中国科学: 信息科学 2021 年 第 51 卷 第 8 期: 1360–1374
SCIENTIA SINICA Informationis
论文

基于 3D 波束成形的隐蔽无线通信威胁区域构建

林钰达[1*], 金梁[1], 黄开枝[1], 韩乾[2]

1. 战略支援部队信息工程大学, 郑州 450002
2. 网络通信与安全紫金山实验室, 南京 211189
* 通信作者. E-mail: linyuda.ieu@foxmail.com

收稿日期: 2020–09–15; 修回日期: 2020–11–09; 接受日期: 2020–12–14; 网络出版日期: 2021–08–02

国家重点研发计划 (批准号: 2017YFB0801900) 项目资助

摘要 为了实时且直观地评估当前隐蔽无线通信系统所面临的未知非法检测威胁, 本文首次定义了隐蔽威胁区域并设计了相应轻量级算法. 首先, 在莱斯衰落信道和噪声不确定条件下构建了基于 3D 波束成形的下行隐蔽无线通信系统模型, 分析了敌方最优检测性能, 推导了系统最小平均隐蔽概率; 然后, 给出了通信速率及连接中断概率闭式表达式, 求解了给定敌方位置时的系统最大化隐蔽吞吐量优化问题; 最后, 针对实际通信场景中无法获知敌方位置或分布规律的情形, 定义了系统隐蔽威胁区域这一新的性能指标, 并设计了相应轻量级算法. 仿真结果验证了系统的隐蔽性能、总体性能, 以及所提算法性能, 揭示了背景噪声、信道环境、天线构造和系统要求等主要参数对隐蔽威胁区域的影响.

关键词 隐蔽无线通信, 隐蔽威胁区域, 3D 波束成形, 莱斯衰落, 噪声不确定

1 引言

随着日益增长的海量关键敏感信息通过无线网络进行传输, 无线通信的安全防护正面临着愈加严峻的挑战. 广泛应用的传统加密技术以及日渐成熟的物理层安全技术被视为保护通信传输内容的有效手段, 然而由于电磁波的广播特性, 它们都无法对传输检测提供保护 [1]. 在海外基地、大使馆、执行 “发现即摧毁” 战略的现代战场等高安全等级的特殊场景下, 隐蔽无线通信技术可以有效防止无线信号被敌方非法截获, 并以此规避众多难以预估的风险和灾难, 因此正不断引起业界的关注和研究.

隐蔽无线通信作为无线通信安全领域中的后起之秀, 是一种通过运用多种信号处理手段以实现敌方低概率检测的无线通信技术. 区别于现代信息隐藏技术通过利用多媒体信息掩体在高层实现信息隐藏, 隐蔽无线通信则是通过利用背景噪声或干扰信号等掩体直接在物理层实现信号隐蔽, 因此保护的是更基础、更广泛的合法通信行为 [2].

引用格式: 林钰达, 金梁, 黄开枝, 等. 基于 3D 波束成形的隐蔽无线通信威胁区域构建. 中国科学: 信息科学, 2021, 51: 1360–1374, doi: 10.1360/SSI-2020-0287
Lin Y D, Jin L, Huang K Z, et al. Threat region development of covert wireless communication based on 3D beamforming (in Chinese). Sci Sin Inform, 2021, 51: 1360–1374, doi: 10.1360/SSI-2020-0287

自 20 世纪初以来, 扩频技术作为隐蔽无线通信的典型代表已经得到了广泛应用, 但是关于其理论限制的研究一直没有得到关注. 直到 Bash 等 [3] 率先证明了隐蔽无线通信的信息论极限 —— 平方根律, 即 AWGN (additive white Gaussian noise) 信道下 n 次信道使用能够可靠且隐蔽地传输最多不超过 $\sqrt{n}$ 比特量级的信息, 有关平方根律的研究随后也在各种不同信道模型中得到了扩展. 然而, 平方根律也揭示了信道使用次数趋于无穷时系统的零隐蔽速率, 为实现具有正隐蔽容量的隐蔽无线通信系统, 人们开始重点关注于隐蔽方案设计以及系统性能优化, 包括采用基于噪声不确定性 [4~6]、配置协作干扰节点 [7~9]、利用已有公开通信掩体等 [10,11] 技术手段实现通信高概率隐蔽, 再通过系统参数设计优化系统隐蔽性能并最大化隐蔽吞吐量, 以此不断推进隐蔽无线通信技术的早日应用.

纵观当前隐蔽无线通信研究, 一方面, 只有少数研究关注了多天线对隐蔽无线通信的增益. 其中, Zheng 等 [12] 首次研究了泊松干扰网络下多天线隐蔽无线通信, 并具体对比了集中式天线系统和分布式天线系统的隐蔽性能. Lin 等 [6] 则在噪声不确定对所有节点均有影响的情形下, 研究了多天线隐蔽无线通信的最优性能. Forouzesh 等 [13] 首次关注了 3D 波束成形技术对隐蔽无线通信的影响, 具体在只存在散射径传播的瑞利 (Rayleigh) 衰落信道下, 重点研究了波束最优仰角和零空间人工噪声的设计. 显然, 相较于传统 2D 波束成形, 3D 波束成形能在水平和垂直两个维度上提供发射能量的汇集, 从而更精细地对准目标用户. 然而, 在同时存在散射径和直射径传播的莱斯 (Rice) 衰落信道中, 3D 波束成形的能量聚焦效应将被进一步放大, 此时敌方接收信号能量也可能获得大幅提升, 因此基于 3D 波束成形的多天线技术是否依然能够实现隐蔽无线通信还有待深入研究.

另一方面, 目前大多数研究都考虑了只存在固定位置的单个敌方 [14~16], 少数研究考虑了存在服从泊松分布的多个敌方 [9,12,17], 还未有研究考虑可以位于任意位置的敌方. 事实上, 实际通信场景中要想掌握敌方具体位置或分布规律具有很大难度, 而敌方所处位置又十分影响着它的检测性能. 比如当敌方距离发送方足够远时, 由于距离衰减其接收信号能量早已淹没在噪声之中, 几乎不可能完成信号检测及还原, 此时无需额外设计就能保证通信相对隐蔽; 而当敌方足够靠近合法接收方时, 只要它采取相同的检测手段, 理论上几乎不可能防止它正确地检测出通信信号. 因此, 亟需定义一种与位置绑定的隐蔽性能评价指标来直观地描述系统隐蔽无线通信所面临的潜在检测威胁.

针对上述两个问题, 本文首先在莱斯信道模型和噪声不确定条件下, 构建了基于 3D 波束成形的系统模型, 分析了敌方最优检测性能, 推导了系统最小平均隐蔽概率. 其次, 给出了通信速率及连接中断概率闭式表达式, 求解了给定敌方位置时的系统最大化隐蔽吞吐量优化问题. 接着, 考虑到实际场景中无法获知敌方位置和分布规律的情形, 首次定义了隐蔽威胁区域这一新的性能评价指标, 并设计了相应轻量级算法. 最后, 通过仿真实验验证了所提系统的隐蔽性能和总体性能, 重点分析了背景噪声、信道环境、天线构造和系统要求等主要参数对隐蔽威胁区域的影响, 为实际隐蔽无线通信系统设计及参数配置提供了理论指导.

2 系统模型

本文考虑一个基于 3D 波束成形的下行隐蔽无线通信系统, 如图 1 所示, 包含基站 Alice、合法接收用户 Bob, 以及可任意移动的未知非法检测敌方 Willie. 其中 Alice 采用均匀平面天线阵列 (uniform planar antenna array, UPA), 依行列方向共配备 $L \times M$ 根天线, 天线高度记为 T. Bob 和 Willie 均为单天线, 并分布在二维平面上. 为便于后续性能分析, 进一步以 Alice 为原点建立三维笛卡尔坐标系.

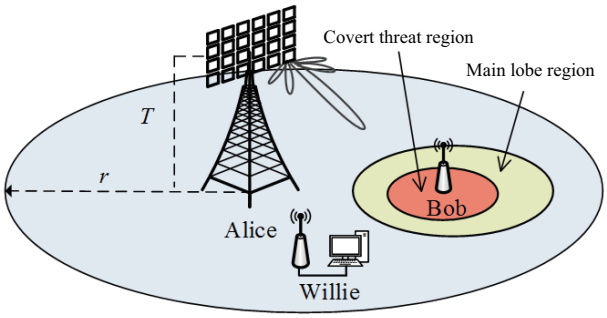


图 1 (网络版彩图) 基于 3D 波束成形的下行隐蔽无线通信系统模型

Figure 1 (Color online) System model of downlink covert wireless communication based on 3D beamforming

假设信道为准静态莱斯衰落, 即

$$\boldsymbol{h}_{az}=\sqrt{\frac{K_z}{K_z+1}}\bar{\boldsymbol{h}}_{az}+\sqrt{\frac{1}{K_z+1}}\tilde{\boldsymbol{h}}_{az}, \tag{1}$$

其中, $z\in\{b,w\}$ 表示 Bob 或 Willie, K_z 表示基站与节点 z 的莱斯 K 因子, $\bar{\boldsymbol{h}}_{az}$ 表示相应视距直达分量, $\tilde{\boldsymbol{h}}_{az}=[\tilde{h}_{az}^1,\tilde{h}_{az}^2,\ldots,\tilde{h}_{az}^M]\sim\mathcal{CN}(\boldsymbol{0},\boldsymbol{I}_{M\times1})$ 表示瑞利衰落分量. 基于 UPA 的几何结构 [18] 可得

$$\bar{\boldsymbol{h}}_{az}=\boldsymbol{a}(\theta_z,\varphi_z)=\boldsymbol{a}_v(\theta_z)\otimes\boldsymbol{a}_h(\theta_z,\varphi_z), \tag{2}$$

$$\boldsymbol{a}_v(\theta_z)=\left[1,\mathrm{e}^{\mathrm{j}2\pi\frac{\Delta d}{\lambda}\sin\theta_z},\ldots,\mathrm{e}^{\mathrm{j}2\pi(M-1)\frac{\Delta d}{\lambda}\sin\theta_z}\right], \tag{3}$$

$$\boldsymbol{a}_h(\theta_z,\varphi_z)=\left[1,\mathrm{e}^{\mathrm{j}2\pi\frac{\Delta d}{\lambda}\cos\theta_z\sin\varphi_z},\ldots,\mathrm{e}^{\mathrm{j}2\pi(M-1)\frac{\Delta d}{\lambda}\cos\theta_z\sin\varphi_z}\right], \tag{4}$$

其中, $\boldsymbol{a}_v(\theta_z)$ 和 $\boldsymbol{a}_h(\theta_z,\varphi_z)$ 分别表示 $\bar{\boldsymbol{h}}_{az}$ 的垂直分量和水平分量, θ_z 和 φ_z 表示是基站相对节点 z 的垂直视角和水平视角, Δd 表示天线间距, λ 表示载波波长.

考虑离散时隙通信系统, 通信块长为 N, 则 Bob 和 Willie 的接收信号可统一表示为

$$y_z[n]=\sqrt{Pd_{az}^{-\alpha}}\boldsymbol{h}_{az}^{\mathrm{H}}\boldsymbol{w}s[n]+r_z[n], \tag{5}$$

其中, $n=1,2,\ldots,N$, P 表示基站发射功率, d_{az} 表示基站与节点 z 之间的距离, α 表示路径衰落因子, $\boldsymbol{w}$ 表示基站预编码矩阵. $s[n]$ 表示基站发给 Bob 的私密信号, 假设基站采用归一化的复高斯随机编码, 即 $s[n]\sim\mathcal{CN}(0,1)$. $r_z[n]$ 表示节点 z 侧方差为 σ_z^2 的高斯白噪声, 即 $r_z[n]\sim\mathcal{CN}\left(0,\sigma_z^2\right)$, 假设 Willie 对其噪声功率存在不确定性, 且服从对数均匀分布 [4~6], 即

$$f_{\sigma_w^2}(x)=\begin{cases}\dfrac{1}{2x\ln\rho}, & \text{if } \dfrac{\sigma_n^2}{\rho}\leqslant x\leqslant\rho\sigma_n^2,\\ 0, & \text{otherwise},\end{cases} \tag{6}$$

其中, σ_n^2 表示 Willie 侧的噪声水平, ρ 表示噪声不确定程度且 $\rho>1$. 噪声不确定性的存在使得 Willie 的接收信噪比可能会低于信号检测所要求的信噪比墙 [19], 从而以一定概率发生检测错误, 为系统实现隐蔽无线通信提供可能.

3 检测性能分析

为定量分析敌方的检测性能, 本节首先介绍了敌方检测过程中所面临的二元假设检验问题, 并基

于虚警率和漏检率给出了检错概率定义. 其次, 计算了敌方接收信号功率的概率密度函数. 最后, 推导了系统最小平均隐蔽概率和敌方最优检测门限.

3.1 二元假设检验

遵循信号检测中的假设检验理论, 首先分析敌方 Willie 的检测方式. Willie 接收信号可表示为

$$y_w[n]=\begin{cases} r_w[n], & \mathcal{H}_0,\\ \sqrt{Pd_{aw}^{-\alpha}}\boldsymbol{h}_{aw}^{\mathrm{H}}\boldsymbol{w}s[n]+r_w[n], & \mathcal{H}_1, \end{cases} \tag{7}$$

其中, $\mathcal{H}_0$ 表示基站未在通信, 反之为 $\mathcal{H}_1$. 由于合法双方采用了复高斯随机编码, 这使得 Willie 无法通过分析接收信号分布来判断隐蔽通信的存在性. 假设 Willie 能同步通信时隙, 此时其最优检测方式已被证明为能量检测法 [7]. 基于二元假设检验, Willie 需进行如下判决

$$P_w \triangleq \frac{1}{N}\sum_{i=1}^{N}|y_w[n]|^2 \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \upsilon, \tag{8}$$

其中, P_w 表示一个通信块内的平均接收功率, υ 表示检测门限, $\mathcal{D}_0$ 表示判定基站未在通信, 反之为 $\mathcal{D}_1$.

假设 Willie 无法得知关于基站发射时机的任何先验信息, 因此一般认为先验传输概率 $\Pr(\mathcal{H}_0)=\Pr(\mathcal{H}_1)=0.5$. 基于 Willie 检测判决的虚警率 $\Pr(\mathcal{D}_1|\mathcal{H}_0)$ 和漏检率 $\Pr(\mathcal{D}_0|\mathcal{H}_1)$, 其检错概率 ξ 可表示为

$$\xi=\Pr(\mathcal{D}_1|\mathcal{H}_0)+\Pr(\mathcal{D}_0|\mathcal{H}_1). \tag{9}$$

其中, $0\leqslant\xi<1$, $\xi=0$ 表示 Willie 可以完全正确地检测到隐蔽通信, ξ 越趋近于 1 表示其检测结果越不具备可信力. 因此, ξ 又被称为隐蔽概率.

3.2 最优检测性能分析

基于系统的鲁棒性设计原则, 我们考虑 Willie 最优情形, 即 Willie 检测判决的信号样本数量 $N\to\infty$, 且 Willie 具备实时调整检测门限的能力. 此时 Willie 的检错概率可表示为

$$\xi(\upsilon,P_w,\sigma_w^2)=\begin{cases} 0, & \sigma_w^2\leqslant\upsilon\leqslant P_w+\sigma_w^2,\\ 1, & \text{otherwise}, \end{cases} \tag{10}$$

其中, $P_w=Pd_{aw}^{-\alpha}|\boldsymbol{h}_{aw}\boldsymbol{w}|^2$ 表示 Willie 接收隐蔽信号功率. 假设基站采用最大比发送 (maximum ratio transmission, MRT) 预编码, 即 $\boldsymbol{w}=\frac{\boldsymbol{h}_{ab}^{\mathrm{H}}}{\|\boldsymbol{h}_{ab}\|}$, 则此时 Alice 至 Willie 的等效信道增益为 [20]

$$|\boldsymbol{h}_{aw}\boldsymbol{w}|^2=\frac{K_bK_wg_{bw}+g_{aw}}{\|\boldsymbol{h}_{ab}\|^2(K_b+1)(K_w+1)}, \tag{11}$$

其中, $g_{aw}\sim\exp(1)$ 表示 Willie 检测信道的瑞利分量增益, $g_{bw}=[\frac{\sin(M\Phi)}{\sin(\Phi)}]^2[\frac{\sin(L\Theta)}{\sin(\Theta)}]^2$ 表示 Willie 检测信道的莱斯分量增益, $\Phi=\pi\frac{\Delta d}{\lambda}(\sin\theta_b-\sin\theta_w)$ 表示 Willie 与 Bob 的水平相位差, $\Theta=\pi\frac{\Delta d}{\lambda}(\cos\theta_b\sin\varphi_b-\cos\theta_w\sin\varphi_w)$ 表示 Willie 与 Bob 的垂直相位差, $\|\boldsymbol{h}_{ab}\|^2$ 为服从莱斯分布的随机变量.

为便于后续分析, 可用 Nakagami 衰落近似莱斯衰落, 由文献 [21] 可知, $|\boldsymbol{h}_{aw}\boldsymbol{w}|^2$ 是服从 Gamma 分布的随机变量, 进一步可推导得到 P_w 的 PDF (probability density function) 为

$$f_{P_w}(x)=\left(\frac{k_w}{\bar{P}_w}\right)^{k_w}\frac{x^{k_w-1}}{\Gamma(k_w)}\exp\left(\frac{-k_wx}{\bar{P}_w}\right), \tag{12}$$

其中, 形状参数 $\alpha = k_w$, 尺度参数 $\beta = k_w/\bar{P}_w$, $\bar{P}_w = \frac{K_b K_w g_{bw} + LM(K_b+K_w+1)}{LM(K_b+1)(K_w+1)} P d_{aw}^{-\alpha}$, $k_w = \frac{(\tilde{K}_w+1)^2}{2\tilde{K}_w+1}$, $\tilde{K}_w = \frac{K_b K_w g_{bw}}{LM(K_b+K_w+1)}$.

至此, σ_w^2 和 P_w 分别是对数均匀随机变量和 Gamma 随机变量, 而由式 (10) 可知, ξ 服从 Bernoulli 分布, 因此可以进一步计算 Willie 的平均检错概率为

$$\bar{\xi}(\upsilon) = \int_0^\infty \int_0^\infty \xi(\upsilon, x, y) f_{\sigma_w^2}(x)\mathrm{d}x f_{P_w}(y)\mathrm{d}y. \tag{13}$$

考虑 Willie 具备设置最优检测门限的能力, 从而获得最优的检测性能, 即

$$\bar{\xi}^* = \min_{\upsilon} \bar{\xi}(\upsilon). \tag{14}$$

由式 (10) 和 (13) 可知, 当 $\upsilon < \sigma_n^2/\rho$, 有 $\xi(\upsilon, P_w, \sigma_w^2) = 0$, 进一步有 $\bar{\xi}(\upsilon) = 0$; 当 $\upsilon \geqslant \sigma_n^2/\rho$, 计算式 (13) 得到

$$\begin{aligned}
\bar{\xi}(\upsilon) &= \int_0^\infty \int_\upsilon^\infty f_{\sigma_w^2}(x)\mathrm{d}x f_{P_w}(y)\mathrm{d}y + \int_0^\infty \int_0^{\upsilon-y} f_{\sigma_w^2}(x)\mathrm{d}x f_{P_w}(y)\mathrm{d}y \\
&= \begin{cases}
\left(\int_0^\infty \int_\upsilon^{\rho\sigma_n^2} + \int_0^{\upsilon-\sigma_n^2/\rho} \int_{\sigma_n^2/\rho}^{\upsilon-y} \right) \dfrac{1}{2x\ln\rho}\mathrm{d}x f_{P_w}(y)\mathrm{d}y, & \rho/\sigma_n^2 \leqslant \upsilon < \rho\sigma_n^2, \\
\left(\int_{\upsilon-\rho\sigma_n^2}^{\upsilon-\sigma_n^2/\rho} \int_{\sigma_n^2/\rho}^{\upsilon-y} + \int_0^{\upsilon-\rho\sigma_n^2} \int_{\sigma_n^2/\rho}^{\rho\sigma_n^2} \right) \dfrac{1}{2x\ln\rho}\mathrm{d}x f_{P_w}(y)\mathrm{d}y, & \upsilon \geqslant \rho\sigma_n^2.
\end{cases}
\end{aligned} \tag{15}$$

进一步对式 (15) 关于 υ 求导计算极小值点, 或者借鉴文献 [6] 关于最优检测门限的证明思路, 都可得到最优检测门限为噪声不确定程度的上界, 即 $\upsilon^* = \rho\sigma_n^2$. 代入 υ^* 至式 (15) 并计算积分后即可得 Willie 最小平均检错概率, 也即系统最小平均隐蔽概率:

$$\bar{\xi}^*(P) = \int_0^{(\rho-1/\rho)\sigma_n^2} \frac{1}{2\ln\rho} \ln \frac{\rho\sigma_n^2}{y + \sigma_n^2/\rho} f_{P_w}(y)\mathrm{d}y. \tag{16}$$

4 隐蔽威胁区域构建

考虑到实际场景中无法获知敌方位置和分布规律的一般情形, 本节重点构建了隐蔽威胁区域这一新的隐蔽性能评价指标来描述系统所面临的未知检测威胁. 首先给出了通信速率及连接中断概率闭式表达式, 提出了最大隐蔽吞吐量优化问题并设计了一种搜索算法. 随后, 首次定义了隐蔽威胁区域, 并基于 “隐蔽性约束拟合简化” 和 “可靠性约束搜索简化” 的思想设计了一种轻量级算法. 最后, 定性对比了两种算法的时间复杂度和精确度.

4.1 通信速率及连接中断概率

在通信系统对隐蔽性能没有要求时, 通信速率和连接中断概率分别反映了通信的有效性和可靠性, 下面首先对其进行分析计算. 已知 Alice 至 Bob 的信道增益为

$$\boldsymbol{h}_{az}\boldsymbol{w} = \sqrt{\frac{K_z}{K_z+1}}\bar{\boldsymbol{h}}_{az}\boldsymbol{w} + \sqrt{\frac{1}{K_z+1}}\tilde{\boldsymbol{h}}_{az}\boldsymbol{w}. \tag{17}$$

由于基站采用 MRT 预编码, Alice 至 Bob 的等效信道增益为

$$|\boldsymbol{h}_{ab}\boldsymbol{w}|^2 = \frac{LMK_b + g_{ab}}{K_b+1}, \tag{18}$$

其中, Gamma 随机变量 $g_{ab} \sim \Gamma(LM,1)$ 表示用户信道的瑞利分量增益. 则 Bob 的接收信噪比表示为

$$\gamma_b = \bar{\gamma}_b |\boldsymbol{h}_{ab}\boldsymbol{w}|^2, \tag{19}$$

其中, $\bar{\gamma}_b = P d_{ab}^{-\alpha}/\sigma_b^2$ 表示 Bob 的单位接收信噪比. 类似地, 可用 Nakagami 衰落近似莱斯衰落, 则 γ_b 是服从 Gamma 分布的随机变量, 进一步可得其 PDF 为

$$f_{\gamma_b}(\gamma) = \left(\frac{k_b}{\bar{\gamma}_b}\right)^{LMk_b} \frac{\gamma^{LMk_b-1}}{\Gamma(LMk_b)} \exp\left(-\frac{k_b\gamma}{\bar{\gamma}_b}\right), \tag{20}$$

其中, 形状参数 $\alpha = LMk_b$, 尺度参数 $\beta = k_b/\bar{\gamma}_b$, $k_b = (K_b+1)^2/(2K_b+1)$.

至此, Alice 至 Bob 的下行通信速率可表示为

$$R_b = \log_2(1+\gamma_b). \tag{21}$$

由于 γ_b 的随机性, 显然 R_b 会存在上下波动, 其连接中断概率可表示为

$$p_{\text{out}} = \Pr(R_b < R), \tag{22}$$

其中, R 表示目标通信速率. 假设 Bob 侧不受噪声不确性影响, 可进一步计算 p_{out} 为

$$\begin{aligned} p_{\text{out}}(P,R) &= \Pr(\log_2(1+\gamma_b) < R) \\ &= \int_0^{2^R-1} f_{\gamma_b}(\gamma)\,\mathrm{d}\gamma \\ &= \int_0^{2^R-1} \left(\frac{k_b}{\bar{\gamma}_b}\right)^{LMk_b} \frac{\gamma^{LMk_b-1}}{\Gamma(LMk_b)} \exp\left(-\frac{k_b\gamma}{\bar{\gamma}_b}\right)\mathrm{d}\gamma \\ &= \frac{\Upsilon(LMk_b, (2^R-1)\frac{k_b}{\bar{\gamma}_b})}{\Gamma(LMk_b)}, \end{aligned} \tag{23}$$

其中, Gamma 函数 $\Gamma(\alpha) = \int_0^\infty \mathrm{e}^{-t}t^{\alpha-1}\mathrm{d}t$, 不完全 gamma 函数 $\Upsilon(\alpha,\mu) = \int_0^\mu \mathrm{e}^{-t}t^{\alpha-1}\mathrm{d}t$.

4.2 最大隐蔽吞吐量及其搜索算法

基于设定的目标通信速率 R 以及推导的连接中断概率 p_{out}, 可得系统吞吐量 $(1-p_{\text{out}})R$, 则满足系统隐蔽性约束、可靠性约束和最大发射功率约束的最大系统吞吐量即为最大隐蔽吞吐量, 即

$$\max_{P,R} \eta = (1-p_{\text{out}})R, \tag{24a}$$

$$\text{s.t. } \bar{\xi}^*(P) \geqslant 1-\varepsilon, \tag{24b}$$

$$p_{\text{out}}(P,R) \leqslant \delta, \tag{24c}$$

$$P \leqslant P_{\max}. \tag{24d}$$

这是一个含 3 个约束条件的二维优化问题, 理论上可以直接通过穷举搜索求出最优解, 但实际上由于极高的计算复杂度而不可能实现, 因此我们首先对该优化问题展开分析. 遵循参考文献 [6] 的优化问题分析思路, 我们发现 η 关于 P 单调递增、关于 p_{out} 单调递减, 而 $\bar{\xi}$ 和 p_{out} 都关于 P 单调递减, 因此为求得最大的隐蔽吞吐量 η^*, 最优发射功率 P^* 应为满足 3 个约束的最大发射功率. 确定 P^* 后, 当 $R \to 0$ 或 $R \to \infty$ (导致 $p_{\text{out}} \to 1$), 有 $\eta = (1-p_{\text{out}})R \to 0$, 因此存在最优目标发射功率 R^* 使 η 最大. 但由于 R^* 的解析式在数学上很难求得, 因此先通过可靠性约束 (24c) 取等确定 R 的上界 R^{Δ}, 再通过在区间 $R \in (0, R^{\Delta}]$ 内进行穷尽搜索, 求得 R^* 和 η^*. 上述分析和求解过程经梳理如算法 1 所示.

Algorithm 1 Search algorithm for maximum covert throughput

Input: Covertness requirement ε, reliability requirement δ, and maximum transmit power requirement $P_{\max}$.

Output: Maximum covert throughput η^*, optimal transmit power P^*, and optimal target rate R^*.

1: Transform the covertness constraint into an equality, and solve the integral equation $\bar{\xi}^*(P)=1-\varepsilon$ for P^{Δ} through binary search. Then, obtain $P^*=\min\{P^{\Delta},P_{\max}\}$ under the maximum transmit power constraint;

2: Transform the reliability constraint into an equality, and obtain R^{Δ} by solving the integral equation $p_{\text{out}}(P^*,R)=\delta$;

3: Set the searching range as $R\in(0,R^{\Delta}]$, and obtain R^* and η^* through one-side exhaustive search.

4.3 隐蔽威胁区域及其轻量级算法

定义1 (隐蔽威胁区域) 已知系统当前隐蔽性要求 ε、可靠性要求 δ、最大发射功率要求 $P_{\max}$ 和隐蔽吞吐量要求 η_l, 针对无法获知敌方位置信息的情形, 定义系统服务区域内 Bob 的隐蔽威胁区域为

$$\text{Area}_D\left(x,y\right)=\left\{(\varphi,D(\varphi))|\eta^*(x,y)<\eta_l,\varepsilon,\delta,P_{\max},(x_b,y_b),r\right\}, \tag{25}$$

其中, $\text{Area}(x,y)=\{\sqrt{x^2+y^2}\leqslant r\}$ 表示基站的服务区, r 表示基站服务半径, Bob 在相对基站方向 $\varphi\in[0,2\pi]$ 距离 $D(\varphi)$ 处, 坐标为 (x_b,y_b), $\eta^*(x,y)$ 表示 Bob 相对 Willie 位于 (x,y) 时的最大隐蔽吞吐量.

显然, 数学上很难求得 $\text{Area}_D\left(x,y\right)$ 的解析式. 容易想到的是基于算法 1 的隐蔽威胁区域一般搜索算法, 即通过算法 1 求解 Willie 位于服务区内任意位置时系统的最大隐蔽吞吐量 $\eta^*(x,y)$, 再与隐蔽吞吐量要求 η_l 进行比较判决, 确定当前 Willie 所处位置是否对隐蔽通信构成威胁, 接着将 Willie 位置遍历整个系统服务区域, 最终得到隐蔽威胁区域 $\text{Area}_D\left(x,y\right)$. 事实上, 算法 1 虽然能够比较精准地求解 $\eta^*(x,y)$, 但是包含两次二分法搜索以及一次单边穷尽搜索, 且搜索过程中包含计算复杂积分和求解积分方程, 算法的时间复杂度较高, 想要借助上述一般搜索算法来快速构建具有高分辨率的隐蔽威胁区域难度极大. 因此, 为满足实际应用中对于隐蔽区域构建的高时效性需求, 亟需设计一种具备低误差率和低时间复杂度的隐蔽威胁区域轻量级算法.

首先, 鉴于算法 1 对原有隐蔽性约束 (24b) 取等时需要求解相对复杂的积分方程, 因此我们希望借助一种低复杂度且较为准确的隐蔽性约束进行替代, 这里首先想到相对简单的基于信噪比墙的隐蔽性约束 [19]. 根据信噪比墙理论, 通信检测的信噪比墙为

$$\gamma_w^{\text{th}}=\rho-\frac{1}{\rho}, \tag{26}$$

其中, ρ 表示噪声不确定程度且 $\rho>1$. 当 Willie 瞬时接收信噪比小于信噪比墙时, 即 $\gamma_w\leqslant\gamma_w^{\text{th}}$, 可认为系统能够实现隐蔽通信. 事实上, 虽然基于信噪比墙的隐蔽性约束计算极为简单, 但只确保了隐蔽概率大于零, 要想实现高性能隐蔽通信, 仍然需要先建立 γ_w 与 $\bar{\xi}^*$ 的函数关系. 已知 $\gamma_w=P_w/\sigma_w^2$, 其中 σ_w^2 和 P_w 分别是对数均匀随机变量和 Gamma 随机变量, 因此相较于 $\bar{\xi}^*(P)$, $\bar{\xi}^*(\gamma_w)$ 的解析式仍会是类似式 (16) 的复杂积分形式, 可预见后续求解也不会得到简化. 不过我们注意到 Willie 平均接收信噪比是与瑞利衰落无关的常量, 即

$$\bar{\gamma}_w(P)=\frac{K_bK_wg_{bw}+LM\left(K_b+K_w+1\right)}{LM\left(K_b+1\right)\left(K_w+1\right)}\frac{Pd_{aw}^{-\alpha}}{\sigma_n^2}. \tag{27}$$

进一步的, 我们在计算简便但误差较大的信噪比墙隐蔽性约束和计算复杂但十分精确的原有隐蔽性约束之间取了折中, 提出了一种基于信噪比墙拟合的隐蔽性约束, 即

$$\mu\bar{\gamma}_w(P)\leqslant\gamma_w^{\text{th}}, \tag{28}$$

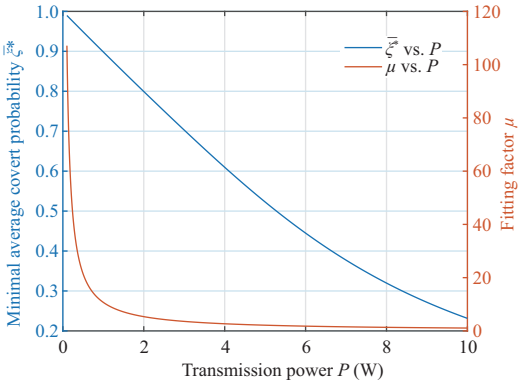


图 2　(网络版彩图) 最小平均隐蔽概率 $\bar{\xi}^*$ 和拟合因子 μ 关于发射功率 P 的变化曲线

Figure 2　(Color online) Minimal average covert probability $\bar{\xi}^*$ and fitting factor μ versus transmission power P

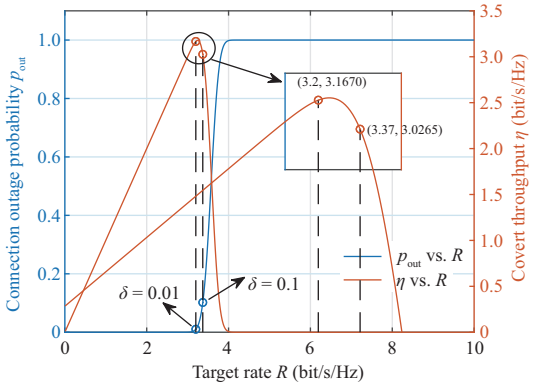


图 3　(网络版彩图) 连接中断概率 p_{out} 和隐蔽吞吐量 η 关于目标速率 R 的变化曲线

Figure 3　(Color online) Connection outage probability p_{out} and covert throughput η versus target rate R

其中, μ 为拟合因子, 理论上可由两种隐蔽性约束式 (24b) 和 (28) 取等后联立方程求得精确解, 但显然无法获得其解析表达式, 仍然需要使用搜索方法. 为此, 我们利用相对简单的图像法解方程来求得 μ 的数值解, 如图 2 所示, 即对于系统给定的隐蔽性要求 ε, 我们可以快速得到 $(\bar{\xi}^*, \mu)$ 的拟合解, 如 $(0.99, 110)$ 和 $(0.90, 11)$. 需要注意的是, 当基站天线数和服务半径、噪声水平和不确定程度、莱斯因子等系统参数变化时, μ 都需要重新配置, 但配置方法不发生改变; 而当 Willie 位置变化时, 经验证 μ 关于 P 的变化曲线对 d_{aw} 是慢变的, 因此可近似在基站服务区内拟合配置相同的 μ. 总的来说, 采用所提基于信噪比墙拟合的隐蔽性约束能明显减小算法 1 的时间复杂度, 但显然也会损失一定的精确度.

另外, 我们尝试对算法 1 中关于可靠性约束的搜索过程进行简化. 虽然无法求得关于 η 极大值点 $R_{\max}$ 的数学解析式, 但是其数值解可以从 η 关于 R 的变化曲线中直接得到, 如图 3 所示. 不难发现, η 仅有一个极大值点, p_{out} 大多数时候趋于 0 或 1, 仅在 R 的一小段区间内从 0 急剧递增到 1. 考虑到实际系统的可靠性要求通常很高, 以图中 $\delta = 0.01$ 和 $\delta = 0.1$ 为例, 分别求解方程 $p_{\text{out}}(P^*, R) = \delta$ 得到 $R^{\Delta} = 3.2$ 和 $R^{\Delta} = 3.37$, 而 $R_{\max} = 3.24$, 其对应 $p_{\text{out}}^{\max} = 0.0192$. 因此, 求解 η^* 的关键在于 δ 与 $p_{\text{out}}^{\max}$ 的大小, 当 $\delta < p_{\text{out}}^{\max}$ 时, 有 $R^{\Delta} < R_{\max}$, 进而有 $R^* = R^{\Delta}$, $\eta^* = (1-\delta)\, R^{\Delta}$, 此时可以省去算法 1 中步骤 3 的单边穷尽搜索; 而当 $\delta \geqslant p_{\text{out}}^{\max}$, 有 $R^{\Delta} \geqslant R_{\max}$, 进而有 $R^* = R_{\max}$, $\eta^* = (1 - p_{\text{out}}^{\max})\, R_{\max}$, 此时可以进一步省去算法 1 中步骤 2 的二分法搜索. 至此, 我们完成了对可靠性约束搜索求解过程的简化.

基于以上分析和简化, 我们提出一种隐蔽威胁区域轻量级算法, 如算法 2 所示.

总的来说, 算法 2 在算法 1 的基础上遵循 “隐蔽性约束拟合简化” 和 “可靠性约束搜索简化” 这两点简化思想进行了轻量化设计, 在牺牲一定精确度的前提下提高了算法的实时性以及实用性. 具体来说, 第 1 点简化思想通过引入拟合因子 μ 具体从 “图像法求方程拟合解” 和 “近似在服务区内拟合配置相同的 μ” 两个方面对求解 P^* 的过程进行了简化, 虽然不可避免地产生了一些误差, 但极大地降低了算法的时间复杂度; 第 2 点简化思想利用了 η 和 p_{out} 关于 R 变化曲线的单调特性以及极值点比较, 仅省去了不必要的搜索过程, 因而在提升算法实时性同时没有降低算法的精确度. 可见两种算法的时间复杂度和精确度定性对比符合我们的直观认识, 后续仿真实验将给出定量验证.

表 1　仿真参数

Table 1　Simulation parameters

Channel model	Antenna model at Alice	Antenna model at Bob and Willie
Rician fading with $K_b = K_w = 3$	$L \times M = 8 \times 4$, $T = 30$ m, $\Delta d/\lambda = 1$	Single antenna
Beamforming mode	Service radius of base station	Path loss exponent
MRT	$r = 100$ m	$\alpha = 3$
Position of Alice	Position of Bob	Position of Willie
(0, 0)	(30, 30)	(20, 25)
Noise level	Noise uncertainty level	Maximum transmission power requirement
$\sigma_b^2 = \sigma_n^2 = -30$ dB	$\rho = 1.1$	$P_{\max} = 10$ W
Covertness requirement	Reliability requirement	Maximum covert throughput requirement
$\varepsilon = 0.1$	$\delta = 0.01$	$\eta_l = 0.1$ bit/s/Hz

Algorithm 2 Lightweight search algorithm for covert threat region

Input: Covertness requirement ε, reliability requirement δ, maximum transmit power requirement $P_{\max}$, and covert throughput requirement η_l.

Output: Covert threat region $\mathrm{Area}_D\,(x, y)$.

1: Calculate the fitting factor μ through image method. Transform the fitting covertness constraint (28) into an equality and compute $P^{\Delta} = \frac{LM\sigma_n^2\gamma_w^{\mathrm{th}}(K_b+1)(K_w+1)}{\mu d_{aw}^{-\alpha}(K_bK_wg_{bw}+LM(K_b+K_w+1))}$. Then, obtain $P^* = \min\{P^{\Delta}, P_{\max}\}$ under the maximum transmit power constraint (24d);

2: Compute the numerical solution of the maximum point $R_{\max}$ for η, and obtain the corresponding $p_{\mathrm{out}}^{\max}$. Next, obtian $\eta^* = (1 - p_{\mathrm{out}}^{\max})\,R_{\max}$ directly when $\delta \geqslant p_{\mathrm{out}}^{\max}$. Otherwise, when $\delta < p_{\mathrm{out}}^{\max}$, transform the reliability constraint (24c) into an equality and obtain R^{Δ} by solving the integral equation $p_{\mathrm{out}}(P^*, R) = \delta$, as well as $\eta^* = (1 - \delta)\,R^{\Delta}$;

3: Traverse the whole system service area with the position of Willie, and calculate $\eta^*(x, y)$. At last, obtain $\mathrm{Area}_D\,(x, y)$ with the comparison of η_l.

5　仿真分析

本节主要从最小平均隐蔽概率、最大隐蔽吞吐量、隐蔽威胁区域, 以及算法的精确度和时间复杂度 4 个方面进行仿真实验, 分析系统的隐蔽性能、总体性能, 以及所提算法性能. 无特殊声明时, 仿真参数设置如表 1 所示.

5.1　最小平均隐蔽概率

首先我们通过图 4 揭示了噪声对系统隐蔽性能的影响. 我们发现最小平均隐蔽概率 $\bar{\xi}^*$ 随噪声不确定程度 ρ 单调递增, 且增长趋势逐渐趋于平缓. 当 $\rho = 1$, 即噪声确定时, 有 $\bar{\xi}^* = 0$, 说明存在噪声不确定是确保系统能够实现隐蔽的前提. 另外, 增大噪声水平 σ_n^2 也能提升 $\bar{\xi}^*$, 且 σ_n^2 的大小基本决定了 $\bar{\xi}^*$ 的上界, 这说明实现系统高概率隐蔽需要相对较大的噪声水平. 总的来说, 上述现象都是因为噪声水平和不确定程度的大小密切影响着 Willie 的检测性能.

图 5 展示了 Willie 位于不同位置时系统的最小平均隐蔽概率. 为保证 $\bar{\xi}^*$ 计算结果的正确性, 其积分计算精度要求较高, 又考虑到 $\bar{\xi}^*$ 热力图生成的时效性, 我们将 Willie 位置变化刻度设置为 1×1. 不难发现, $\bar{\xi}^*$ 的热区形状类似于波束成形的主瓣区, 且 Willie 越靠近 Bob, 系统的 $\bar{\xi}^*$ 越接近零, 这是因为主瓣区信号能量集中, 有利于 Willie 的能量检测及正确判决. 另外, 由于波束旁瓣效应, 当 Willie 位于旁瓣覆盖区域时, 系统隐蔽性能也相对较差. 而当 Willie 比较靠近基站 Alice 时, 由于部分泄露信

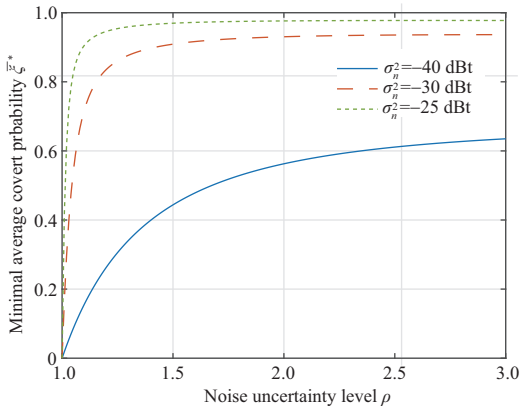


图 4 (网络版彩图) 最小平均隐蔽概率 $\bar{\xi}^*$ 关于噪声不确定程度 ρ 和噪声水平 σ_n^2 的变化曲线

Figure 4 (Color online) Minimal average covert probability $\bar{\xi}^*$ versus noise uncertainty level ρ and noise level σ_n^2

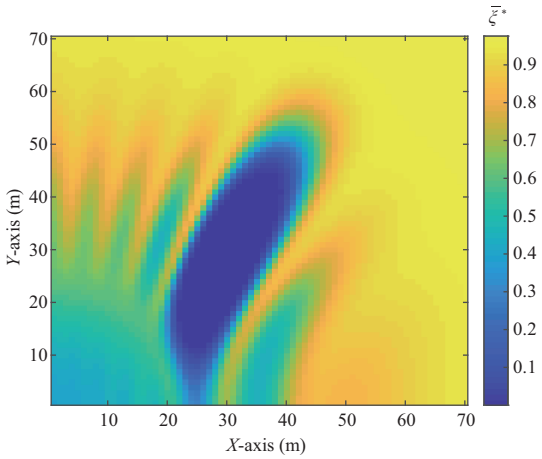


图 5 (网络版彩图) 最小平均隐蔽概率 $\bar{\xi}^*$ 关于 Willie 位置变化的热力图 ($P = 10$ W)

Figure 5 (Color online) Thermogram of the minimal average covert probability $\bar{\xi}^*$ versus the Willie's position ($P = 10$ W)

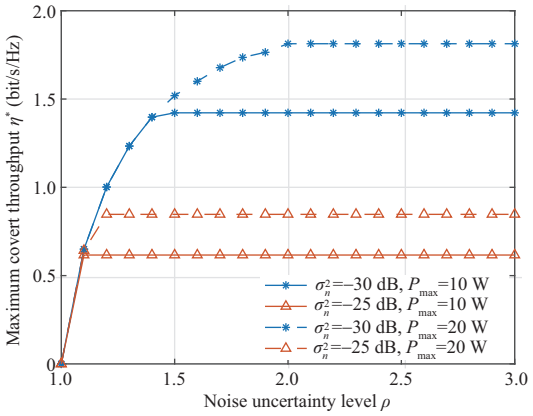


图 6 (网络版彩图) 最大隐蔽吞吐量 η^* 关于噪声不确定程度 ρ、噪声水平 σ_n^2 和最大发射功率 $P_{\max}$ 的变化曲线

Figure 6 (Color online) Maximum covert throughput η^* versus noise uncertainty level ρ, noise level σ_n^2, and maximum transmission power P

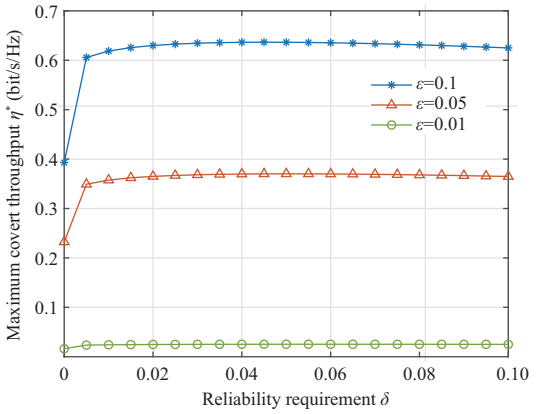


图 7 (网络版彩图) 最大隐蔽吞吐量 η^* 关于可靠性要求 δ 和隐蔽性要求 ε 的变化曲线

Figure 7 (Color online) Maximum covert throughput η^* versus reliability requirement δ and covertness requirement ε

号传播的路径损耗很小, 导致 Willie 接收信号功率较大, 系统隐蔽性能同样不高.

5.2 最大隐蔽吞吐量

图 6 展示了在给定 Willie 位置、系统隐蔽性及可靠性要求下, 噪声和最大发射功率要求对最大隐蔽吞吐量的影响. 可以发现 η^* 随 ρ 先单调递增, 然后保持恒定. 这是因为当 ρ 较小时, 为了满足隐蔽性约束, 最优发射功率 P^* 相对较小, 相应 η^* 较小; 而当 ρ 大于一定阈值, 此时隐蔽性要求更容易满

足, 但由于最大发射功率 $P_{\max}$ 的限制, η^* 不再增大, 因此从图中也可以发现增大 $P_{\max}$ 能够提升 η^* 的上限. 另外, 虽然增大噪声水平 σ_n^2 更有利于实现高概率隐蔽, 但由于噪声对通信本身固有的不利影响, 增大 σ_n^2 也会拉低 η^* 的上限.

进一步的, 图 7 揭示了系统可靠性要求和隐蔽性要求对最大隐蔽吞吐量的影响. 首先可以发现增大 ε 能够提升, 这与我们直观认识一致, 即对系统的隐蔽性要求越宽松, 相同条件下系统所能达到的隐蔽吞吐量越大. 另外, η^* 随 δ 先单调递增, 然后几乎保持恒定, 其中的原因可以用图 3 中连接中断概率 p_{out} 关于目标速率 R 的变化来简单解释, 关键还在于 δ 与目标速率极大值点 $R_{\max}$ 所对应 $p_{\text{out}}^{\max}$ 的大小关系, 即一旦 $\delta \geqslant p_{\text{out}}^{\max}$, η^* 即可取得最大值. 值得一提的是, 图中 η^* 的缓慢下降趋势是由于当 δ 较大时, 关于搜索最优目标速率 R^* 的搜索区间变大, 从而导致最终求解结果 η^* 的误差略微变大.

5.3 隐蔽威胁区域

基于 4.3 小节所设计的隐蔽威胁区域轻量级算法, 并依据表 1 中默认的仿真参数, 我们首先快速构建了具有高分辨率的最大隐蔽吞吐量热力图及隐蔽威胁区域, 如图 8(a) 所示, 并以此作为对照组, 对比分析了一些主要系统参数对隐蔽威胁区域的影响, 如图 8(b)–(h) 所示.

图 8(a) 首先展示了最大隐蔽吞吐量 η^* 随 Willie 位置变化的热力图, 其中隐蔽威胁区域已标红. 可以发现隐蔽威胁区域位于靠近 Bob 的部分主瓣区, 直观上来理解, 因为该部分区域信号能量最为集中, 有利于 Willie 对抗噪声不确定性, 迫使满足隐蔽性要求和可靠性要求的最大发射功率很小, 最终导致 $\eta^* < \eta_l$. 另外可以发现, 当 Willie 位于旁瓣区域或比较靠近 Alice 时, η^* 也相对较小, 这分别是由于波束旁瓣效应以及信号传播的低路径损耗造成的.

当莱斯因子 K 增大 10 倍后, 热力图及隐蔽威胁区域如图 8(b) 所示. 此时 $K_b = K_w = 30$, 视距信号功率远大于多径信号功率, 波束成形的能量泄露减少, 系统服务区内 η^* 的上界增大. 除此之外, 此时的隐蔽威胁区域变成了点环状, 根本上是由于 Willie 检测信道的莱斯分量增益 g_{bw} 随距离 d_{bw} 的起伏式衰减而造成了 η^* 在主瓣区的波小幅度动, 再结合 η_l 的设置, 最终形成了点环状隐蔽威胁区域的现象.

图 8(c) 和 (d) 分别改变了天线间距和天线类型. 当增大天线间距, 使其与载波波长比值为 $\Delta d/\lambda = 1.5$ 时, 可以发现隐蔽威胁区域变小, 这是由于基站的波束聚焦能力得到了提升, 不过显然天线阵列所占用的空间也变大了. 另外, 当天线类型由 8×4 均匀平面阵列 UPA 改变为由 32 根天线组成的均匀线性阵列 (uniform linear array, ULA) 时, 可以发现隐蔽威胁区域明显变大. 这是由于 2D 波束成形只能在水平方向提供一定的聚焦能力, 所以当 Willie 靠近基站或者位于波束辐射方向上, Willie 接收信号能量都相对较大, 从而导致 η^* 较小, 对比图 8(a) 也可看出 3D 波束成形对于隐蔽通信的显著优势. 总的来说, 这与我们的直观认识一致, 即通过改变天线构造来尽可能提升波束聚焦能力, 减少目标区域以外的信号能量泄露, 从而在其他条件不变的情况下达到缩小隐蔽威胁区域的目的.

图 8(e) 和 (f) 展示了噪声对隐蔽威胁区域的影响. 可以发现, 当噪声水平提高到 $\sigma_n^2 = -20$ dB 时, η^* 的热区变得非常集中, 但是隐蔽威胁区域几乎没有变化. 因为噪声是所提通信系统的唯一掩体, 无论 Willie 位于什么位置, 增大 σ_n^2 都更有利于系统满足隐蔽性约束, 也就更容易达到 η^* 的上界, 因此热区变得集中; 又因为噪声不利于通信本身, 增大 σ_n^2 也会降低 η^* 的上界, 但综合最优发射功率 P^* 的提高, 隐蔽威胁区域没有变化. 另外, 当噪声不确定程度提高到 $\rho = 1.5$ 时, Willie 正确检测难度明显增大, 由于未考虑噪声不确定对 Bob 接收的影响, 因此可以发现隐蔽威胁区域明显缩小.

最后, 图 8(g) 和 (h) 分别改变了系统可靠性要求和隐蔽性要求. 当可靠性要求提高到 $\delta = 0.001$ 时, 隐蔽威胁区域略微增大; 当隐蔽性要求提高到 $\varepsilon = 0.01$ 时, 隐蔽威胁区域明显增大. 其根本原因在

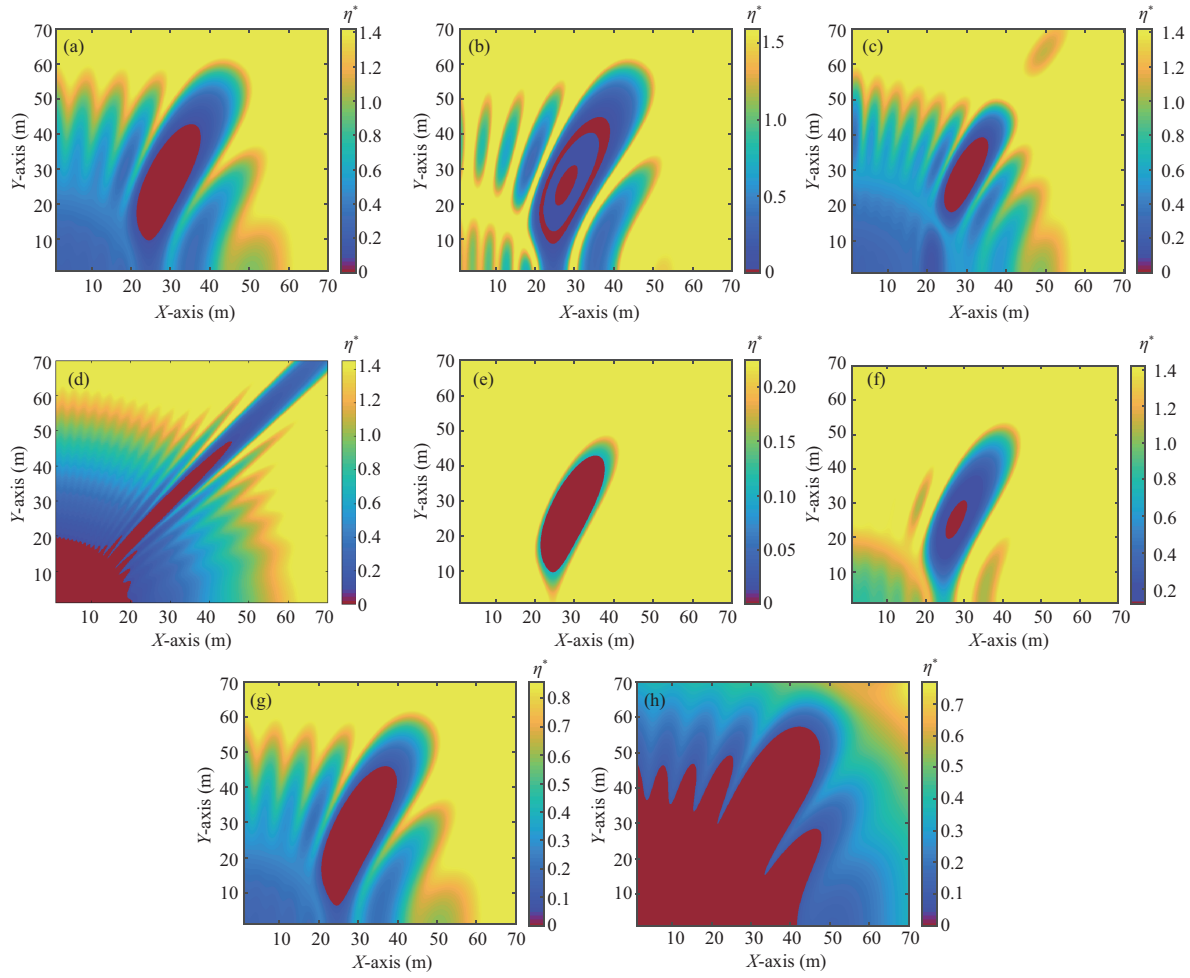


图 8　(网络版彩图) 最大隐蔽吞吐量热力图及隐蔽威胁区域

Figure 8　(Color online) Thermogram of the maximum covert throughput and the covert threat region. (a) Matched group; (b) $K_b = K_w = 30$; (c) $\Delta d/\lambda = 1.5$; (d) ULA with 32 antennas; (e) $\sigma_n^2 = -20$ dB; (f) $\rho = 1.5$; (g) $\delta = 0.001$; (h) $\varepsilon = 0.01$

于对任意位置的 Willie 而言, 提高隐蔽性要求或者过分提高可靠性要求都会降低系统最大隐蔽吞吐量 η^*, 从而导致隐蔽威胁区域的增大.

5.4　算法的精确度和时间复杂度

以算法 1 为基准, 我们通过图 9 定量对比了所提隐蔽威胁区域轻量级算法 (算法 2) 的实时性和精确性. 图 9(a) 为基于算法 1 构建的隐蔽威胁区域, 对比基于算法 2 的图 8(a) 可以发现, 除区域分辨率外直观上难以看出明显差别. 由 4.3 小节分析已知, 算法 2 简化求解 η^* 的误差全部来源于 P^*, 具体如图 9(a) 所示, 观察发现误差相对较大处位于主、旁瓣的外边界. 图 9(c) 和 (d) 进一步展示了 η^* 的误差和误差率, 不难看出误差几乎都在 0.018 以下, 误差率基本都在 2% 以下. 值得注意的是, η^* 的误差率在隐蔽威胁区域和基站远场区域趋近于零, 其原因是两种算法在对应区域所求得的 P^* 分别都为 $P_{\min}$ 或 $P_{\max}$. 此外, 基于同一硬件条件, 两种算法的代码运行时间分别为 629.7 和 29.8 s, 算法 2 的消耗时间下降 95.3%. 总的来说, 通过实验我们验证了算法 2 相较于算法 1 在保留了高精确度特性

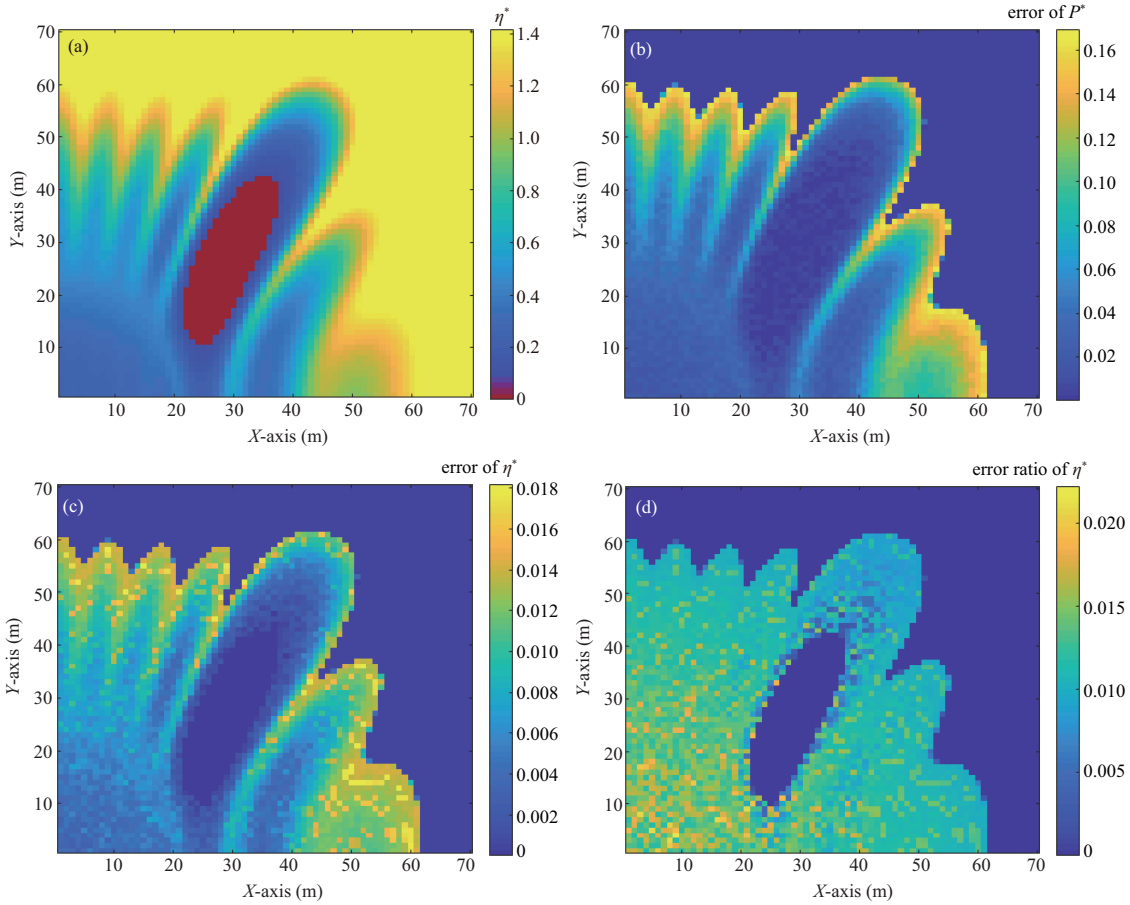


图 9 (网络版彩图) 最优发射功率和最大隐蔽吞吐量误差热力图

Figure 9 (Color online) Thermogram of the optimal transmission power and the maximum covert throughput. (a) Covert threat region based on Algorithm 1; (b) error of P^*; (c) error of η^*; (d) error ratio of η^*

的同时, 极大地降低了算法的时间复杂度, 更普遍地适用于对实时性有一定需求的隐蔽威胁区域构建场景.

总的来说, 我们在系统设计时需要考虑实际的无线信道环境和背景噪声特征, 制定合理的系统隐蔽性要求、可靠性要求, 及隐蔽吞吐量要求, 再基于隐蔽威胁区域构建的实时性、准确性, 及分辨率需求选择合适的算法, 生成最大隐蔽吞吐量热力图及隐蔽威胁区域, 最终完成对当前系统所面临的未知非法检测威胁的评估. 另外, 必要时还可以通过改变天线参数来达到缩小隐蔽威胁区域的目的.

6 结论

本文在莱斯衰落信道和噪声不确定条件下, 首先构建了基于 3D 波束成形的下行隐蔽无线通信系统模型; 其次, 基于信号检测的假设检验理论分析了敌方最优检测性能, 推导了系统最小平均隐蔽概率; 然后, 给出了系统瞬时通信速率及连接中断概率闭式表达式, 求解了给定敌方位置下的系统最大化隐蔽吞吐量优化问题; 最后, 针对实际通信场景中无法获知敌方位置或分布规律的情形, 首次定义了隐蔽威胁区域这一新的系统评价指标, 并设计了相应轻量级算法. 仿真结果验证了系统的隐蔽性能、总

体性能, 以及所提算法性能, 表明了主要系统参数对隐蔽威胁区域的影响. 为尽可能减小系统所面临的未知非法检测威胁, 下一步可针对缩小隐蔽威胁区域的具体方案进行深入研究, 比如向隐蔽威胁区域发送定向人工噪声、利用超材料天线控制波束捷变等.

参考文献

1 Wang J Q. Research on the key technologies for low probability of intercept wireless communication. Dissertation for Ph.D. Degree. Chengdu: University of Electronic Science and Technology, 2019 [王健全. 低截获概率无线通信关键技术研究. 博士学位论文. 成都: 电子科技大学, 2019]

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

3 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

4 He B, Yan S H, Zhou X Y, et al. On covert communication with noise uncertainty. IEEE Commun Lett, 2017, 21: 941–944

5 Hien Q, Sang W K. Covert communication under channel uncertainty and noise uncertainty. In: Proceedings of IEEE International Conference on Communications (ICC), Shanghai, 2019. 211–216

6 Lin Y D, Jin L, Zhou Y, et al. Performance analysis of beamforming based covert wireless communication with uncertain noise. J Commun, 2020, 41: 49–58 [林钰达, 金梁, 周游, 等. 噪声不确定时基于波束成形的隐蔽无线通信性能分析. 通信学报, 2020, 41: 49–58]

7 Sobers T V, Bash B A, Guha S, et al. Covert communication in the presence of an uninformed jammer. IEEE Trans Wirel Commun, 2017, 16: 6193–6206

8 Soltani R, Goeckel D, Towsley D, et al. Covert wireless communication with artificial noise generation. IEEE Trans Wirel Commun, 2018, 17: 7252–7267

9 He B, Yan S H, Zhou X Y, et al. Covert wireless communication with a poisson field of interferers. IEEE Trans Wirel Commun, 2018, 17: 6005–6017

10 Shahzad K, Zhou X Y, Yan S H. Covert communication in fading channels under channel uncertainty. In: Proceedings of Vehicular Technology Conference (VTC Spring), Sydney, 2017. 321–325

11 Tao L W, Yang W W, Yan S H, et al. Covert communication in downlink noma systems with random transmit power. IEEE Commun Lett, 2020, 12: 642–645

12 Zheng T X, Wang H M, Ng D, et al. Multi-antenna covert communications in random wireless networks. IEEE Trans Wirel Commun, 2019, 18: 1974–1987

13 Forouzesh M, Azmi P, Mokari N, et al. Covert communication using null space and 3D beamforming: uncertainty of Willie's location information. IEEE Trans Veh Technol, 2020, 69: 8568–8576

14 Shahzad K, Zhou X Y, Yan S H, et al. Achieving covert wireless communications using a full-duplex receiver. IEEE Trans Wirel Commun, 2018, 17: 8517–8530

15 Shahzad K, Zhou X Y, Yan S H. Covert wireless communication in presence of a multi-antenna adversary and delay constraints. IEEE Trans Veh Technol, 2019, 68: 12432–12436

16 Sun L L, Xu T Z, Yan S H, et al. On resource allocation in covert wireless communication with channel estimation. IEEE Trans Commun, 2020, 11: 4651–4663

17 Liu Z H, Liu J J, Zeng Y, et al. Covert wireless communications in IoT systems: hiding information in interference. IEEE Wirel Commun, 2017, 25: 46–52

18 Li X, Jin S, Suraweera H, et al. Line-of-sight based statistical 3D beamforming for downlink massive MIMO systems. In: Proceedings of IEEE International Conference on Communications (ICC), Kuala Lumpur, 2016. 421–426

19 Tandra R, Sahai A. SNR walls for signal detection. IEEE J Sel Topics Signal Process, 2008, 2: 4–17

20 Song H T. Research on intrinsic security transmission technology for massive MIMO. Dissertation for Master's Degree. Zhengzhou: PLA Strategic Support Force Information Engineering University, 2018 [宋昊天. 面向大规模 MIMO 的内生安全传输技术研究. 硕士学位论文. 郑州: 战略支援部队信息工程大学, 2018]

21 Yan S H, Malaney R. Location-based beamforming for enhancing secrecy in Rician wiretap channels. IEEE Trans Wirel Commun, 2016, 15: 2780–2791

Threat region development of covert wireless communication based on 3D beamforming

Yuda LIN[1*], Liang JIN[1], Kaizhi HUANG[1] & Qian HAN[2]

1. *PLA Strategic Support Force Information Engineering University, Zhengzhou* 450002*, China*;
2. *Purple Mountain Laboratories: Networking, Communications and Security, Nanjing* 211189*, China*
* Corresponding author. E-mail: linyuda.ieu@foxmail.com

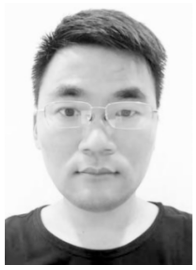
Abstract In order to evaluate the unknown and illegal detecting threat intuitively for real-time covert wireless communication systems, the covert threat region is defined for the first time and the corresponding lightweight algorithm is also designed. Firstly, a system model of downlink covert wireless communication based on 3D beamforming is constructed with Rician fading channel and noise uncertainty. And then the optimal detecting performance of the enemy is analyzed, also the minimum average covert probability of the system is derived. Furthermore, after obtaining the closed-form expressions of communication rate and connection outage probability, the optimization problem for maximum covert throughput with the given position of the enemy is solved. Finally, considering the actual communication scenario where the enemy's location or distribution law cannot be obtained, a new performance measurement called the covert threat region is defined, and the corresponding lightweight algorithm is designed subsequently. Simulation results verify the system covertness performance, overall performance and the performance of the proposed algorithm, and show the influence of main parameters on the covert threat region, such as background noise, channel characteristics, antenna structures, and system requirements.

Keywords covert wireless communication, covert threat region, 3D beamforming, Rician fading, noise uncertainty

Yuda LIN was born in 1994. He received his B.E. degrees in Beijing Institute of Technology in 2017. Currently, he is a successive master-doctor program candidate at PLA Strategic Support Force Information Engineering University in Zhengzhou. His research interests include covert wireless communication and physical layer security.

Liang JIN was born in 1969. He received his Ph.D. degree at Xi'an Jiaotong University, Xi'an, in 1999. Currently, he is a professor at PLA Strategic Support Force Information Engineering University. His research interests include wireless communication, physical layer security, and smart antenna.

Kaizhi HUANG was born in 1973. She received her Ph.D. degree in communication and information system from Tsinghua University. Currently, she he is a professor and serving as a leader of Wireless Mobile Communication Innovation Technology Team at PLA Strategic Support Force Information Engineering University. Her research interests include wireless mobile communication network and physical layer security.



Qian HAN was born in 1987. He received his B.E degree from PLA Strategic Support Force Information Engineering University in Zhengzhou. Currently, he is an engieer at Purple Mountain Laboratories in Nanjing. His research interests include massive MIMO and physical layer security.