表示为

$$P_D = \Pr\left\{E(t_0, \triangle t, f_W, \triangle f, R_{AW}, \theta_{AW}) > E_{\text{th}}\right\}. \tag{9}$$

3 Willie 检测性能分析

3.1 Willie 接收能量分析

Willie 判断 Alice 是否在传输信息的根本依据是其侦收到能量的多寡, Willie 侦收到的能量包含两部分, 一部分来自接收机噪声, 另一部分来自于 Alice 的传输信号. 因此本小节先推导在多维域检测模型下 Willie 侦收到来自 Alice 的能量表达式, 然后推导 Willie 的接收机噪声服从的分布.

定理1 Willie 在位置 $(R_{AW}, \theta_{AW}, \varphi)$ 处, 在 $(t_0, t_0 + \triangle t)$ 时间段, 观测 $(f_W - \triangle f, f_W + \triangle f)$ 的频谱获得的来自 Alice 的能量为

$$E_S = \frac{T_S^2}{2P_{\text{ave}}} \frac{D_A(\theta_{AW})}{D_A(\theta_{AB})} \cdot \left(\frac{d_{AB}}{d_{AW}}\right)^2 \cdot \frac{e_W}{e_B} \cdot \frac{D_{W\max}}{D_{B\max}} \frac{2n_B}{T_S} \gamma_{AB} \sum_{n_1 \in \mathcal{N}} \sum_{n_2 \in \mathcal{N}} A_{n_1} A_{n_2} I(n_1, n_2),$$

其中, $P_{\text{ave}} = \frac{M^2-1}{6}$ 为码元平均功率, n_B 为 Bob 的单边功率谱密度, γ_{AB} 为 Bob 的接收信噪比, $\mathcal{N}$ 代表 Willie 接收到的码元在原 Alice 发送信号中的码元位置集合, A_n 代表在位置 n 处的码元幅度, $I(n_1, n_2) = \int_{f_W - f_c - \Delta f}^{f_W - f_c + \Delta f} \cos\left[2\pi(n_1 - n_2)T_S f\right] \text{sinc}^2(T_S \pi f) \mathrm{d}f$.

证明 对频带信号进行带通滤波所得信号的能量与对其基带信号进行相应位置滤波所得信号的能量有一定的倍数关系. 设基带信号为

$$r_b(t)=\sqrt{\frac{P_{rW}}{P_{\text{ave}}}}\sum_{n=0}^{N_GN_Q}A_ng(t-nT_S)G_{T_G}(t)G_{t_0,\Delta t}(t). \tag{10}$$

对其使用中心频率为 f_W-f_c, 宽度为 $2\Delta f$ 的滤波器进行滤波, 滤波后的信号表达为

$$r_{b2}(t)=\sqrt{\frac{P_{rW}}{P_{\text{ave}}}}\left(\sum_{n=0}^{N_GN_Q}A_ng(t-nT_S)G_{T_G}(t)G_{t_0,\Delta t}(t)\right)*\frac{\sin(2\pi\Delta ft)}{\pi t}\mathrm{e}^{\mathrm{j}2\pi(f_W-f_c)t}, \tag{11}$$

其中, $*$ 代表卷积. 来自 Alice 的能量 E_S 可以表示为

$$\begin{aligned}
E_S&=2\int_{-\infty}^{+\infty}\left|\frac{1}{2}r_{b2}(t)\right|^2\mathrm{d}t\\
&=\frac{P_{rW}}{2P_{\text{ave}}}\int_{-\infty}^{+\infty}\left|\mathcal{F}\left\{\sum_{n=0}^{N_GN_Q}A_ng(t-nT_S)G_{T_G}(t)G_{t_0,\Delta t}(t)\right\}\times G_{f_W-f_c,\Delta f}(f)\right|^2\mathrm{d}f\\
&=\frac{P_{rW}}{2P_{\text{ave}}}\int_{-\infty}^{+\infty}\left|\sum_{n_1\in\mathcal{N}}A_{n_1}\mathrm{e}^{-\mathrm{j}2\pi f(n_1+\frac{1}{2})T_S}\right|^2\times\left[\frac{\sin(T_S\pi f)}{\pi f}\right]^2G_{f_W-f_c,\Delta f}(f)\mathrm{d}f\\
&=\frac{T_S^2P_{rW}}{2P_{\text{ave}}}\int_{-\infty}^{+\infty}\sum_{n_1\in\mathcal{N}}A_{n_1}\mathrm{e}^{-\mathrm{j}2\pi f(n_1+\frac{1}{2})T_S}\sum_{n_2\in\mathcal{N}}A_{n_2}\mathrm{e}^{\mathrm{j}2\pi f(n_2+\frac{1}{2})T_S}\times\mathrm{sinc}^2(T_S\pi f)G_{f_W-f_c,\Delta f}(f)\mathrm{d}f\\
&=\frac{T_S^2P_{rW}}{2P_{\text{ave}}}\int_{f_W-f_c-\Delta f}^{f_W-f_c+\Delta f}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}}A_{n_1}A_{n_2}\mathrm{e}^{-\mathrm{j}2\pi f(n_1-n_2)T_S}\mathrm{sinc}^2(T_S\pi f)\mathrm{d}f\\
&=\frac{T_S^2P_{rW}}{2P_{\text{ave}}}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}}A_{n_1}A_{n_2}\underbrace{\int_{f_W-f_c-\Delta f}^{f_W-f_c+\Delta f}\cos[2\pi(n_1-n_2)T_Sf]\mathrm{sinc}^2(T_S\pi f)\mathrm{d}f}_{I(n_1,n_2)}\\
&=\frac{T_S^2P_{rW}}{2P_{\text{ave}}}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}}A_{n_1}A_{n_2}I(n_1,n_2),
\end{aligned} \tag{12}$$

其中, $\mathcal{N}$ 代表 Willie 接收到的码元在原 Alice 发送信号中的码元位置的标号集合, A_n 代表在位置 n 处的码元幅度, $P_{\text{ave}}=\frac{M^2-1}{6}$ 为码元平均功率, $G_{f_W-f_c,\Delta f}(f)=1$ $(f_W-f_c-\Delta f<f<f_W-f_c+\Delta f)$, $\mathrm{sinc}(T_S\pi f)=\frac{\sin(T_S\pi f)}{T_S\pi f}$.

假设 Bob 的接收信噪比为 γ_{AB}, Bob 的单边噪声功率谱密度为 n_B, 那么 Bob 的接收功率可以表示为

$$P_{rB}=\frac{2n_B}{T_S}\gamma_{AB}. \tag{13}$$

结合式 (3) 和 (13), 可以得到 Bob 的接收信噪比为 γ_{AB} 时, Alice 的发射功率为

$$P_t=\frac{2n_B}{T_S}\gamma_{AB}\frac{4\pi d_{AB}^2\times4\pi f_c^2}{e_AD_A(\theta_{AB})e_BD_{B\max}c^2}. \tag{14}$$

根据式 (2), 可以得到 Willie 的接收功率 P_{rW} 为

$$P_{rW}=\frac{2n_B}{T_S}\gamma_{AB}\frac{4\pi d_{AB}^2\times4\pi f_c^2}{e_AD_A(\theta_{AB})e_BD_{B\max}c^2}\times e_A\frac{D_A(\theta_{AW})}{4\pi d_{AW}^2}\cdot e_WD_{W\max}\frac{c^2}{4\pi f_c^2}$$

$$= \frac{D_A(\theta_{AW})}{D_A(\theta_{AB})} \cdot \left(\frac{d_{AB}}{d_{AW}}\right)^2 \cdot \frac{e_W}{e_B} \cdot \frac{D_{W\max}}{D_{B\max}} \frac{2n_B}{T_S} \gamma_{AB}. \tag{15}$$

将式 (15) 带入式 (12), 可以得到 Willie 在位置 $(R_{AW}, \theta_{AW}, \varphi)$ 处, 在 $(t_0, t_0 + \triangle t)$ 时间段, 观测 $(f_W - \triangle f, f_W + \triangle f)$ 的频谱获得的来自 Alice 的能量为

$$E_S = \frac{T_S^2}{2P_{\text{ave}}} \frac{D_A(\theta_{AW})}{D_A(\theta_{AB})} \cdot \left(\frac{d_{AB}}{d_{AW}}\right)^2 \cdot \frac{e_W}{e_B} \cdot \frac{D_{W\max}}{D_{B\max}} \frac{2n_B}{T_S} \gamma_{AB} \sum_{n_1 \in \mathcal{N}} \sum_{n_2 \in \mathcal{N}} A_{n_1} A_{n_2} I(n_1, n_2). \tag{16}$$

E_S 即 Willie 在多维域检测模型下侦收到的来自 Alice 的信号能量.

证明完毕!

下面继续推导 Willie 接收机侦收到的噪声能量的概率分布.

定理2 Willie 在位置 $(R_{AW}, \theta_{AW}, \varphi)$ 处, 在 $(t_0, t_0 + \triangle t)$ 时间段, 观测 $(f_W - \triangle f, f_W + \triangle f)$ 的频谱检测到的噪声能量近似服从均值为 $2n_W \Delta f \Delta t$, 方差为 $4\Delta t \Delta f n_W^2$ 的高斯分布.

证明 单边功率谱密度为 n_W, 带宽为 $2\Delta f$, 中心频率为 f_W 的窄带平稳高斯随机噪声能量与双边功率谱密度为 n_W, 带宽为 $2\Delta f$ 的低通高斯随机噪声 $n_b(t)$ 的能量相同. 因此有

$$\int_{t_0}^{t_0+\Delta t} n_{rW}^2(t) \mathrm{d}t = \int_{t_0}^{t_0+\Delta t} n_b^2(t) \mathrm{d}t. \tag{17}$$

对式 (17) 进行以 $\frac{1}{2\Delta f}$ 为间隔抽样, 可以得到

$$\int_{t_0}^{t_0+\Delta t} n_b^2(t) \mathrm{d}t = \sum_{k=1}^{2\Delta f \Delta t} n_b^2 \left(t_0 + k\frac{1}{2\Delta f}\right) \frac{1}{2\Delta f}. \tag{18}$$

由于 $n_b(t)$ 为低通平稳高斯噪声, 因此对其以 $\frac{1}{2\Delta f}$ 为间隔抽样得到的各个随机变量是相互独立的. 可以计算式 (18) 均值为

$$\begin{aligned} E\left[\sum_{k=1}^{2\Delta f \Delta t} n_b^2 \left(t_0 + k\frac{1}{2\Delta f}\right) \frac{1}{2\Delta f}\right] &= \frac{1}{2\Delta f} \sum_{k=1}^{2\Delta f \Delta t} E\left[n_b^2 \left(t_0 + k\frac{1}{2\Delta f}\right)\right] \\ &= 2n_W \Delta f \Delta t. \end{aligned} \tag{19}$$

计算 (18) 的方差

$$\begin{aligned} D\left[\sum_{k=1}^{2\Delta f \Delta t} n_b^2 \left(t_0 + k\frac{1}{2\Delta f}\right) \frac{1}{2\Delta f}\right] &= \frac{1}{4\Delta f^2} \sum_{k=1}^{2\Delta f \Delta t} D\left[n_b^2 \left(t_0 + k\frac{1}{2\Delta f}\right)\right] \\ &= \frac{1}{4\Delta f^2} \sum_{k=1}^{2\Delta f \Delta t} \left\{E\left[n_b^4 \left(t_0 + k\frac{1}{2\Delta f}\right)\right] - E^2\left[n_b^2 \left(t_0 + k\frac{1}{2\Delta f}\right)\right]\right\} \\ &= 4\Delta t \Delta f n_W^2. \end{aligned} \tag{20}$$

根据中心极限定理, 多个独立同分布的随机变量的和近似服从高斯分布, 故 $\int_{t_0}^{t_0+\Delta t} n_{rW}^2(t) \mathrm{d}t$ 近似服从均值为 $2n_W \Delta f \Delta t$, 方差为 $4\Delta t \Delta f n_W^2$ 的高斯分布.

证明完毕!

3.2 Willie 检测概率分析

定理3 Willie 的检测门限 E_{th} 设置为平均噪声能量 $2n_W\Delta f\Delta t$ 且 Alice-Bob 链路的接收信噪比为 γ_{AB} 时, Willie 的检测概率满足不等式

$$\frac{1}{2} \leqslant P_D \leqslant \frac{1}{2} + \frac{1}{\sqrt{2\pi}}\varepsilon_{\max}, \tag{21}$$

其中, $\varepsilon_{\max} = \frac{(M-1)^2}{2\sqrt{\Delta t\Delta f}n_W}\frac{T_S^2}{2P_{\text{ave}}}\frac{D_A(\theta_{AW})}{D_A(\theta_{AB})} \times \left(\frac{d_{AB}}{d_{AW}}\right)^2 \cdot \frac{e_W}{e_B} \cdot \frac{D_{W\max}}{D_{B\max}}\frac{2n_B}{T_S}\gamma_{AB}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}}|I(n_1,n_2)|$.

证明 考虑一种特殊情况, 当 Alice 根本没发送信号或者说 Willie 完全没有抓到任何信号能量时一定有 $E_S = 0$. 此时 Willie 的检测概率一定降到最低, Willie 的检测概率可以表示为

$$P_D \geqslant \Pr\{E_N > 2n_W\triangle f\triangle t\} = \Pr\left\{\int_{t_0}^{t_0+\Delta t} n_{rW}^2(t)\mathrm{d}t > 2n_W\triangle f\triangle t\right\}. \tag{22}$$

根据定理 2, 式 (22) 可以被继续计算成

$$P_D \geqslant \Pr\left\{\frac{\int_{t_0}^{t_0+\Delta t} n_{rW}^2(t)\mathrm{d}t - 2n_W\triangle f\triangle t}{2\sqrt{\Delta t\Delta f}n_W} > 0\right\} = \frac{1}{2}. \tag{23}$$

因此, $P_D \geqslant \frac{1}{2}$. 根据式 (9), Willie 的检测概率可以进一步写成

$$\begin{aligned} P_D &= \Pr\{E_S + E_N > 2n_W\Delta f\Delta t\} \\ &= \Pr\left\{\frac{T_S^2}{2P_{\text{ave}}}\frac{D_A(\theta_{AW})}{D_A(\theta_{AB})} \cdot \left(\frac{d_{AB}}{d_{AW}}\right)^2 \cdot \frac{e_W}{e_B} \cdot \frac{D_{W\max}}{D_{B\max}}\frac{2n_B}{T_S}\right. \\ &\quad \left. \times \gamma_{AB}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}} A_{n_1}A_{n_2}I(n_1,n_2) + \int_{t_0}^{t_0+\Delta t} n_{rW}^2(t)\mathrm{d}t > 2n_W\Delta f\Delta t\right\}. \end{aligned} \tag{24}$$

设集合 $\mathcal{N}$ 的元素个数为 $|\mathcal{N}|$, 每一个 A_n 均有 M 个取值, 那么对于标号为 $\mathcal{N}$ 内元素的序列, 一共有 $M^{|\mathcal{N}|}$ 种取值方式, 设序列的第 k 种取值方式的具体数值为 $a_{k,n}$ $(n \in \mathcal{N})$. 假设每个符号的幅值相互独立且每个符号取不同幅值的概率均为 $\frac{1}{M}$, 根据全概率公式将式 (24) 进行拆解

$$\begin{aligned} P_D &= \sum_{k=1}^{M^{|\mathcal{N}|}} \Pr\left\{\frac{T_S^2}{2P_{\text{ave}}}\frac{D_A(\theta_{AW})}{D_A(\theta_{AB})} \cdot \left(\frac{d_{AB}}{d_{AW}}\right)^2 \cdot \frac{e_W}{e_B} \cdot \frac{D_{W\max}}{D_{B\max}}\frac{2n_B}{T_S}\gamma_{AB}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}} a_{k,n_1}a_{k,n_2}I(n_1,n_2)\right. \\ &\quad \left. + \int_{t_0}^{t_0+\Delta t} n_{rW}^2(t)\mathrm{d}t > 2n_W\Delta f\Delta t\right\} \times \prod_{n\in\mathcal{N}} \Pr\{A_n = a_{k,n}\} \\ &= \frac{1}{M^{|\mathcal{N}|}}\sum_{k=1}^{M^{|\mathcal{N}|}} \Pr\left\{\frac{T_S^2}{2P_{\text{ave}}}\frac{D_A(\theta_{AW})}{D_A(\theta_{AB})} \cdot \left(\frac{d_{AB}}{d_{AW}}\right)^2 \cdot \frac{e_W}{e_B} \cdot \frac{D_{W\max}}{D_{B\max}}\frac{2n_B}{T_S}\gamma_{AB}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}} a_{k,n_1}a_{k,n_2}I(n_1,n_2)\right. \\ &\quad \left. + \int_{t_0}^{t_0+\Delta t} n_{rW}^2(t)\mathrm{d}t > 2n_W\Delta f\Delta t\right\}. \end{aligned} \tag{25}$$

根据定理 2, 式 (25) 可以继续改写为

$$P_D = \frac{1}{M^{|\mathcal{N}|}}\sum_{k=1}^{M^{|\mathcal{N}|}} \Pr\left\{\frac{\int_{t_0}^{t_0+\Delta t} n_{rW}^2(t)\mathrm{d}t - 2n_W\Delta f\Delta t}{2\sqrt{\Delta t\Delta f}n_W}\right.$$

$$
\left.\begin{aligned}
&> \underbrace{-\frac{1}{2\sqrt{\Delta t\Delta f}n_W}\frac{T_S^2}{2P_{\rm ave}}\frac{D_A(\theta_{AW})}{D_A(\theta_{AB})}\times\left(\frac{d_{AB}}{d_{AW}}\right)^2\cdot\frac{e_W}{e_B}\cdot\frac{D_{W\max}}{D_{B\max}}\frac{2n_B}{T_S}\gamma_{AB}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}}a_{k,n_1}a_{k,n_2}I(n_1,n_2)}_{\varepsilon_k}\\
&=\frac{1}{M^{|\mathcal{N}|}}\sum_{k=1}^{M^{|\mathcal{N}|}}\left[\frac{1}{2}+\int_0^{\varepsilon_k}\frac{1}{\sqrt{2\pi}}{\rm e}^{-\frac{t^2}{2}}{\rm d}t\right]\\
&=\frac{1}{2}+\frac{1}{\sqrt{2\pi}M^{|\mathcal{N}|}}\sum_{k=1}^{M^{|\mathcal{N}|}}\int_0^{\varepsilon_k}{\rm e}^{-\frac{t^2}{2}}{\rm d}t.
\end{aligned}\right\}\tag{26}
$$

取 $a_{k,1},\ldots,a_{k,|\mathcal{N}|}=M-1$ 并且在 $I(n_1,n_2)$ 两侧加上绝对值, 将 ε_k 放大, 即取

$$
\varepsilon_{\max}=\frac{(M-1)^2}{2\sqrt{\Delta t\Delta f}n_W}\frac{T_S^2}{2P_{\rm ave}}\frac{D_A(\theta_{AW})}{D_A(\theta_{AB})}\times\left(\frac{d_{AB}}{d_{AW}}\right)^2\cdot\frac{e_W}{e_B}\cdot\frac{D_{W\max}}{D_{B\max}}\frac{2n_B}{T_S}\gamma_{AB}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}}|I(n_1,n_2)|,\tag{27}
$$

有 $\varepsilon_{\max}\geqslant\max_k\varepsilon_k$. 因此令 $\varepsilon_k=\varepsilon_{\max}$ 就可以将式 (26) 放大, 即

$$
P_D\leqslant\frac{1}{2}+\frac{1}{\sqrt{2\pi}}\int_0^{\varepsilon_{\max}}{\rm e}^{-\frac{t^2}{2}}{\rm d}t.\tag{28}
$$

设函数 $f(x)=\int_0^x{\rm e}^{-\frac{t^2}{2}}{\rm d}t\ (x>0)$. 因为当 $t>0$ 时, 必定有 ${\rm e}^{-\frac{t^2}{2}}<1$ 成立, 故一定有不等式

$$
\int_0^x{\rm e}^{-\frac{t^2}{2}}{\rm d}t<x\tag{29}
$$

成立. 因此, 式 (28) 可以再次放大成

$$
P_D\leqslant\frac{1}{2}+\frac{1}{\sqrt{2\pi}}\varepsilon_{\max}.\tag{30}
$$

综上所述, 当 Willie 使用噪声能量平均值作为检测门限时其检测概率 P_D 的上下限为 $\frac{1}{2}\leqslant P_D\leqslant\frac{1}{2}+\frac{1}{\sqrt{2\pi}}\varepsilon_{\max}$.

证明完毕!

根据定理 3, 可以发现当 Willie 将检测门限 $E_{\rm th}$ 设置为其接收机噪声平均功率时, Willie 的检测概率的下限可高达 0.5. Willie 的虚警概率 α 可以用下式计算:

$$
\begin{aligned}
\alpha&=\Pr\{\mathcal{D}_1|\mathcal{H}_0\}\\
&=\Pr\left\{\frac{E_S-2n_W\Delta f\Delta t}{2\sqrt{\Delta t\Delta t}n_W}\geqslant\frac{E_{\rm th}-2n_W\Delta f\Delta t}{2\sqrt{\Delta t\Delta t}n_W}\right\}\\
&=\Pr\left\{\frac{E_S-2n_W\Delta f\Delta t}{2\sqrt{\Delta t\Delta t}n_W}\geqslant 0\right\}\\
&=\frac{1}{2}.
\end{aligned}\tag{31}
$$

目前的通信系统常常使用直接序列扩频或跳频手段以逃避侦测方的侦察. 当 Alice 使用扩频通信时, 其信号的功率谱密度甚至会低于噪声功率谱密度. 若 Willie 将 $E_{\rm th}$ 设置为平均噪声功率, 则 Willie 可以较容易地检测到 Alice 的信号, 但与此同时带来的问题就是虚警概率 α 高达 $\frac{1}{2}$. 若提高 Willie 的检测门限 $E_{\rm th}$, 其虚警概率 α 就会相应的降低, 但同时其检测能力就会大幅度下降. 因此检测概率和虚警概率是一对矛盾. 若 Willie 不能承受高虚警率的代价, Willie 还有另外一种检测方式, 纽曼 – 皮尔逊检验, 即通过控制虚警概率 α 为某一较小的数值来设置检测门限 $E_{\rm th}$.

定理4 Willie 使用纽曼 – 皮尔逊检测, 即 Willie 限制其虚警概率为一较小的定值 α 且 Alice-Bob 链路的接收信噪比为 γ_{AB} 时, Willie 的检测概率满足不等式

$$\alpha \leqslant P_D \leqslant \alpha + \int_{\Phi^{-1}(1-\alpha)-\varepsilon_{\max}}^{\Phi^{-1}(1-\alpha)} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t, \tag{32}$$

其中, $\varepsilon_{\max} = \frac{(M-1)^2}{2\sqrt{\Delta t \Delta f} n_W} \frac{T_S^2}{2P_{\mathrm{ave}}} \frac{D_A(\theta_{AW})}{D_A(\theta_{AB})} \times \left(\frac{d_{AB}}{d_{AW}}\right)^2 \cdot \frac{e_W}{e_B} \cdot \frac{D_{W\max}}{D_{B\max}} \frac{2n_B}{T_S} \gamma_{AB} \sum_{n_1 \in \mathcal{N}} \sum_{n_2 \in \mathcal{N}} |I(n_1, n_2)|$, $\Phi(\cdot) = \int_{-\infty}^{\cdot} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t$, $\Phi^{-1}(\cdot)$ 为 $\Phi(\cdot)$ 的反函数.

证明 对于纽曼 – 皮尔逊检验, 其门限值 E_{th} 根据下式确定 [27]:

$$\begin{aligned}
\Pr\{\mathcal{D}_1|\mathcal{H}_0\} &= \Pr\left\{\frac{\int_{t_0}^{t_0+\Delta t} n_{rW}^2(t)\mathrm{d}t - 2n_W \Delta f \Delta t}{2\sqrt{\Delta t \Delta f} n_W} > \frac{E_{\mathrm{th}} - 2n_W \Delta f \Delta t}{2\sqrt{\Delta t \Delta f} n_W}\right\} \\
&= \Phi\left(-\frac{E_{\mathrm{th}} - 2n_W \Delta f \Delta t}{2\sqrt{\Delta t \Delta f} n_W}\right) \\
&= \alpha.
\end{aligned} \tag{33}$$

可以反解出门限值 E_{th} 为

$$E_{\mathrm{th}} = 2n_W \Delta f \Delta t + 2\sqrt{\Delta f \Delta t} n_W \Phi^{-1}(1-\alpha). \tag{34}$$

此时 Willie 的检测概率 P_D 为

$$\begin{aligned}
P_D =& \Pr\{\mathcal{D}_1|\mathcal{H}_1\} \\
=& \Pr\left\{\frac{T_S^2}{2P_{\mathrm{ave}}} \frac{D_A(\theta_{AW})}{D_A(\theta_{AB})} \cdot \left(\frac{d_{AB}}{d_{AW}}\right)^2 \cdot \frac{e_W}{e_B} \cdot \frac{D_{W\max}}{D_{B\max}} \frac{2n_B}{T_S} \gamma_{AB} \sum_{n_1 \in \mathcal{N}} \sum_{n_2 \in \mathcal{N}} A_{n_1} A_{n_2} I(n_1, n_2) \right. \\
&\left. + \int_{t_0}^{t_0+\Delta t} n_{rW}^2(t)\mathrm{d}t > E_{\mathrm{th}}\right\} \\
=& \frac{1}{M^{|\mathcal{N}|}} \sum_{k=1}^{M^{|\mathcal{N}|}} \Pr\left\{\frac{\int_{t_0}^{t_0+\Delta t} n_{rW}^2(t)\mathrm{d}t - 2n_W \Delta f \Delta t}{2\sqrt{\Delta f \Delta t} n_W} > \underbrace{\frac{E_{\mathrm{th}} - 2n_W \Delta f \Delta t}{2\sqrt{\Delta f \Delta t} n_W}}_{\Phi^{-1}(1-\alpha)}\right. \\
&\left. - \underbrace{\frac{1}{2\sqrt{\Delta f \Delta t} n_W} \frac{T_S^2}{2P_{\mathrm{ave}}} \frac{D_A(\theta_{AW})}{D_A(\theta_{AB})} \cdot \left(\frac{d_{AB}}{d_{AW}}\right)^2 \cdot \frac{e_W}{e_B} \cdot \frac{D_{W\max}}{D_{B\max}} \frac{2n_B}{T_S} \gamma_{AB} \sum_{n_1 \in \mathcal{N}} \sum_{n_2 \in \mathcal{N}} a_{k,n_1} a_{k,n_2} I(n_1, n_2)}_{\varepsilon_k}\right\} \\
=& \alpha + \frac{1}{M^{|\mathcal{N}|}} \sum_{k=1}^{M^{|\mathcal{N}|}} \int_{\Phi^{-1}(1-\alpha)-\varepsilon_k}^{\Phi^{-1}(1-\alpha)} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t.
\end{aligned} \tag{35}$$

考虑最差的情况, 即 Willie 侦测不到任何的来自 Alice 的信号能量, 故 $\varepsilon_k = 0$, 可以得到 Willie 检测概率的下限

$$P_D \geqslant \alpha. \tag{36}$$

观察式 (35) 中的积分项 $\int_{\Phi^{-1}(1-\alpha)-\varepsilon_k}^{\Phi^{-1}(1-\alpha)} \frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{t^2}{2}}\mathrm{d}t$, 可以发现 ε_k 越大, 积分的数值越大, 计算所得的 Willie 检测概率 P_D 也越大. 与定理 3 的推导方式类似, 仍然令 $a_{k,1},\ldots,a_{k,|\mathcal{N}|}=M-1$ 并且在 $I(n_1,n_2)$ 两侧加上绝对值, 可以得到取到所有 ε_k 的一致上限 $\varepsilon_{\max}$ 为

$$\varepsilon_{\max}=\frac{(M-1)^2}{2\sqrt{\Delta t\Delta f}n_W}\frac{T_S^2}{2P_{\mathrm{ave}}}\frac{D_A(\theta_{AW})}{D_A(\theta_{AB})}\times\left(\frac{d_{AB}}{d_{AW}}\right)^2\cdot\frac{e_W}{e_B}\cdot\frac{D_{W\max}}{D_{B\max}}\frac{2n_B}{T_S}\gamma_{AB}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}}|I(n_1,n_2)|. \tag{37}$$

把式 (35) 中所有的 ε_k 替换成 $\varepsilon_{\max}$, 可得检测概率的上限为

$$P_D\leqslant\alpha+\int_{\Phi^{-1}(1-\alpha)-\varepsilon_{\max}}^{\Phi^{-1}(1-\alpha)}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{t^2}{2}}\mathrm{d}t. \tag{38}$$

综上所述, 当 Willie 使用纽曼 – 皮尔逊将虚警概率限制为定值 α 时, 其检测概率 P_D 的上下限为 $\alpha\leqslant P_D\leqslant\alpha+\int_{\Phi^{-1}(1-\alpha)-\varepsilon_{\max}}^{\Phi^{-1}(1-\alpha)}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{t^2}{2}}\mathrm{d}t$.

证明完毕!

根据定理 4, 虚警概率 α 就是检测概率 P_D 的下限, 若保持其他条件不变, 提高虚警概率 α, 检测概率 P_D 必定整体上升.

4 Alice-Bob 隐蔽性能分析

结合第 3 节中所推导的 Willie 检测概率以及 Bob 的接收误码率, 即可讨论 Alice-Bob 之间能够进行隐蔽通信的条件.

定理5 若不等式

$$\frac{M^2-1}{3}\ln\frac{M-1}{3M\delta}<\epsilon\frac{\sqrt{2\pi\Delta t\Delta f}}{3T_S}\frac{M^2-1}{(M-1)^2}\frac{D_A(\theta_{AB})}{D_W(\theta_{AW})}\left(\frac{d_{AW}}{d_{AB}}\right)^2\frac{e_B}{e_W}\frac{D_{B\max}}{D_{W\max}}\frac{n_W}{n_B}\frac{1}{\sum\limits_{n_1\in\mathcal{N}}\sum\limits_{n_2\in\mathcal{N}}|I(n_1,n_2)|} \tag{39}$$

成立, 那么 Alice-Bob 一定可以设计出一个通信系统满足在 Willie 的检测概率不超过 $\frac{1}{2}+\epsilon$ 的条件下, 以低于 δ 的误码率进行通信.

证明 根据定理 3 , 若 Alice 想让 Willie 的检测概率小于 $\frac{1}{2}+\epsilon$, 那么必须满足条件

$$\frac{1}{\sqrt{2\pi}}\varepsilon_{\max}\leqslant\epsilon. \tag{40}$$

将式 (37) 带入式 (40), 可以得到满足 Willie 的检测概率不超过 $\frac{1}{2}+\epsilon$ 的 Alice-Bob 的接收信噪比 γ_{AB} 为

$$\gamma_{AB}\leqslant\epsilon\frac{\sqrt{2\pi\Delta t\Delta f}}{3T_S}\frac{M^2-1}{(M-1)^2}\frac{D_A(\theta_{AB})}{D_A(\theta_{AW})}\left(\frac{d_{AW}}{d_{AB}}\right)^2\frac{e_B}{e_W}\frac{D_{B\max}}{D_{W\max}}\frac{n_W}{n_B}\frac{1}{\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}}|I(n_1,n_2)|}. \tag{41}$$

由于 Alice-Bob 使用 ASK 调制信号进行通信, 故 Bob 的误码率可以表示为

$$P_e=\left(1-\frac{1}{M}\right)\mathrm{erfc}\left(\sqrt{\frac{3}{M^2-1}\gamma_{AB}}\right). \tag{42}$$

根据附录 A 的证明当 $\gamma_{AB} > \frac{2.05\left(M^2-1\right)}{3}$ 时, 有不等式

$$\operatorname{erfc}\left(\sqrt{\frac{3}{M^2-1}\gamma_{AB}}\right) \leqslant \frac{1}{3}\mathrm{e}^{-\frac{3}{M^2-1}\gamma_{AB}} \tag{43}$$

恒成立.

故 Bob 的误码率满足

$$P_e \leqslant \frac{1}{3}\left(1-\frac{1}{M}\right)\mathrm{e}^{-\frac{3}{M^2-1}\gamma_{AB}}. \tag{44}$$

根据式 (44), 若需要要求 Bob 的无码率不允许超过 δ, 那么只要 Alice-Bob 的接收信噪比满足条件

$$\frac{1}{3}\left(1-\frac{1}{M}\right)\mathrm{e}^{-\frac{3}{M^2-1}\gamma_{AB}} \leqslant \delta. \tag{45}$$

整理可以获得 Bob 误码率小于 δ 的充分条件为

$$\gamma_{AB} \geqslant \frac{M^2-1}{3}\ln\frac{M-1}{3M\delta}. \tag{46}$$

故只要式 (41) 和 (46) 存在交集, 则 Alice-Bob 一定可以设计出一个通信系统满足在 Willie 的检测概率不超过 $\frac{1}{2}+\epsilon$ 的条件下, 以低于 δ 的误码率进行通信.

证明完毕!

5 扩维域能量弥散系统中的博弈原则

5.1 Alice-Bob 实现隐蔽通信的系统设计原则

观察式 (35), 当 α 固定时, ε_k 越小, Willie 的检测概率就越小. 根据式 (16) 可以得到, 当 Alice 的信息序列 a_n 满足第 k 种排列时, Willie 能够侦收到的信号能量 $E_{S,k}$ 为

$$E_{S,k} = \frac{T_S^2}{2P_{\text{ave}}}\frac{D_A(\theta_{AW})}{D_A(\theta_{AB})}\cdot\left(\frac{d_{AB}}{d_{AW}}\right)^2\cdot\frac{e_W}{e_B}\cdot\frac{D_{W\max}}{D_{B\max}}\frac{2n_B}{T_S}\gamma_{AB}\sum_{n_1\in\mathcal{N}}\sum_{n_2\in\mathcal{N}}a_{k,n_1}a_{k,n_2}I(n_1,n_2). \tag{47}$$

结合式 (35) 中定义的 ε_k, 可以得到

$$\varepsilon_k = \frac{E_{S,k}}{2\sqrt{\Delta f\Delta t n_W}}. \tag{48}$$

因此, 减小 $E_{S,k}$ 即可减小 ε_k, 从而降低 Willie 的检测概率 P_D. 再次强调, $E_{S,k}$ 是当 Alice 发送信息序列 a_n 为 $M^{|\mathcal{N}|}$ 中排列中的第 k 个序列时, Willie 在位置 $(R_{AW},\theta_{AW},\varphi)$ 处, 在 $(t_0,t_0+\triangle t)$ 时间段, 观测 $(f_W-\triangle f, f_W+\triangle f)$ 的频谱获得的来自 Alice 的能量表征, 即, $E_{S,k}$ 是时、频、空所构成的高维空间中一处微元上所对应的能量数值. 从而, 可以得到以下两条结论.

- 实现 Alice-Bob 隐蔽通信的核心指导性原则是降低时、频、空所构成的高维空间中任意微元上所对应的能量数值, 即降低无线通信信号在 Willie 接收机处的接收能量 $E_{S,k}$.
- 时域猝发、扩展频谱以及提高天线方向性是分别在时、频、空 3 个维域中降低 Willie 侦收能量密度的有效手段.

5.2 Willie 侦听 Alice 的系统设计原则

根据定理 4, Willie 的检测概率 P_D 的下限为虚警概率 α. 若 Willie 提高虚警概率 α, 则其检测概率会得到显著的提升. 因此, 在 Willie 能够承受虚警的代价时, 可以通过提高虚警概率以提升系统的检测性能. 当 Willie 不能承受虚警的代价时, 通过提高虚警概率来提升检测性能是不可取的.

观察式 (35), 当 α 固定时, ε_k 越大, Willie 的检测概率就越大. 因此, Willie 提升检测概率的核心指导原则是提升 ε_k. 值得注意的是, 根据式 (48), Willie 不仅可以通过优化其多维域能量侦收窗口来提升能量密度 $E_{S,k}$ 以提升 ε_k 从而提升检测概率, 还可以通过改进接收机硬件、降低噪声能量以提高 ε_k 从而提高检测概率.

5.3 Alice 与 Willie 的博弈体现

虽然 Alice 与 Willie 均会优化 $E_{S,k}$, 但是其区别在于 Willie 需要提高 $E_{S,k}$ 而 Alice 需要降低 $E_{S,k}$. 所以, 两者的优化思路完全不同.

Alice 的优化目标是, 调整其发射机以及信号的参数想尽一切办法让 Willie 在位置 $(R_{AW}, \theta_{AW}, \varphi)$, 时间段 $(t_0, t_0+\triangle t)$ 以及频段 $(f_W-\triangle f, f_W+\triangle f)$ 上侦收的能量 $E_{S,k}$ 尽量的低, 甚至要求任意位置, 任意时段以及任意频谱上侦收的能量 $E_{S,k}$ 尽量的低. 而 Willie 的优化目标是, 调整其侦收的时 – 频 – 空多维域窗口, 以使得其在设置好的多维域窗口下侦收到的能量 $E_{S,k}$ 尽可能的高. 当 Alice 改变空间中能量分布时, Willie 必须调整侦收策略以获得更好的侦收效果, Alice 也要对 Willie 的侦收策略变化做出相应的防备. 因此 Alice 隐蔽通信与 Willie 侦测信号的矛盾归根结底是 Alice 信号的能量泄漏与 Willie 对信号能量捕捉的矛盾.

6 基于扩维域能量弥散的隐蔽通信原则

在前面的 4 个节中, 利用无线信号传播的本质 (即无线信号能量在空间中的扩散), 本文首先研究分析了 Alice-Bob-Willie 隐蔽通信模型中 ASK 调制信号在时频空三维域弥散时系统的 Alice-Bob 隐蔽传输性能和 Willie 检测性能, 然后总结归纳了扩维域能量弥散系统中的博弈原则. 接下来, 本节将进一步推演出基于扩维域能量弥散的隐蔽通信系统的一般性数学模型并给予证明.

6.1 基于扩维域能量弥散隐蔽通信系统的一般性数学模型

当 Alice 传输的隐蔽通信信号受到其多个参数的调制时, 设 Alice 的通信信号包含 N_s 个相互独立的正交参数向量 $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \ldots, \boldsymbol{x}_{N_s}$, 这些正交参数向量张成一个 $\sum_{k=1}^{N_s}\mathrm{Dim}(\boldsymbol{x}_k)$ 维度的正交向量空间, 记为 $\boldsymbol{S}$. 向量空间 $\boldsymbol{S}$ 中的任意一点 $\Phi=(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \ldots, \boldsymbol{x}_{N_s})$ 均与此通信信号在该点处微元上捕捉的某一能量数值相对应. 设 Alice 发送信息时, 在由 N_s 个正交的微元 $\Delta x_1, \Delta x_2, \ldots, \Delta x_{N_s}$ 上捕捉的能量数值为 $E(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{N_s})$, 其中, $\boldsymbol{x}_1=(\boldsymbol{x}_1, \Delta x_1), \ldots, \boldsymbol{x}_{N_s}=(\boldsymbol{x}_{N_s}, \Delta x_{N_s})$.

那么, 在这个 $\sum_{k=1}^{N_s}\mathrm{Dim}(\boldsymbol{x}_k)$ 维正交向量空间 $\boldsymbol{S}$ 中的某点 Φ 处的能量密度可以定义为

$$\mathcal{E}(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{N_s})=\lim_{\Delta x_{N_s}\to 0}\cdots\lim_{\Delta x_2\to 0}\lim_{\Delta x_1\to 0}\frac{E(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{N_s})}{\Delta x_1\Delta x_2\cdots\Delta x_{N_s}}. \tag{49}$$

当节点 $L\in\{\mathrm{Willie}, \mathrm{Bob}\}$. L 在各个维度上的观测集合分别为 $\chi_{L,1}, \chi_{L,2}, \ldots, \chi_{L,N_s}$. 利用上式给出的能量密度定义, 可求得节点 L 检测到的能量为

$$E_{D,L}=\int_{\chi_{L,N_s}}\cdots\int_{\chi_{L,2}}\int_{\chi_{L,1}}\mathcal{E}(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{N_s})\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_{N_s}. \tag{50}$$

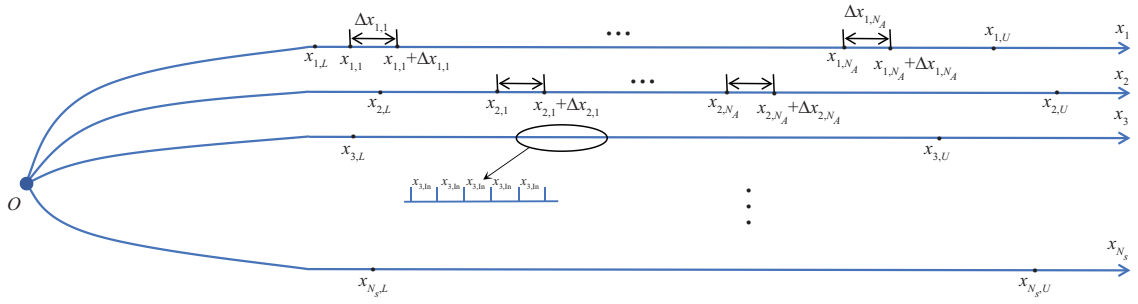

图 5　(网络版彩图) N_s **维向量空间**

Figure 5　(Color online) N_s-dimensional vector space

站在 Alice-Bob 的角度, 实现隐蔽通信的有效手段就是: 在保证 Alice-Bob 信息可靠传输的前提下 (即 Bob 收到的能量 $E_{D,\mathrm{Bob}}$ 满足 Alice-Bob 最低限的可靠传输), 在多维域中进行能量弥散, 尽可能地减小 Willie 侦收到的 Alice-Bob 通信信号能量 (即尽可能最小化 $E_{D,\mathrm{Willie}}$).

有鉴于此, 我们给出基于扩维域能量弥散隐蔽通信的核心思想是: 扩充 Alice-Bob 通信信号正交维域数, 将无线通信信号的能量在更高维域的正交空间中进行弥散. 从而, 增大 Willie 侦收 Alice-Bob 通信信号的难度, 降低 Willie 对 Alice-Bob 通信信号侦听概率. 即可用如下定理 6 来表示.

定理6　Alice 将其隐蔽通信信号弥散至的空间维数 N_s 越高, 其隐蔽性能越强.

证明　如图 5 所示, 设变量 $x_1, x_2, \ldots, x_{N_s}$ [3], 其张成一个 N_s 维向量空间记为 $\boldsymbol{S}_{N_s}$. Alice 通过调整信号的参数 $x_1, x_2, \ldots, x_{N_s}$, 将信号的能量弥散在空间 $\boldsymbol{S}_{N_s}$ 中. 假设 Willie 知晓 Alice 的能量在空间 $\boldsymbol{S}_{N_s}$ 的分布范围, 设分布范围为集合为

$$\mathcal{X}_1 = (x_{1,L}, x_{1,U}), \ldots, \mathcal{X}_{N_s} = (x_{N_s,L}, x_{N_s,U}). \tag{51}$$

若 Alice 进行 N_A 次信息传输, 设其通信信号的参量 $x_1, x_2, \ldots, x_{N_s}$ 实际分布的范围为

$$\begin{aligned}
\mathcal{O}_1 &= \{(x_{1,1}, x_{1,1}+\Delta x_{1,1}), (x_{1,2}, x_{1,2}+\Delta x_{1,2}) \cdots (x_{1,N_A}, x_{1,N_A}+\Delta x_{1,N_A})\}, \\
\mathcal{O}_2 &= \{(x_{2,1}, x_{2,1}+\Delta x_{2,1}), (x_{2,2}, x_{2,2}+\Delta x_{2,2}) \cdots (x_{2,N_A}, x_{2,N_A}+\Delta x_{2,N_A})\}, \\
&\vdots \\
\mathcal{O}_{N_s} &= \{(x_{N_s,1}, x_{N_s,1}+\Delta x_{N_s,1}), (x_{N_s,2}, x_{N_s,2}+\Delta x_{N_s,2}) \cdots (x_{N_s,N_A}, x_{N_s,N_A}+\Delta x_{N_s,N_A})\}.
\end{aligned} \tag{52}$$

将空间 $\boldsymbol{S}_1$ 的每一个维度分别以 $\Delta x_{1,\mathrm{In}}, \Delta x_{2,\mathrm{In}}, \ldots, \Delta x_{N_A,\mathrm{In}}$ 为间隔进行切片分段, 即 $\Delta x_{1,\mathrm{In}}$, $\Delta x_{2,\mathrm{In}}, \ldots, \Delta x_{N_A,\mathrm{In}}$ 分别为各个维度的最小间隔单元, 于是空间 $\boldsymbol{S}_1$ 便离散成了一个 N_s 维的 '网格', Willie 在 '网格' 中选取一些网格作为其侦听范围. 称 Willie 能够完整地将 Alice 信号弥散在各个维度的能量全部抓取的概率为 Willie 的能量全侦听概率, 并将 Willie 的能量全侦听概率记为 P_{N_s}, 可以计

3) 本小节的开头将此 N_s 个变量设成更一般化的向量. 这是因为像空间维域这样的维域本身就包含了 3 个正交的维度. 将空域看作 3 个正交维度的维域处理与将空域的 3 个维度拆分单独处理是等价的. 故这里为了简化计算, 将所有包含多个维度的维域均拆解为多个维度单独处理. 另外为了表达简单, 我们这里认为变量 $x_1, x_2, \ldots, x_{N_s}$ 均是连续的. 但应注意在实际物理通信信号中这 N_s 个变量不一定均为连续变量. 例如码域中包含两个变量, 一个是扩频码本的数量, 另一个是单个扩频码本中扩频码的数量. 但由于我们后续会将高维空间 '网格' 化, 因此即使是连续变量后续也会被离散化. 这便是我们将所有变量看作连续变量的原因.

算 P_{N_s} 为

$$\begin{aligned}P_{N_s} &= \frac{\sum_{j=1}^{N_A}\frac{\Delta x_{1,j}}{\Delta x_{1,\mathrm{In}}}\frac{\Delta x_{2,j}}{\Delta x_{2,\mathrm{In}}}\cdots\frac{\Delta x_{N_s,j}}{\Delta x_{N_s,\mathrm{In}}}}{\frac{x_{1,U}-x_{1,L}}{\Delta x_{1,\mathrm{In}}}\frac{x_{2,U}-x_{2,L}}{\Delta x_{2,\mathrm{In}}}\cdots\frac{x_{N_s,U}-x_{N_s,L}}{\Delta x_{N_s,\mathrm{In}}}}\\ &= \frac{\sum_{j=1}^{N_A}\Delta x_{1,j}\Delta x_{2,j}\cdots\Delta x_{N_s,j}}{(x_{1,U}-x_{1,L})(x_{2,U}-x_{2,L})\cdots(x_{N_s,U}-x_{N_s,L})}.\end{aligned} \tag{53}$$

当 Alice 将隐蔽通信信号的能量弥散到 $n-1$ $(n\geqslant 2)$ 个维域时, Willie 的能量全侦收概率为

$$P_{n-1}=\frac{\sum_{j=1}^{N_A}\Delta x_{1,j}\Delta x_{2,j}\cdots\Delta x_{n-1,j}}{(x_{1,U}-x_{1,L})(x_{2,U}-x_{2,L})\cdots(x_{n-1,U}-x_{n-1,L})}. \tag{54}$$

当 Alice 将隐蔽通信信号的能量弥散到 n 个维域时, Willie 的能量全侦收概率为

$$P_{n}=\frac{\sum_{j=1}^{N_A}\Delta x_{1,j}\Delta x_{2,j}\cdots\Delta x_{n-1,j}\Delta x_{n,j}}{(x_{1,U}-x_{1,L})(x_{2,U}-x_{2,L})\cdots(x_{n-1,U}-x_{n-1,L})(x_{n,U}-x_{n,L})}. \tag{55}$$

不等式

$$\sum_{j=1}^{N_A}(\Delta x_{1,j}\Delta x_{2,j}\cdots\Delta x_{n-1,j})\cdot\Delta x_{n,j}<\sum_{j=1}^{N_A}(\Delta x_{1,j}\Delta x_{2,j}\cdots\Delta x_{n-1,j})\cdot\sum_{j=1}^{N_A}\Delta x_{n,j} \tag{56}$$

恒成立. 故下面的不等式链一定恒成立

$$\begin{aligned}&\frac{\sum_{j=1}^{N_A}(\Delta x_{1,j}\Delta x_{2,j}\cdots\Delta x_{n-1,j})\cdot\Delta x_{n,j}}{(x_{1,U}-x_{1,L})(x_{2,U}-x_{2,L})\cdots(x_{n-1,U}-x_{n-1,L})(x_{n,U}-x_{n,L})}\\ &<\frac{\sum_{j=1}^{N_A}(\Delta x_{1,j}\Delta x_{2,j}\cdots\Delta x_{n-1,j})\cdot\sum_{j=1}^{N_A}\Delta x_{n,j}}{(x_{1,U}-x_{1,L})(x_{2,U}-x_{2,L})\cdots(x_{n-1,U}-x_{n-1,L})(x_{n,U}-x_{n,L})}\\ &<\frac{\sum_{j=1}^{N_A}\Delta x_{1,j}\Delta x_{2,j}\cdots\Delta x_{n-1,j}}{(x_{1,U}-x_{1,L})(x_{2,U}-x_{2,L})\cdots(x_{n-1,U}-x_{n-1,L})},\end{aligned} \tag{57}$$

即, $P_n<P_{n-1}$ $(n\geqslant 2)$. 即 Willie 的能量全侦收概率 P_n 关于向量空间维数 n 单调递减.

因此, 随着 Alice 将其信号能量所弥散的空间的维数 N_s 的增加, Willie 的能量全侦收概率降低, 即 Alice 的隐蔽性能增强.

证明完毕!

6.2 基于扩维域能量弥散隐蔽通信系统的物理模型实例

6.1 小节已经建立了扩维域能量弥散隐蔽通信系统的一般数学模型, 并在定理 6 中证明了 Alice 信号能量所弥散的空间维度越高, 其隐蔽性能越强. 由于定理 6 是抽象化的数学结论, 不具有时、频、空、码的物理意义, 因此接下来, 将给出当 Alice 将信号能量所弥散的空间由时域空间逐渐扩维域至时、频、空、码高维度空间时, Alice 的隐蔽性能逐渐增强的实例[4]. 值得强调的是本文中的维度和维域是不同的概念. 维度是指描述高维空间的变量, 是数学概念. 而维域是指如时、频、空、码这样的实体化的物理概念. 一个维域可能包含多个维度, 例如: 空间维域包含 θ, φ, r 3 个维度. 另外, 在现实世界对信号进行扩维域时, 新维域所包含的维度不一定是连续的变量, 码域即是如此.

4) 本小节所建立的扩维域能量弥散隐蔽通信模型是高度抽象化的模型, 选取合适的参数集即可建立针对跳时, 跳频, 直扩甚至更多种技术相结合的隐蔽分析模型.

当直接序列扩频技术被应用于隐蔽通信后, 描述信号参数的向量空间便增加了新的维域, 即码域. 下面我们以当信号能量从时、频、空构成的高维空间弥散扩维域至时、频、空、码构成的更高维度空间时的隐蔽通信性能变化为例来验证本文前面提出的基于扩维域能量弥散隐蔽通信原则的正确性.

假设 Willie 知晓 Alice 发送隐蔽信息的时间、频率、空间以及码本的范围, 故我们将 Alice 的可发送总时间集, 可发送总频段集, 可辐射空间区域以及可发送总码本集合设置为[5)]

$$
\begin{aligned}
&\mathcal{T}=(t_L,t_U),\\
&\mathcal{F}=(f_L,f_U),\\
&\mathcal{S}=\{(\theta,\varphi,r)|0\leqslant r\leqslant r_0\},\\
&\mathcal{C}=\left\{\begin{matrix} c_{1,1} & c_{1,2} & \cdots & c_{1,Q_c}\\ c_{2,1} & c_{2,2} & \cdots & c_{2,Q_c}\\ \vdots & \vdots & \ddots & \vdots\\ c_{M_c,1} & c_{M_c,2} & \cdots & c_{M_c,Q_c}\end{matrix}\right\}=\{\mathcal{C}_1,\mathcal{C}_2,\ldots,\mathcal{C}_{M_c}\},
\end{aligned}
\tag{58}
$$

其中, r_0 为 Alice 信号能量的最大可侦测半径其数值与接收机的性能有关, $\mathcal{C}_k$ $(k=1,\ldots,M_c)$ 为包含 Q_c 个扩频码的集合, $\mathcal{C}_k$ 中所有码的码长为 $N_{c,k}$. 设时间变量 $t\in\mathcal{T}$, 频率变量 $f\in\mathcal{F}$, 空间位置变量 $(\theta,\varphi,r)\in\mathcal{S}$, 码域变量 $c_{k,n}\in\mathcal{C}$ 代表第 k 个码本中的第 n 个扩频码.

于是, 变量 t, f, θ, φ, r, k, n 张成了一个七维有限空间, 该七维有限空间内的能量分布为 Alice 发送信号的策略所决定. 将 Alice 进行 N_A 次发送短时猝发信号的时、频、空、码参数用向量表征, 那么 Alice 发送信号的时间向量、频率向量、辐射区域向量以及扩频码向量分别可以表示为

$$
\begin{aligned}
&\mathcal{T}_A=[(t_1,t_1+\Delta t_1),(t_2,t_2+\Delta t_2),\ldots,(t_{N_A},t_{N_A}+\Delta t_{N_A})],\\
&\mathcal{F}_A=[\mathcal{F}_1,\ldots,\mathcal{F}_{N_A}],\\
&\mathcal{S}_A=[S_{\mathrm{rad}},\ldots,S_{\mathrm{rad}}],\\
&\mathcal{C}_A=[\mathcal{C}_1,\ldots,\mathcal{C}_{N_A}],
\end{aligned}
\tag{59}
$$

其中, N_A 为 Alice 进行时域猝发的次数, $\mathcal{F}_1,\ldots,\mathcal{F}_{N_A}$ 分别为每次时猝发送时所用的频率集合, $S_{\mathrm{rad}}=\left\{(\theta,\varphi,r)|-\frac{\theta_0}{2}\leqslant\theta\leqslant\frac{\theta_0}{2},0\leqslant r\leqslant r_0\right\}$ 为 Alice 天线的辐射区域且每次时猝发送的辐射区域完全相同, $\mathcal{C}_1,\ldots,\mathcal{C}_{N_A}$ 分别为每次时猝发送使用的来自单一扩频码本的扩频码集合.

值得注意的是由于 Alice 可以使用多载波/跳频的策略, 因此 N_A 个频率集合允许存在交集且每一个集合不一定只包含一个频段. 下面计算当 Alice 分别将能量弥散到单个至多个维域时对应的 Willie 全侦收概率 P_v. 若 Alice 只采取时域猝发的隐蔽策略, 以每一个符号符号周期 T_S 为网格宽度, 那么 Willie 的能量全侦收概率 P_1 可以表示为

$$
P_1=\frac{\sum_{j=1}^{N_A}\frac{\Delta t_j}{T_S}}{\frac{t_U-t_L}{T_S}}=\frac{\sum_{j=1}^{N_A}\Delta t_j}{t_U-t_L}.
\tag{60}
$$

5) 实际上 Alice 发送信号的能量弥散于时、频、空、码构成的高维空间内. 我们分别以时域和频域上的能量分布为例, 解释能量的分布. 若 Alice 选择持续慢速地发送信号, 那么当只观察时域时, 能量仅分布在时域轴上一段较长的区间. 若 Alice 选择随机时猝发送信号, 那么当只观察频域时, 能量会在时域轴上一系列极窄区间上离散分布. 若 Alice 采用直接序列扩频, 那么当只观察频域时, 能量仅仅分布在频域轴上一段较长的区间. 若 Alice 采用跳频, 那么当只观察频域时, 能量会在频率轴上一系列区间上离散分布.

表 1 Willie 接收来自 Alice 能量的仿真参数

Table 1 Simulation parameters of Willie receiving energy from Alice

M	T_S (s)	T_I (s)	T_G (s)	N_Q	f_c (MHz)	f_W (MHz)	Δf (Hz)	d_{AW} (km)	P_t (W)
4	0.001	0.5	5	10	1.6	1.6	1000	2000	0.1

若 Alice 采取时域猝发 + 多载波/跳频的隐蔽策略, 以每一个符号符号周期 R_S 为时域网格宽度, $\Delta f_{\rm In}$ 为频域网格宽度, 那么 Willie 的能量全侦收概率 P_2 可以表示为

$$P_2=\frac{\sum_{j=1}^{N_A}\frac{\Delta t_j}{T_S}\frac{|\mathcal{F}_j|}{\Delta f_{\rm In}}}{\frac{t_U-t_L}{T_S}\frac{f_U-f_L}{\Delta f_{\rm In}}}=\frac{\sum_{j=1}^{N_A}\Delta t_j|\mathcal{F}_j|}{(t_U-t_L)(f_U-f_L)}, \tag{61}$$

其中, $|\mathcal{F}_j|$ 为 Alice 第 j 次时域猝发所用频率总宽度.

若 Alice 采取时域猝发 + 多载波/跳频 + 波束赋形的策略, Willie 的能量全侦收概率 P_3 可以表示为

$$P_3=\frac{\sum_{j=1}^{N_A}\frac{\Delta t_j}{T_S}\frac{|\mathcal{F}_j|}{\Delta f_{\rm In}}\theta_0}{\frac{t_U-t_L}{T_S}\frac{f_U-f_L}{\Delta f_{\rm In}}2\pi}=\frac{\theta_0\sum_{j=1}^{N_A}\Delta t_j|\mathcal{F}_j|}{2\pi(t_U-t_L)(f_U-f_L)}. \tag{62}$$

若 Alice 采取时域猝发 + 多载波/跳频 + 波束赋形 + 直接序列扩频的策略, Willie 的能量全侦收概率 P_4 可以表示为

$$P_4=\frac{\sum_{j=1}^{N_A}\frac{\Delta t_j}{T_S}\frac{|\mathcal{F}_j|}{\Delta f_{\rm In}}\theta_0}{\frac{t_U-t_L}{T_S}\frac{f_U-f_L}{\Delta f_{\rm In}}2\pi Q_cM_c}=\frac{\theta_0\sum_{j=1}^{N_A}\Delta t_j|\mathcal{F}_j|}{2\pi(t_U-t_L)(f_U-f_L)Q_cM_c}. \tag{63}$$

由于 $\sum_{j=1}^{N_A}\Delta t_j\sum_{j=1}^{N_A}|\mathcal{F}_j|>\sum_{j=1}^{N_A}\Delta t_j|\mathcal{F}_j|$, 因此有不等式

$$P_2=\frac{\sum_{j=1}^{N_A}\Delta t_j|\mathcal{F}_j|}{(t_U-t_L)(f_U-f_L)}<\frac{\sum_{j=1}^{N_A}\Delta t_j\sum_{j=1}^{N_A}|\mathcal{F}_j|}{(t_U-t_L)(f_U-f_L)}<\frac{\sum_{j=1}^{N_A}\Delta t_j}{t_U-t_L}=P_1 \tag{64}$$

成立.

那么, 有不等式链

$$P_1>P_2>P_3>P_4 \tag{65}$$

成立.

显然, Alice 依次将能量弥散至从仅有时间的单维域空间扩展至时、频、空、码的多维域空间的过程中, 隐蔽性能逐渐提升.

7 仿真结果与讨论

7.1 Willie 对来自 Alice 信号能量的侦收

本小节利用蒙特卡罗仿真的手段对 Willie 侦收来自 Alice 信号的能量多寡进行分析. 若不做特殊说明, 本小节设置仿真参数的数值如表 1 所示.

分别取时间窗口长度 $\Delta t=0.1,0.4,0.8,1$, 滑动窗口起点从 $t_0=0$ 到 $t_0=12$ 得到 Willie 检测到的来自 Alice 的信号能量变化如图 6(a) 所示. 图 6(a) 中窗口的宽度均较小, 当 Willie 的时域窗口滑动

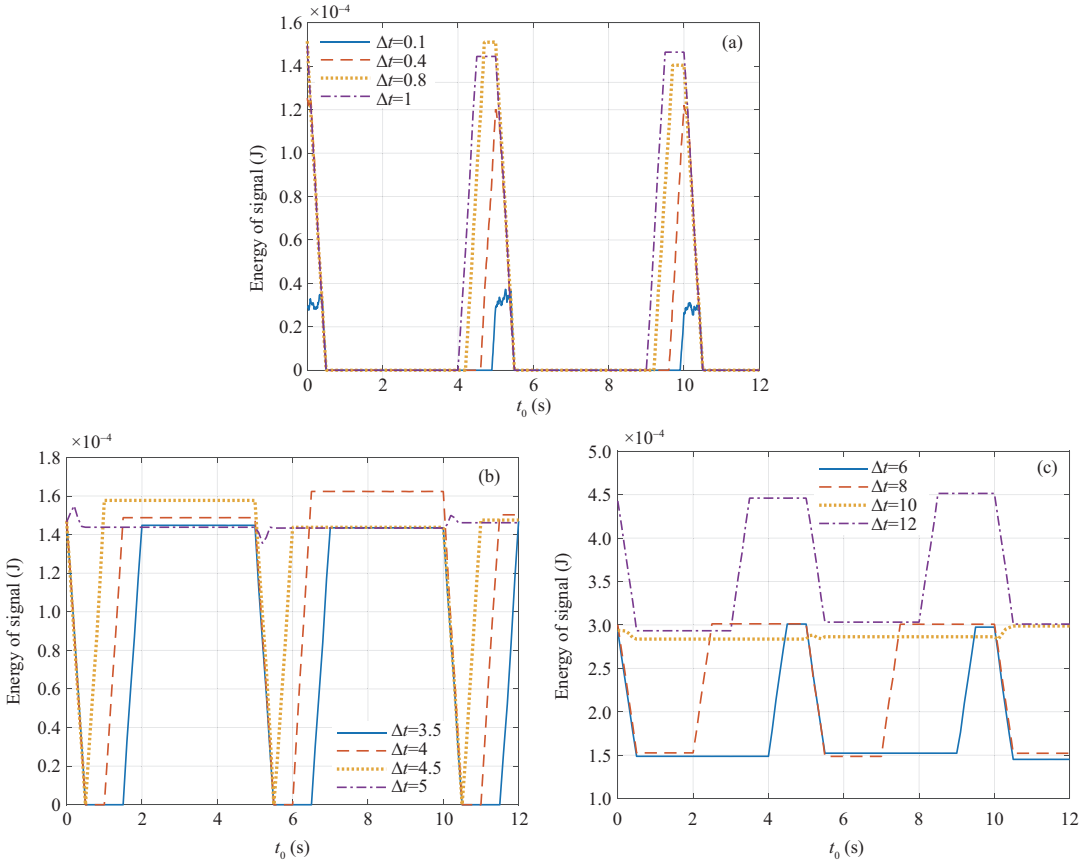

图 6 (网络版彩图) 当 (a) $\Delta t = 0.1, 0.4, 0.8, 1$, (b) $\Delta t = 3.5, 4, 4.5, 5$, (c) $\Delta t = 6, 8, 10, 12$ 时滑动时间窗口得到的能量变化

Figure 6 (Color online) Energy change sliding the time window when (a) $\Delta t = 0.1, 0.4, 0.8, 1$, (b) $\Delta t = 3.5, 4, 4.5, 5$, and (c) $\Delta t = 6, 8, 10, 12$

时, 其检测到的能量展现为时有时无的周期性变化. Willie 使用较小尺度的时域窗口侦收 Alice 能量时, 容易因时间窗口与 Alice 信息发送窗口错位而侦收不到任何信号能量.

分别取时间窗口长度 $\Delta t = 3.5, 4, 4.5, 5$, 滑动窗口起点从 $t_0 = 0$ 到 $t_0 = 12$ 得到 Willie 检测到的来自 Alice 的信号能量变化如图 6(b). 当时域检测窗口宽度与 Alice 发送信号的时猝加沉默周期 T_G 尺度相仿时, 窗口位置对 Willie 侦收到的能量的影响较小.

分别取时间窗口长度 $\Delta t = 6, 8, 10, 12$, 滑动窗口起点从 $t_0 = 0$ 到 $t_0 = 12$ 的到 Willie 检测到的来自 Alice 的信号能量变化如图 6(c). 当 Willie 时域滑动窗口的宽度较大于 T_G 大时, 无论如何滑动窗口, 总能接收到部分能量, 但是能量随时间呈现忽高忽低的周期性变化. 当检测窗口为 T_G 的整数倍时, 检测的能量较为稳定.

定义 $f_{\text{slide}} = f_W - f_c$. 改变 $P_t = 0.8\text{W}$. 分别取 $\Delta t = 0.3, 2.5, 7.5$ 3 个时间窗口进行观测, 并滑动频率窗口使得 f_{slide} 从 -2000 Hz 变动到 2000 Hz, 可以得到 Willie 接收到能量的曲线如图 7(a). 限制时间窗口的宽度为 $\Delta t = 7.5$ 分别取发射功率 $P_t = 0.1, 0.4, 0.8$ W 进行观测, 并滑动频率窗口使得 f_{slide} 从 -2000 Hz 变动到 2000 Hz, 可以得到 Willie 接收到能量的曲线如图 7(b) 所示. 从图 7(a) 和 (b) 可以看出, 只有 Willie 的接收中心频域 f_W 与 Alice 信号载波频率 f_c 近似相等时才能接收到大部分能

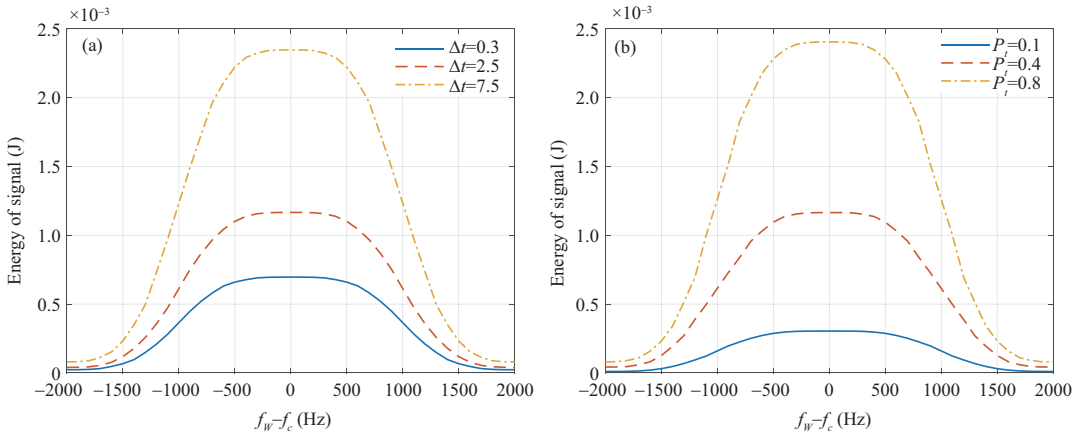

图 7 (网络版彩图) 当 (a) $\Delta t = 0.3, 2.5, 7.5$ 和 (b) $P_t = 0.1, 0.4, 0.8$ 时滑动频率窗口得到的能量变化

Figure 7 (Color online) Energy change sliding frequency window when (a) $\Delta t = 0.3, 2.5, 7.5$ and (b) $P_t = 0.1, 0.4, 0.8$

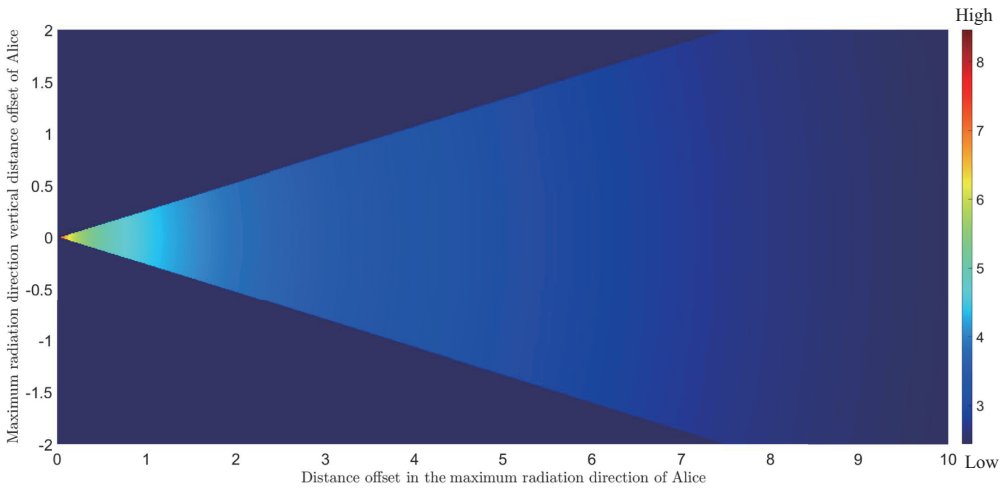

图 8 (网络版彩图) 当 Willie 的位置变化时其接收到的能量分布图

Figure 8 (Color online) Energy distribution received by Willie in changing position

量, 当 $f_{\text{slide}} = f_W - f_c$ 比较大时, Willie 侦测到的能量迅速降低.

固定参数 $\Delta t = 1$, $f_{\text{slide}} = 0$, $P_t = 1$, 而其他参数的设值均与表 1 相同. 设定 Alice 的天线锥形波束的有效覆盖角度为 $\frac{\pi}{6}$. 以 Alice 为原点, Alice 天线的最大辐射方向为轴, 假设 Willie 与 Alice 的距离为 d_{AW}, Willie 与 Alice 连线与轴的夹角为 φ_{AW}, 即 Willie 的位置坐标为 (d_{AW}, φ_{AW}), 当 Willie 处于空间不同位置时, 其检测到的信号能量图可以定性表示为图 8. 可以看出, 当 Alice 使用锥形波束时, Willie 若站在锥形波束以外, 他接收不到任何的能量; 若 Willie 站在波束以内, 他接收到的能量随着距离 d_{AW} 增大而减小.

7.2 Willie 检测概率与 Bob 的误码率

本小节结合定理 3 和 5 计算出当 Bob 的误码率满足 $P_e \leqslant \delta$ 且同时 Willie 的检测概率满足 $P_D \leqslant \frac{1}{2} + \epsilon$ 的限制条件, 并在此限制条件下改变不同参数的取值以分析 Alice-Willie-Bob 三方的系统

表 2 Willie 接收来自 Alice 能量的仿真参数

Table 2 Simulation parameters of Willie receiving energy from Alice

T_S (s)	T_I (s)	T_G (s)	N_Q	f_c (MHz)	f_{slide} (Hz)	Δf (Hz)	d_{AW} (m)	d_{AB} (m)
0.001	0.5	8	10	600	2000	1000	8500	800
M	$\frac{n_W}{n_B}$	$\frac{e_W}{e_B}$	$\frac{D_{B\max}}{D_{W\max}}$	θ_0	θ_{AB}	θ_{AW}	t_0 (s)	Δt (s)
4	2.2	0.6	4	$\frac{\pi}{6}$	0	$\frac{\pi}{13}$	0	2

参数对 Willie 和 Bob 的检测性能和误码性能的影响. 假设 Bob 能够忍受的误码率上限 $\delta = 5\times 10^{-4}$, Alice 能够接受的 Willie 的检测概率上限为 $0.5+\epsilon = 0.55$. 根据定理 5, 设计出满足条件的一种工况条件, 具体的参数设置如表 2 所示. 本小节使用蒙特卡罗方法对 Willie 的检测概率进行仿真. 并在仿真图中设置蓝色铅垂线以分割 Bob 的误码率 $P_e \leqslant \delta$ 和 $P_e > \delta$ 的区域, 也设置橙色铅垂线以分割 Willie 的检测概率 $P_D < \frac{1}{2}+\epsilon$ 和 $P_D \geqslant \frac{1}{2}+\epsilon$ 的区域. 仿真结果证明了定理 3 和 5 计算出的工况条件是满足限制条件的. 若没有特殊说明, 本小节中所有仿真图的参数默认与表 2 一致.

令 Willie 的时间窗口宽度 $\Delta t = 2, 1, 0.5$ s, 分别仿真出 Willie 的检测概率和 Bob 的误码率随着 Bob 接收机信噪比变化的曲线如图 9(a) 所示. 可以得出结论: 当 Willie 的时间窗口包含一个 Alice 的时猝发送周期时, Willie 的接收时间窗口设置的越窄, 其检测概率越高. 这是合理的. 因为若 Willie 的时间窗口过大时, Willie 的接收机将接收到更多的噪声能量把信号能量淹没.

保持其他参数取值不变, 改变 Alice 信号的时猝持续时长 $T_I = 0.3, 0.5, 0.8, 1$ s, 得到的 Willie 检测概率和 Bob 误码率随 Bob 的接收信噪比变化曲线如图 9(b) 所示. 当缩短 Alice 信号模型的时猝持续时长 T_I 时, Willie 的检测概率曲线下降, 即 Alice 获得更好的隐蔽性能, 但这是以牺牲 Alice 的发送信息量为代价的.

保持其他参数不变, 更改码元周期 $T_S = 0.0005, 0.001, 0.005$, 得到的 Willie 检测概率和 Bob 的误码率随 Bob 接收信噪比变化曲线如图 9(c) 所示. 当降低 Alice 信号的符号速率, 即扩大码元周期时, Willie 的检测概率有明显的下降. 因此降低发送信号的符号速率可以提高信号的隐蔽性.

保持其他参数取值不变, 当 $\Delta f = 50$ Hz, 令 $f_{\text{slide}} = f_W - f_c = 250, 500, 750, 1000$, 可以得到 Willie 的检测概率和 Bob 的误码率随 Bob 接收机信噪比变化曲线如图 10(a) 所示. 为了便于表示 Willie 频率窗口与 Alice 信号的重叠关系, 设 δ_0 为 Willie 频率窗口与 Alice 的信号频谱主带的重叠百分比, δ_i^+ 为 Willie 频率窗口与 Alice 信号右侧第 i 个旁瓣重叠百分比, δ_i^- 为 Willie 频率窗口与 Alice 信号左侧第 i 个旁瓣重叠百分比. 当 Willie 的频率检测窗口 Δf 比较窄的时候, 只要 Willie 的频率窗口还在 Alice 信号的主瓣内, Willie 就能获得较大的检测性能, 但是一旦 Willie 的频率窗口移动到 Alice 信号的主瓣以外, 其检测性能迅速下降. 若 Alice 可以通过一定手段得知 Willie 的频率窗口宽度较窄, 那么 Alice 就可以考虑使用例如跳频的手段以躲避 Willie 的检测.

保持其他参数不变, 取 $\Delta f = 1000$ Hz, 改变 $f_{\text{slide}} = 1000, 1500, 2000, 2500$, 得到 Willie 的检测概率和 Bob 的误码率随 Bob 接收机信噪比变化曲线如图 10(b) 所示. 结合图 10(a) 和 (b), 当 Willie 使用小频率窗口检测时, 频率窗口刚移出 Alice 信号频谱的主瓣, 其检测性能就迅速下降, 而Willie 使用较大频率窗口检测时, 频率窗口移出 Alice 信号频率的主瓣时, 其检测性能是缓慢下降的. 若 Willie 知晓 Alice 信号的频谱大概分布范围, 那么其应该使用较小的频率窗口以检测 Alice 的信号. 若 Willie 对 Alice 信号的频谱分布范围了解甚少, 则应先使用大频率窗口进行广泛的搜索.

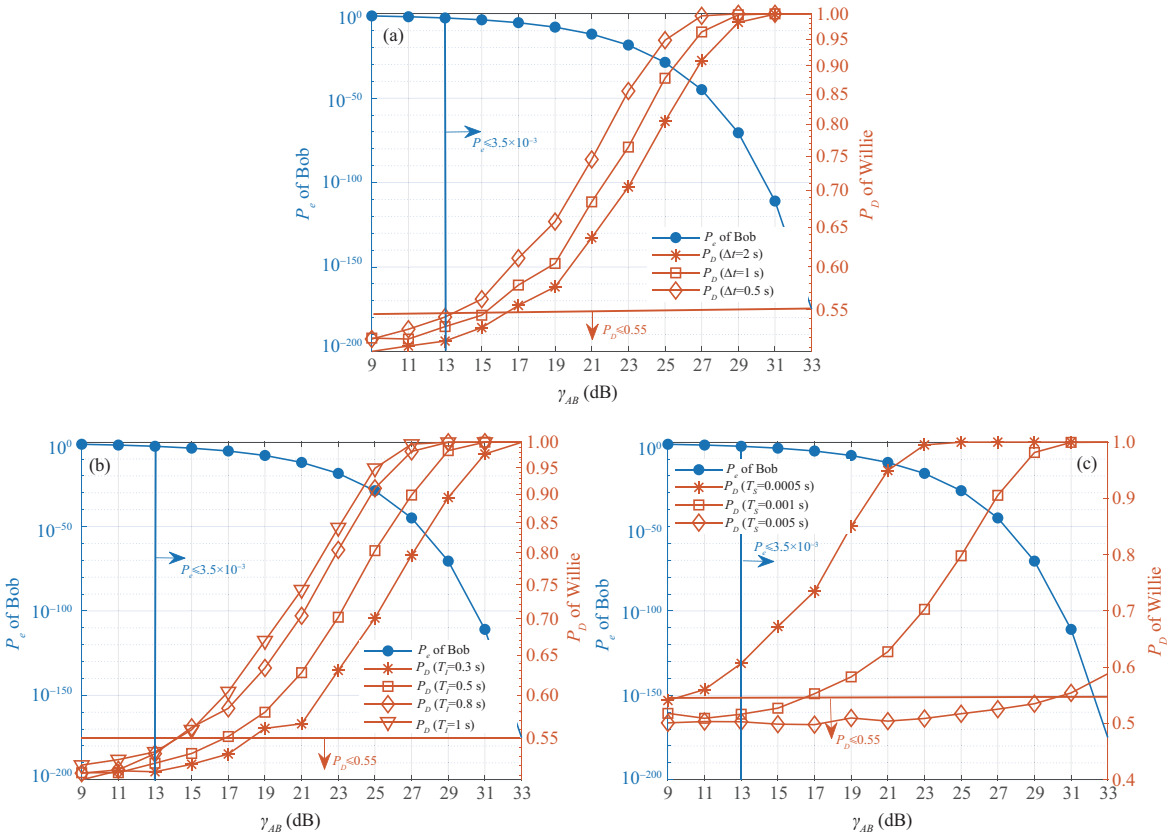

图 9 (网络版彩图) (a) $\Delta t = 0.5, 1, 2$, (b) $T_I = 0.3, 0.5, 0.8, 1$, (c) $T_S = 0.0005, 0.001, 0.005$ 时 Willie 的检测概率与 Bob 的误码率

Figure 9 (Color online) Detection probability of Willie and error rate when (a) $\Delta t = 0.5, 1, 2$, (b) $T_I = 0.3, 0.5, 0.8, 1$, and (c) $T_S = 0.0005, 0.001, 0.005$

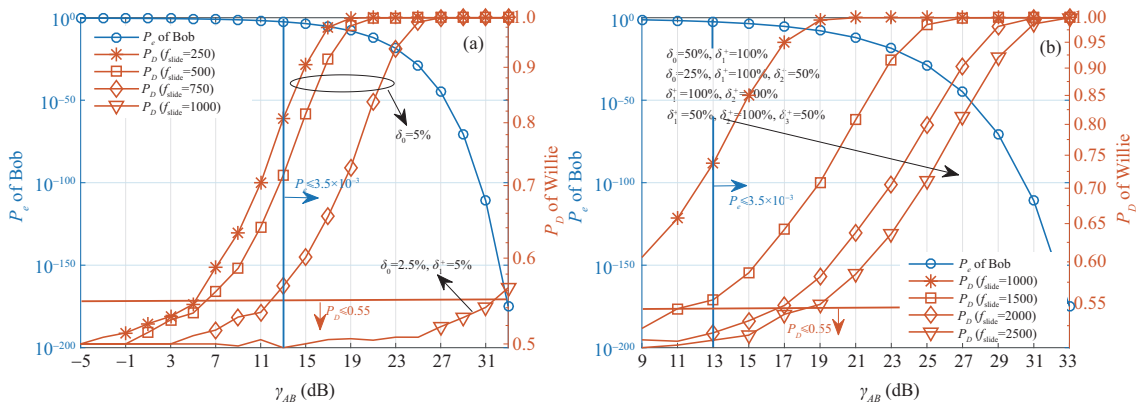

图 10 (网络版彩图) (a) $f_{\text{slide}} = 250, 500, 750, 1000$ 和 (b) $f_{\text{slide}} = 1000, 1500, 2000, 2500$ 时 Willie 的检测概率与 Bob 的误码率

Figure 10 (Color online) Detection probability of Willie and error rate when (a) $f_{\text{slide}} = 250, 500, 750, 1000$ and (b) $f_{\text{slide}} = 1000, 1500, 2000, 2500$

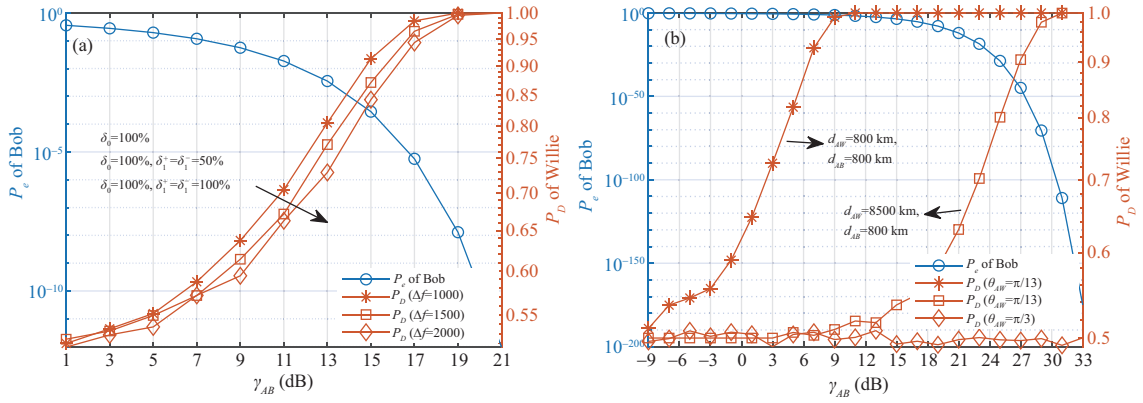

图 11　(网络版彩图) (a) $\Delta f = 1000, 1500, 2000$ 时 Willie 的检测概率与 Bob 的误码率; (b) Willie 在 3 个不同位置时的检测概率与 Bob 的误码率

Figure 11　(Color online) (a) Detection probability of Willie and error rate when $\Delta f = 1000, 1500, 2000$; (b) detection probability of Willie in three different positions and error rate of Bob

保持其他参数不变, 设定 $f_{\text{slide}} = 0$, 并改变 $\Delta f = 1000, 1500, 2000$ Hz, 得到 Willie 的检测概率和 Bob 的误码率随 Bob 的接收机信噪比的变化曲线如图 11(a) 所示. 虽然 Willie 使用较宽的频率窗口可以更容易与 Alice 的信号主瓣产生重叠从而检测到信号, 但是从图 11(a) 中可以看出盲目地增大频率窗口宽度并不能提高检测概率, 反而会降低检测概率.

保持其他参数不变, 令 Willie 的 3 个位置坐标分别为 $d_{AW} = 800$ km, $\theta_{AW} = \frac{\pi}{13}$; $d_{AW} = 8500$ km, $\theta_{AW} = \frac{\pi}{13}$; $d_{AW} = 800$ km, $\theta_{AW} = \frac{\pi}{3}$. 针对 Willie 的这 3 个位置仿真出 Willie 的检测概率以及 Bob 的误码率曲线如图 11(b) 所示. 可以发现, 当 Willie 距离 Alice 的距离较远时比较适合进行隐蔽通信. 在卫星通信中 Willie 可以看作是敌方的高轨侦察卫星, Bob 是己方的低轨通信卫星, Alice 为地面的信号发射方, 由于 Willie 和 Bob 均在各自的轨道上运行, 故当 Willie 和 Bob 的距离较远时可以进行较为安全的通信. 当 Willie 位置角度为 $\theta_{AW} = \frac{\pi}{3}$ 时, Willie 在 Alice 天线的零陷中, 此时 Willie 几乎接收不到任何信号, 故其检测概率始终保持在 0.5, 因此合理地设计具有方向性辐射图的天线并将天线的零陷始终对准 Willie, Alice 也可以实现满足一定要求的隐蔽通信.

保持其他参数不变, 令 $f_{\text{slide}} = 0$ 并分别取 $\alpha = 0.3, 0.2, 0.1, 10^{-2}, 10^{-4}$, 得到 Willie 的检测概率随 Alice-Bob 的接收机信噪比 γ_{AB} 的变化曲线如图 12 所示. 可以看出, 随着虚警概率 α 的减小, Willie 的检测性能也随着下降. 换句话说, Willie 的虚警概率和检测概率是一对矛盾对于某些战时场景 Willie 判断出敌方在传输信号后, 就要立刻做出反击, 但反击的同时也会暴露自己的位置, 故在这种反击代价过大的场景, 必须要牺牲一定的检测性能以换取超低的虚警概率. 而对于单纯的信号监听场景, 检测到信号存在与否是最重要的, 故在这种代价较小的场景, 可以考虑牺牲一些算力, 使用较高的虚警概率检测器以获得更高的检测性能.

8　思考与展望

前述部分阐述了基于扩维域能量弥散的隐蔽通信模型, 通过数值计算和系统仿真对该模型进行了分析并归纳得到了一些指导性的结论. 在本节中, 我们将对本文提出的基于扩维域能量弥散的隐蔽通信模型在实际无线隐蔽通信系统的设计和优化方面的运用可行性进行详细的分析和展望.

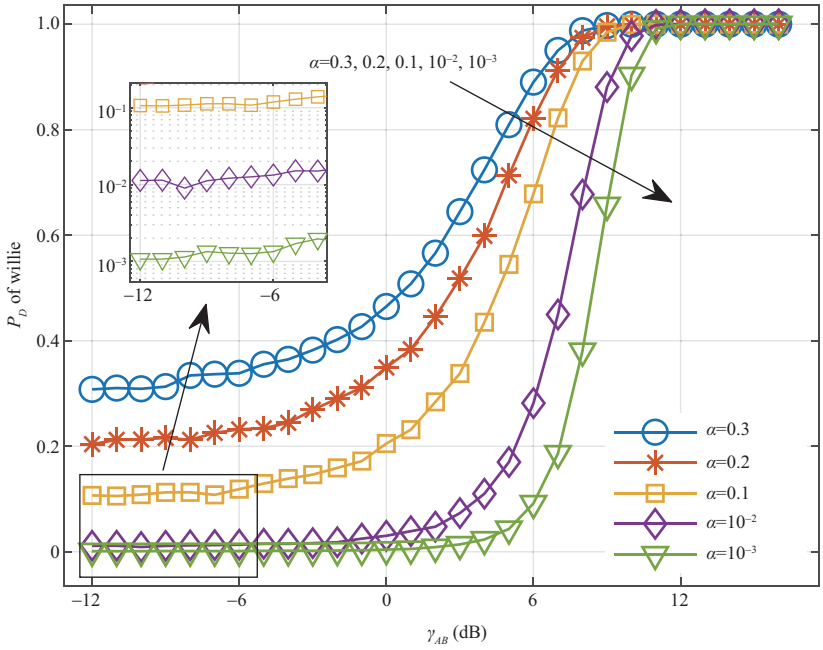

图 12 (网络版彩图) $\alpha = 0.3, 0.2, 0.1, 10^{-2}, 10^{-3}$ **时 Willie 的检测概率**

Figure 12 (Color online) Detection probability of Willie when $\alpha = 0.3, 0.2, 0.1, 10^{-2}, 10^{-3}$

8.1 无线隐蔽通信的内生矛盾

在实际工程运用中, 通常使用隐蔽性和可靠性来分别描述一个通信系统中 Alice-Bob 通信链路抗 Willie 侦测的隐蔽性能和 Bob 处抗衰落抗干扰的接收可靠性. 在后续部分中, 我们将分别用隐蔽概率和可靠概率来量化研究无线通信系统的隐蔽性和可靠性.

定义:

• 系统的隐蔽概率. $P_C = 1 - P_D$, 其中, P_D 为侦听方检测概率. 易知, 系统的隐蔽性反映了 Willie 对 Alice 发出信号的侦测性能. 即当检测率 P_D 越高时, 系统的隐蔽性越差; 反之, 亦然.

• 系统的可靠概率. $P_R = 1 - P_e$, 其中, P_e 指接收方的误码率. 易知, 系统的可靠性反映了 Bob 对 Alice 发出信号的接收性能. 即当误码率 P_e 越低时, 系统的可靠性越高; 反之, 亦然.

从以上对和可靠性的量化定义可以得到[6]: 系统隐蔽性与 Willie 处的接收信噪能量比 ($\gamma_W = E_b G_{AB}/N_0$, 其中, E_b 为 Alice 发送信号的单比特能量, G_{AW} 为 Alice-Willie 链路的信号能量增益) 成反比; 而系统可靠性与 Bob 处的接收信噪能量比 ($\gamma_B = E_b G_{AW}/N_0$, 其中, G_{AB} 为 Alice-Bob 链路的信号能量增益) 成正比.

这样, 当其他系统参数 (如 G_{AB}, G_{AW}, N_0 等) 给定的情况下, 随着 Alice 发送信号的单比特能量 E_b 的增大, 系统的可靠性会上升, 但与此同时系统的隐蔽性也会下降. 那么, 我们可以清晰地看出: 对于无线通信系统而言, 其传输行为的隐蔽性和可靠性是一对相互制约的内生矛盾.

辩证唯物主义告诉我们: 矛盾是推动事物发展的源泉, 矛盾双方既对立又统一, 共同推动事物的发展. 故此, 无线隐蔽通信系统的实现途径就是在动态时变的无线传输环境中探寻和利用通信行为隐蔽性和可靠性这一对固有内生矛盾的对立和统一机理.

6) 为了便于分析, 我们假设 Bob 和 Willie 处 AWGN 的单比特接收能量相同且均为 N_0.

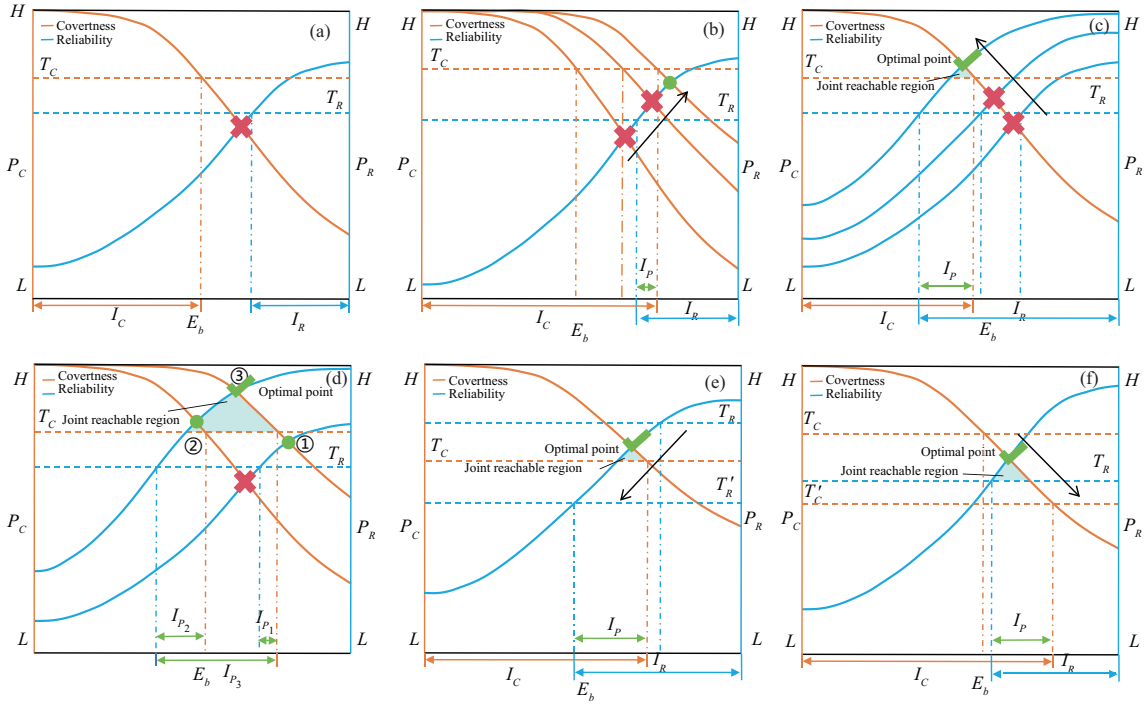

图 13　(网络版彩图) 不同情况下的可靠性和隐蔽性曲线示意图

Figure 13　(Color online) Sketch map of reliable and covert performance curves in (a) case 1, (b) case 2, (c) case 3, (d) case 4, (e) case 5, and (f) case 6

8.2　无线隐蔽通信系统的实现原理及技术途径

假若无线隐蔽通信系统须满足一定的隐蔽指标, 即 $P_C > T_C$, 满足这一指标的 E_b 的区间称为隐蔽区间 I_C. 同时, 为了保证无线信息在 Alice 和 Bob 之间的可靠传输, 无线隐蔽通信系统还必须满足一定的可靠性指标, 即 $P_R > T_R$, 满足这一指标的 E_b 的区间称为可靠区间 I_R. 当 I_C 与 I_R 存在非空交集时, 则将两区间的交集称为可达区间 I_P. 换句话说, 当发射机发送信号的单比特能量 $E_b \in I_P$ 时, 则可实现无线隐蔽高可靠传输.

根据 8.1 小节中对隐蔽性和可靠性这一内生矛盾的分析, 如图 13 所示, 下面我们将 Alice 发送信号的单比特能量 E_b 为横轴变量来分析和刻画可靠性和隐蔽性曲线的不同存在情况.

图 13 中橙色和蓝色曲线分别代表隐蔽概率和可靠概率曲线; 橙色、蓝色和绿色区间分别代表隐蔽区间 I_C, 可靠区间 I_R 和可达区间 I_P; 隐蔽性和可靠性的指标约束分别为 $P_C > T_C$ 和 $P_R > T_R$; 浅绿色区域为由隐蔽概率曲线、可靠概率曲线以及系统可靠概率阈值曲线或隐蔽概率阈值曲线共同决定的隐蔽性可靠性联合可达域. 下面将分别分析图 13 中所示的 6 种不同情况.

• 情况 1. 在此情况中, 隐蔽区间 I_C 和可靠区间 I_R 没有交集, 因此不存在可达区间. 进一步观察可以发现隐蔽概率曲线和可靠概率曲线的交点此时低于隐蔽性阈值 T_C 以及可靠性阈值 T_R.

• 情况 2. 在此情况下, 当隐蔽概率曲线抬升时, 隐蔽概率曲线与可靠概率曲线的交点逐渐上移, 这样可达区间便从无到有并逐渐变宽. 在实际场景中, 发送方 Alice 可以采取本文前述的一些扩维域能量弥散途径或设法恶化 Willie 侦收质量等手段, 如施加人工干扰或者人工噪声等策略, 可以提升隐蔽概率曲线从而使得可达区间从无到有或从窄到宽.

• 情况 3. 在此情况中, 当可靠概率曲线抬升时, 隐蔽概率曲线与可靠概率曲线的交点逐渐上移, 这样可达区间从无到有并逐渐变宽. 在实际场景中, 在发送方 Alice 不改变发送参数 (如每比特发射能量 E_b 等) 的前提下, 接收方 Bob 可以通过一些手段来改善信号的接收质量, 如采用更高性能的接收机或 Alice-Bob 双方使用性能更强的编译码策略等方法, 实现可靠概率曲线的提升从而获得更宽的可达区间.

• 情况 4. 在此情况中, 当仅有隐蔽概率曲线抬升或仅有可靠概率曲线抬升时, 隐蔽概率曲线与可靠概率曲线的交点均会逐渐上移 (分别对应图 13 中的交点 ① 和 ②), 可达区间实现从无到有的质变 (分别对应图 13 中的可达区间 I_{P_1} 和 I_{P_2}). 当隐蔽概率曲线和可靠概率曲线均抬升时, 隐蔽概率曲线与可靠概率从曲线交于点 ③. 可以发现, 交点 ③ 所对应情形的可行区间 I_{P_3} 宽于 I_{P_1} 和 I_{P_2}. 在隐蔽概率曲线和可靠概率曲线抬升的过程中, 隐蔽概率曲线与可靠概率曲线的交点随之升高, 当交点的纵坐标高于 $\max\{T_C, T_R\}$ 时, 可行区间必然存在. 当隐蔽概率曲线与可靠概率曲线的交点纵坐标高于 $\max\{T_C, T_R\}$ 时, 称两曲线交点可分布的区域为联合可达域, 如图 13(d) 中阴影区域所示. 交点 ③ 为联合可达域的最高点, 其对应的可达区间最长, 同时具有最优的 "隐蔽性 – 可靠性", 称交点 ③ 为联合最优可达点. 实际上情况 4 是情况 2 与情况 3 的结合.

• 情况 5. 在此情况中, 接收方 Bob 将可靠性能阈值从 T_R 降低到 T'_R, 即可在不改变可靠概率和隐蔽概率工作曲线的条件下实现可达区间. 在实际场景中, 在发送方 Alice 不改变发送参数 (如每比特发射能量 E_b 等) 的前提下, 接收方 Bob 可以通过采用一些可提升接收增益的策略, 诸如使用多天线分集接收, 改善 Bob 处的信号接收可靠性, 从而产生可达区间.

• 情况 6. 在此情况中, 当隐蔽性能指标从 T_C 降低到 T'_C 时, 在不改变可靠概率和隐蔽概率工作曲线的条件下产生可达区间. 在实际场景中, 如在卫星通信场景中, 电子侦察卫星 Willie 的侦收性能可能极高. 然而, 当电子侦察卫星 Willie 处于非地球静止轨道时, 由于其在轨运行必须服从一定物理运动规律, 这样它难以在其轨道上的任何位置均对目标地面区域或者目标空域维持不变的检测性能. 再如, 当电子侦察卫星 Willie 工作于地球静止轨道时, 由于其在轨位置相对于地球而言保持静止不变, 其对广袤的地球表面或空域的侦收能力是不一致的. 因此, Alice-Bob 双方可以利用 Willie 侦收性能的时空不一致性, 以较低的隐蔽性能阈值进行信息传输.

在以上的分析中, 可以明显地发现: 可达区间的加宽一定伴随着隐蔽概率曲线和可靠概率曲线交点的升高. 当交点高于 $\max\{T_C, T_R\}$ 时, 联合可达域则出现, 而联合最优可达点所对应的可达区间更宽且具有最强的隐蔽性和可靠性. 分析隐蔽概率曲线和可靠概率曲线交点的高低与可达区间和联合可达域是否存在的关系, 可以归纳总结出以下 3 条结论:

• 当隐蔽概率曲线和可靠概率曲线的交点同时高于 T_C 和 T_R 时, 一定存在可达区间和联合可达区域.

• 当隐蔽概率曲线和可靠概率曲线的交点仅仅高于 T_C 或 T_R 时, 可能存在可达区间, 但无联合可达区域.

• 当隐蔽概率曲线和可靠概率曲线的交点同时低于 T_C 和 T_R 时, 一定不存在可达区间和联合可达区域.

• 当联合可达域存在时, 隐蔽概率曲线和可靠概率曲线的交点即为该系统可实现的最优联合 "隐蔽性 – 可靠性".

综上所述, 我们可以看到: 实现无线隐蔽通信系统的技术途径就是通过系统设计产生并工作于非空隐蔽性可靠性联合可达域.

鉴于篇幅所限, 我们将在未来的工作中对影响 Alice-Bob-Willie 三点隐蔽通信模型的各种系统因

素进行量化并推导出隐蔽概率曲线和可靠概率曲线的解析表达式, 再根据解析表达式设计能够提升隐蔽概率曲线和可靠概率曲线交点纵坐标的可行方案.

9 结论

本文提出了扩维域能量弥散隐蔽通信模型, 并在此模型的基础上分别推导了 Alice 的隐蔽存在条件以及 Willie 的检测概率表达式; 然后, 结合所得的理论分析表达式, 绘制了 Willie 检测能量和检测概率的仿真结果, 从博弈的角度为 Alice 和 Willie 的通信行为设计提供了一些建议. 最后, 针对实际场景中的无线隐蔽通信系统的设计与实现, 本文揭示了无线通信系统隐蔽性和可靠性这一固有内生矛盾并辩证地指出了破解和平衡该矛盾, 以及实现无线隐蔽通信的原理和技术途径.

针对 Alice 和 Willie 的博弈过程, 本文得到如下结论:

• 当 Alice 采用短时猝发策略进行信息发送时, Willie 的时域检测窗口应与 Alice 信号时猝时长相仿. Willie 时域窗口过短或过长均会降低检测概率.

• 当 Willie 使用较小的频率窗口在频段上进行频率搜索比使用较大频率窗口的检测效果好. 当 Willie 对 Alice 发送信号的频谱范围几乎一无所知时, 可以先用大频率窗口缩小频率范围, 再用小频率窗口精确搜索.

• 当 Alice 的符号速率恒定时, 采用更短的时猝持续时间可以提高其信号的隐蔽性.

• 当 Alice 短时猝发的持续时长固定时, 采用更低的符号速率可以显著地提高信号隐蔽性.

• 当 Alice 知晓 Willie 的大致位置时, Alice 可以采取将天线辐射的零陷指向 Willie 的方法以降低 Willie 所在位置的能量密度.

• 当 Willie 不能承受虚警所带来的代价时, Alice 可以获得宽松的隐蔽条件. 当 Willie 能承受虚警所带来的代价时, Willie 可以适当降低检测门限以获得较高的检测概率.

• 当 Alice 将信号能量弥散至更多的维域时, Alice 会获得更高的隐蔽性能.

参考文献

1 Makhdoom I, Abolhasan M, Lipman J. A comprehensive survey of covert communication techniques, limitations and future challenges. Comput Secur, 2022, 120: 102784

2 Chen W Y, Luo J S, Wang F G, et al. Survey of capacity limits and implementation techniques in wireless covert communication. J Commun, 2022, 43: 203–218 [陈炜宇, 骆俊杉, 王方刚, 等. 无线隐蔽通信容量限与实现技术综述. 通信学报, 2022, 43: 203–218]

3 Pickholtz R, Schilling D, Milstein L. Theory of spread-spectrum communications — a tutorial. IEEE Trans Commun, 1982, 30: 855–884

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, et al. Hiding information in noise: fundamental limits of covert wireless communication. IEEE Commun Mag, 2015, 53: 26–31

6 Bash B A, Goeckel D, Towsley D. Covert communication gains from adversary's ignorance of transmission time. IEEE Trans Wireless Commun, 2016, 15: 8394–8405

7 Goeckel D, Bash B, Guha S, et al. Covert communications when the warden does not know the background noise power. IEEE Commun Lett, 2015, 20: 236–239

8 Che P H, Bakshi M, Jaggi S. Reliable deniable communication: hiding messages in noise. In: Proceedings of IEEE International Symposium on Information Theory, 2013. 2945–2949

9 Wang L, Wornell G W, Zheng L. Fundamental limits of communication with low probability of detection. IEEE Trans Inform Theor, 2016, 62: 3493–3503

10 Bloch M R. Covert communication over noisy channels: a resolvability perspective. IEEE Trans Inform Theor, 2016, 62: 2334–2354
11 Ma R, Yang X, Pan G, et al. Covert communications with channel inversion power control in the finite blocklength regime. IEEE Wireless Commun Lett, 2021, 10: 835–839
12 Wang J, Li J, Xiao S, et al. Continuous message transmission for covert communication. IEEE Commun Lett, 2024, 28: 463–467
13 Kumar Arumugam K S, Bloch M R. Embedding covert information in broadcast communications. IEEE Trans Inform Forensic Secur, 2019, 14: 2787–2801
14 Karakoc N, Duman T M. Rate selection for wireless random access networks over block fading channels. IEEE Trans Commun, 2019, 68: 1604–1616
15 Tao L, Yang W, Yan S, et al. Covert communication in downlink NOMA systems with random transmit power. IEEE Wireless Commun Lett, 2020, 9: 2000–2004
16 Wang Y, Yan S, Yang W, et al. Covert communications with constrained age of information. IEEE Wireless Commun Lett, 2020, 10: 368–372
17 Yang W, Lu X, Yan S, et al. Age of information for short-packet covert communication. IEEE Wireless Commun Lett, 2021, 10: 1890–1894
18 Huang K W, Wang H M, Towsley D, et al. LPD communication: a sequential change-point detection perspective. IEEE Trans Commun, 2020, 68: 2474–2490
19 Yang Z, Yue P, Wang S, et al. Energy-efficient optimization for RIS-aided MIMO covert communications. IEEE Internet Things J, 2023, 10: 18993–19003
20 Song D, Yang Z, Pan G, et al. RIS-assisted covert transmission in satellite-terrestrial communication systems. IEEE Int Things J, 2023, 10: 19415–19426
21 Cankara M N, Cek M E. Covert digital communication using random frequency hopped spread-spectrum. In: Proceedings of the 8th International Conference on Electrical and Electronics Engineering, 2021. 490–493
22 Scholtz R. Multiple access with time-hopping impulse modulation. In: Proceedings of IEEE Military Communications Conference, 1993. 447–450
23 Bharadwaj A, Townsend J K. Evaluation of the covertness of time-hopping impulse radio using a multi-radiometer detection. In: Proceedings of Communications for Network-Centric Operations: Creating the Information Force, 2001. 128–134
24 An J P, Ding H C, Wang S. Low-to-no-power covert communication based on energy dispersion. Sci Sin Inform, 2023, 53: 2266–2282 [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]
25 An J P. Space-Aerial Covert Communications. Beijing: National Defence Industry Press, 2023 [安建平. 空天隐蔽通信. 北京: 国防工业出版社, 2023]
26 Balanis C A. Antenna Theory: Analysis and Design. New Jersey: John Wiley and Sons, 2016
27 Kay S M. Fundamentals of Statistical Signal Processing: Detection Theory. New Jersey: Prentice-Hall, 1993

附录 A

设函数 $f(x)=\frac{1}{3}\mathrm{e}^{-x}-\mathrm{erfc}(x)=\frac{1}{3}\mathrm{e}^{-x}-\frac{2}{\sqrt{\pi}}\int_{\sqrt{x}}^{\infty}\mathrm{e}^{-t^2}\mathrm{d}t$. 对 $f(x)$ 求导可得 $\frac{\mathrm{d}f(x)}{\mathrm{d}x}=\mathrm{e}^{-x}(\frac{1}{\sqrt{\pi x}}-\frac{1}{3})$. 求 $f(x)$ 的二阶导数可得 $\frac{\mathrm{d}^2f(x)}{\mathrm{d}x^2}=-\mathrm{e}^{-x}(\frac{1}{\sqrt{\pi x}}-\frac{1}{2\sqrt{\pi}x^{\frac{3}{2}}}-\frac{1}{3})$.

当 $2.05<x<\frac{9}{\pi}$ 时, 很容易得到下面 3 个条件:

$$\begin{cases} f(2.05)>0, \\ f'(x)>0, \\ f'\left(\dfrac{9}{\pi}\right)=0. \end{cases} \tag{A1}$$

根据式 (A1), 可得 $f(x)>0,\ 2.05<x<\frac{9}{\pi}$. 当 $x>\frac{9}{\pi}$ 时, 进一步可得如下 4 个条件:

$$\begin{cases} f\left(\dfrac{9}{\pi}\right)>0, \\ f(\infty)\to 0, \\ f'(x)<0, \\ f''(\infty)\to 0^{+}. \end{cases} \tag{A2}$$

因此, 可以推出 $f(x)>0,\ x>\frac{9}{\pi}$.

综上所述可得 $f(x)>0,\ x>2.05$. 令 $x=\frac{3}{M^2-1}\gamma_{AB}$, 可得: 当 $\gamma_{AB}>\frac{2.05(M^2-1)}{3}$ 时, 下面的不等式成立:

$$\operatorname{erfc}\left(\sqrt{\frac{3}{M^2-1}\gamma_{AB}}\right)\leqslant\frac{1}{3}\mathrm{e}^{-\frac{3}{M^2-1}\gamma_{AB}}. \tag{A3}$$

Covert communications based on energy dispersion in extended dimensions

Jianping AN[1], Zihan NI[1], Shuai WANG[1*], Gaofeng PAN[1] & Hao YIN[2]

1. *School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing* 100081*, China*;
2. *Academy of Military Sciences, Beijing* 100091*, China*
* Corresponding author. E-mail: swang@bit.edu.cn

Abstract Wireless communication technology is an indispensable means of information transmission in the thriving data era, while wireless security is particularly crucial in establishing the foundation of this era. In certain specific scenarios, the transmitter must not only ensure the security of the information content but also aim to achieve the transmission behavior of wireless signals without being detected by eavesdroppers. In response to the serious threat of radio eavesdropping, traditional covert communication methods depend on dispersing energy in one or two domains to minimize the probability of detection. For example, the code division multiple access technology based on the spread spectrum disperses energy in the frequency domain. Burst transmission technology disperses energy in discrete time intervals in the time domain while combining burst transmission with frequency hopping disperses energy in both time and frequency domains. The paper initially backtracks the physical nature of energy dispersion in wireless signal transmission. The covert communication model has been expanded from a single-domain energy dispersion to a multi-domain approach, encompassing the time, frequency, and space domains. By employing this model and tools such as radio propagation and digital signal processing theory, the paper models the energy dispersion of wireless signals in the three domains of time, frequency, and space. An energy detector is designed for eavesdropping in the three domains of time, frequency, and space. Subsequently, the expressions for capturing energy by the eavesdropper are derived using the multi-domain detection model. The expressions for the upper and lower boundaries of the eavesdropper's detection probability using average noise energy as the threshold, as well as those for the upper and lower boundaries of the detection probability under the Neyman-Pearson energy detector, are also derived. Subsequently, combining theoretical derivation and analysis, we deduce and prove the guiding principles of multi-domain energy dispersion-based covert communication. Subsequently, the paper explores simulations and discussions, from a game-theoretic perspective, of the conditions for the covert presence of the transmitter under the multi-domain energy detection model and the strategies for improving the eavesdropper's capabilities. Finally, the inherent contradiction and interaction mechanism between the covertness and reliability of wireless covert communications are revealed for practical design and realization. Then, the principle and technical approach to achieving wireless covert transmission are provided.

Keywords covert communications, energy dispersion in multi-domains, radio propagation theory, interception of radio signal, Neyman-Pearson detection