研究论文

对抗监察者干扰攻击的博弈策略

吴金星,邸兴,尹川,宋瑞祯,李铁林

摘要 针对主动监察者兼具信号检测与干扰能力时隐蔽通信面临的传输暴露和链路干扰问题,提出一种基于双层博弈的抗监察者干扰隐蔽通信策略。发射机在多个可用信道中随机选择部分信道传输上行信号,接收机采用最大比合并方式进行接收;监察者基于三元假设检验判别空闲信道、人工噪声信道和上行信号信道,并依据检测结果实施针对性干扰。为增加监察者的检测不确定性,协作干扰机在未承载上行信号的可用信道中随机选择部分信道发送人工噪声。在此基础上,分别以最小化上行信号检测概率、最大化检测概率以及最大化检测错误概率为发射机、监察者和协作干扰机的优化目标,在通信信噪比、虚警概率及功率等约束下构建三方双层博弈模型,并对发射信道数量、监察者检测阈值及人工噪声信道数量等策略变量进行联合求解。仿真结果表明,所提策略能够有效增加监察者的检测不确定性,降低上行信号被检测和有效干扰的概率,同时改善合法通信链路的传输性能。研究结果可为主动检测与干扰威胁下的高安全无线通信和抗干扰隐蔽传输提供理论参考。

关键词 隐蔽通信;博弈论;物理层安全;人工噪声;三元假设检验;信道分配

在无线通信系统中,确保安全性是最重要的问题之一。为了保护隐私信息,物理层安全技术引起了广泛关注[1]。尽管物理层安全技术可以保护隐私信息的内容不被窃听,但通信行为本身仍然暴露了敏感信息[2]。与物理层安全技术不同,隐蔽通信在更高层次上保证了无线通信的安全性,可以屏蔽通信行为,使其不被潜在的监视者发现[3]。

隐蔽通信在过去 10 年中得到了广泛研究。Bash-等[3]发现了在加性高斯白噪声信道上的隐蔽通信的平方根定律之后,多种技术和场景被用来提高隐蔽性能。Shahzad 等[4]通过分析监视者的固有噪声不确定性,提高了隐蔽通信的速率。Sobers 等[5]和 Zheng 等[6]通过引入协作干扰机来增加监视者的干扰不确定性,从而保护传输。目前,隐蔽通信技术在隐蔽认知无线电系统[7]、智能反射面[8]、中继网络[9]及时间敏感网络[10]等领域引起了广泛关注。

尽管隐蔽通信在各种无线场景中得到了广泛研究,但大多数研究假设监察者仅具有检测能力,现有研究较少关注隐蔽失败的风险。事实上,在做出决策之前检测每个时隙是可行的。Ma 等[11]假设认知用户首先检测主用户的存在,然后决定是否传输。此外,监视者可能还具有干扰能力。Che 等[12]提出,监察者通过干扰辅助诱导发射机增加传输功率。总之,具有主动干扰能力的监视者可能对隐蔽通信构成潜在风险。

为了解决上述问题,本研究考虑了一个监视者,其目的不仅是检测上行传输,还要干扰通信。协作干扰机发送诱饵以迷惑功率受限的监视者。因此,监视者可能会将干扰功率分配给空闲信道,此时激活信道的检测概率和干扰程度都会降低。基于此场景,本研究提出三方通信终端的双层博弈模型。发送端和监察者分别在下层博弈中解决用于传输的信道数量和

中国飞行试验研究院,西安 710089

收稿日期:2025-09-03;修回日期:2026-02-09

作者简介:吴金星,高级工程师,研究方向为飞行试验,电子信箱:jinxingwu_xidian@163.com

引用格式:吴金星,邸兴,尹川,等. 对抗监察者干扰攻击的博弈策略[J]. 科技导报,2026,44(18):152-158;doi:10.3981/j.issn.1000-7857.2025.09.00016

三元假设检验的阈值。接收端和协作干扰机在上层博弈中工作,并根据下层博弈的结果计算发送人工噪声的信道数量问题。

1　系统模型

如图 1 所示,考虑在有监察者(W)存在的情况下,信源(A)向接收机(B)进行上行隐蔽传输的场景。在每个时隙中,A 被激活的概率为 p。若 A 被激活,她将会在 M 个信道中随机选择 c 条信道,并将传输功率平均分配到这些信道上传输上行信号。B 使用最大比合并(maximal ratio combining, MRC)来接收上行信号。监察者在检测阶段确定是否存在上行信号并进行干扰。若 W 认为某条信道存在 A 的信号,则对该信道施加干扰。如果 W 的检测结果是不存在上行信号,则在所有 M 个信道上发送干扰。合法系统为了迷惑 W,设置协作干扰器(J)通过发送人工噪声保持 v 个信道活跃($v>c$)。协作干扰机所选择发送人工噪声的 $v-c$ 条信道,与信源 A 用于上行传输的 c 条信道是彼此正交、互不重叠的。因此,从物理层信号接收的角度看,合法接收机 B 在接收其期望的上行链路信号时,完全不会受到协作干扰机 J 所发人工噪声的任何带内干扰。

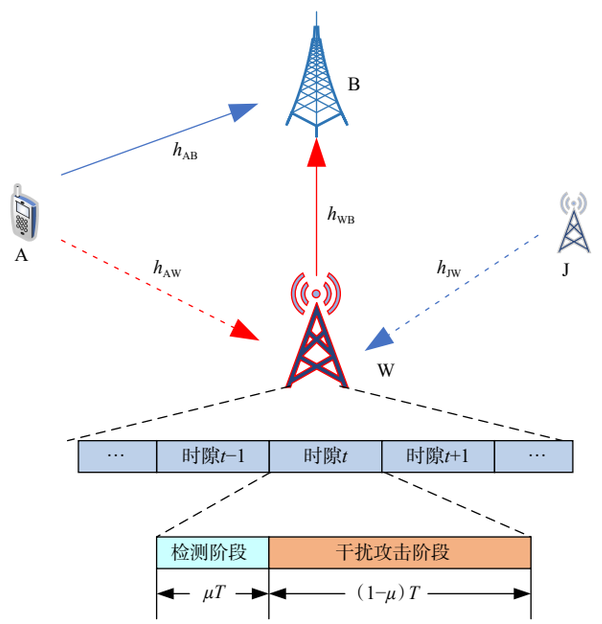


图 1　系统模型

本研究假设 h_{sr}^{k} 表示从 s 到 r 的第 k 条信道,其中,$s\in\{a,j,w\}$ 且 $r\in\{w,b\}$,a、j、w、b 分别代表信源、协作干扰机、监察者和接收机。在 B 的接收信道中采用瑞利衰落。考虑到对合法用户不利的情况,假设 W 在加性高斯白噪声信道中接收信号。假设 P_T 和 P_W 分别表示 A 和 W 所使用的传输功率。采用 P_{A}^{M}、P_{J}^{M}、P_{W}^{M} 分别表示信源、干扰器和监察者的最大功率。由于 A 均匀地将功率分配给 c 条信道,可得 $P_T=P_{\mathrm{A}}^{M}/c$。类似地,$P_W=P_{\mathrm{W}}^{M}/N_d$,其中 N_d 表示 W 检测后认为 A 所使用的信道数量。当 A 被激活时,J 的总功率被平均分配,每条信道功率为 $P_{AN}=P_{\mathrm{J}}^{M}/v$;而当 A 未被激活时,功率 $P_{AN}=P_{\mathrm{J}}^{M}/(v-c)$ 将用于 $v-c$ 个信道。A_t、J_t、W_t 分别表示在第 t 个时隙中 A 使用的信道集合、J 使用的信道集合及 W 干扰的信道集合。

假设 W 不仅能检测到 A 的传输,还能干扰 B 的接收。因此,在每个时隙中,对于 W 来说,首先需要检测并判断每个信道中是否存在 A 的信号,然后对存在上行信号的信道进行干扰。W 检测 A 的时长为 μT,然后干扰 B 的时长为 $(1-\mu)T$。假设 W 在每个信道中于 T 内能够检测 D 个符号。

2　监察者检测性能分析

W 采用三元假设检验模型来检测上行链路传输[13]。基于每个信道的独立三元假设检验问题,定义并计算 W 的错误检测概率。

2.1　假设检验

在 H_0(A 和 J 均不存在)、假设 H_1(J 存在)和 H_2(A 存在)3 种情况之间进行三元假设检验

$$\begin{cases}\mathcal{H}_0, & y_w^{k,t}=n_w^{k,t}\\ \mathcal{H}_1, & y_w^{k,t}=\sqrt{P_{AN}}j+n_w^{k,t}\\ \mathcal{H}_2, & y_w^{k,t}=\sqrt{P_T}s+n_w^{k,t}\end{cases}\tag{1}$$

式中,符号 $n_w^{k,t}$ 表示在第 t 个检测时隙中第 k 个符号的加性高斯白噪声,其方差为 σ_0^2;干扰信号用 j 表示,上行信号用 s 表示。

在检测阶段,W 使用似然比检验(likelihood ratio test, LRT)来寻找 A。首先,确定信道是空闲还是忙碌。其次,当信道忙碌时,确定信号是由 A 还是 J 发送的。因此,可以将三元假设检验分为以下 2 个二元假设检验问题

$$L_0=\frac{p(y;\mathcal{H}_2)}{p(y;\mathcal{H}_0)}\gtrless\lambda_0,\ L_1=\frac{p(y;\mathcal{H}_2)}{p(y;\mathcal{H}_1)}\gtrless\lambda_1 \tag{2}$$

式中,λ_0,λ_1为二元假设检验问题的 2 个判决阈值。

很容易就能得到空闲与忙碌状态之间的判决准则

$$Y=\sum_{d=0}^{D-1}(y[d])^2\lessgtr\eta_0=\frac{D}{2}\ln\frac{\sigma_0^2}{\sigma_2^2}+\frac{\sigma_0^2-\sigma_2^2}{2\sigma_0^2\sigma_2^2}+\ln\lambda_0 \tag{3}$$

从式(3)可以看出,当 W 检测到$L_0<0$且$Y<\eta_0$时,信道状态将会被判断为空闲状态。根据概率分布函数$Y\sim\chi_D^2$可得,当 H_0 为实际状态时,W 认定信道状态为空闲的概率可写作

$$\begin{aligned}P(\mathcal{D}_0|\mathcal{H}_0)&=\int_0^{\eta_0/\sigma_0^2}\frac{1}{2^{N/2}\Gamma(D/2)}y^{N/2-1}e^{-y/2}\mathrm{d}y\\&=1-\frac{\Gamma(D/2,\eta_0/\sigma_0^2)}{\Gamma(D/2)}\end{aligned} \tag{4}$$

式中,$\Gamma(s,x)$是上不完全伽马函数,$\Gamma(x)$是伽马函数。

假设辅助干扰节点的功率不小于 A,即$P_T\leqslant P_J$情况进行分析。检测概率可写作

$$\Pr(\mathcal{D}_2\mid\mathcal{H}_2)=\frac{\Gamma(D/2,\eta_0/\sigma_2^2)}{\Gamma(D/2)}-\frac{\Gamma(D/2,\eta_1/\sigma_2^2)}{\Gamma(D/2)} \tag{5}$$

其判决准则可写作

$$\begin{cases}\mathcal{H}_0, & Y<\eta_0\\ \mathcal{H}_1, & \eta_1\leqslant Y\\ \mathcal{H}_2, & \eta_0\leqslant Y<\eta_1\end{cases} \tag{6}$$

根据上述准则,可以得到 $\Pr(\mathcal{D}_2\mid\mathcal{H}_0)=\frac{\Gamma(D/2,\eta_0/\sigma_0^2)}{\Gamma(D/2)}-\frac{\Gamma(D/2,\eta_1/\sigma_0^2)}{\Gamma(D/2)}$,$\Pr(\mathcal{D}_2\mid\mathcal{H}_1)=\frac{\Gamma(D/2,\eta_0/\sigma_1^2)}{\Gamma(D/2)}-\frac{\Gamma(D/2,\eta_1/\sigma_1^2)}{\Gamma(D/2)}$。

以上推导得到了监察者进行三元假设检验的判决准则,其中阈值η_0和η_1是决定其检测性能的核心参数。在本研究所构建的博弈论框架中,监察者是一个主动的、智能的博弈方,其目标是最大化自身的效用函数。因此,阈值不再是被动给定的外生参数,而是监察者为实现其最优效用而动态调整的策略变量,监察者通过优化选择这 2 个阈值,来精细地权衡其检测行为的收益与代价,即成功检测并干扰上行信号与因虚警而浪费干扰功率。

2.2 检测错误概率

考虑到 A 是否被激活会改变 $P(H_0)$ 和 $P(H_1)$,W 将误检概率重写

$$\begin{aligned}P_F=&\Pr\left(\mathcal{D}_2\mid\overline{\mathcal{H}_2}\right)=\Pr\left(A_{\text{activated}},\mathcal{D}_2\mid\overline{\mathcal{H}_2}\right)+\\&\Pr\left(A_{\text{not activated}},\mathcal{D}_2\mid\overline{\mathcal{H}_2}\right)\end{aligned} \tag{7}$$

基于贝叶斯可以按如下方式计算误检概率

$$\begin{aligned}P_F=&P_{F0}\left[p\frac{M-\nu}{M-c}+(1-p)\frac{M-\nu}{M}\right]+\\&P_{F1}\left[p\frac{\nu-c}{M-c}+(1-p)\frac{\nu}{M}\right]\end{aligned} \tag{8}$$

为了后续表述的便捷性,定义如下 2 个函数

$$\begin{aligned}\phi_0&=p\frac{M-\nu}{M-c}+(1-p)\frac{M-\nu}{M},\\\phi_1&=p\frac{\nu-c}{M-c}+(1-p)\frac{\nu}{M}\end{aligned} \tag{9}$$

基于此定义,监察者的检测错误概率可表示为误检概率与漏检概率之和,写作$\xi=P_M+P_F$。式中,$P_M=1-P(\mathcal{D}_2|\mathcal{H}_2)$,$P_F=P_{F0}\phi_0+P_{F1}\phi_1$。

3 博弈模型构建和求解

构建 A、W 和 J 的效用函数,并将此问题设计为一个双层博弈模型,分别进行求解。

3.1 效用函数

为了在被检测到的概率较低的情况下传输上行信息,A 的效用写作

$$\begin{aligned}&\max_c 1-P_D\\&\text{s.t.}\quad\gamma_{\text{worst}}\geqslant\beta\\&\quad c\in\{1,2,\cdots\nu\}\end{aligned} \tag{10}$$

该问题表明 A 正在通过调整 c 来努力降低被 W 检测到的概率 P_D,且需满足最差的传输信噪比$\gamma_{\text{worst}}\geqslant\beta$以及 $c\in\{1,2,\cdots,\nu\}$。后者意味着激活的信道数量将少于 ν。γ_{worst}表示在最坏情况下接收端 B 的信噪比,是 A 在决策时需要考虑的保守性能估计,此时在A_t中的所有信道都被 W 识别为存在信号γ_{worst}。它确保了即使面对监察者最有效的干扰,通信链路仍能满足一个基本的可靠性约束。这正是 A 的效用函数中约束项的来源,也引导着 A 在“降低被发现概率”和“保障通信鲁棒性”之间进行权衡。γ_{worst}可以写作如下形式

$$\gamma_{\text{worst}}=\sum_{i\in\mathcal{A}_t}w_i\frac{P_T|h_{ab}^i|^2}{(1-\mu)P_JE\left\{|h_{wb}^i|^2\right\}+\sigma_b^2} \tag{11}$$

式中,w_i表示 MRC 的比率,$P_J=P_W^M/N_d$,σ_b^2表示加性高斯白噪声的方差。

由于 A 无法获取N_d和h_{wb}，假设 A 用平均值来替代它们。考虑到检测概率和虚警概率，$E\{N_d\}$可以写作如下形式

$$E\{N_d\}=P_D+(M-v)P_{F0}+(v-c)P_{F1} \tag{12}$$

W 的目标是寻找并干扰上行通信。由于 W 认为在所有检测到的信道上均匀分配干扰功率，干扰性能将与 N_d 呈负相关。显然，干扰的准确性与 P_D 有关，而干扰功率与 P_F 呈负相关。基于上述分析，可以将 W 的效用函数表述为

$$\begin{aligned}&\max_{\eta_0,\eta_1} P_D\\ &\text{s.t.}\quad P_F\leqslant\alpha\end{aligned} \tag{13}$$

为了迷惑 W，J 通过发送人工噪声来提高 W 的错误检测概率 ξ。因此，可以将 J 的效用函数设计为

$$\begin{aligned}&\max_{v} \xi\\ &\text{s.t.}\quad \gamma_{\text{worst}}\geqslant\beta\\ &\quad v\in\{1,2,\cdots M\}\end{aligned} \tag{14}$$

3.2 双层博弈求解

将U_A,U_W,U_J设计为一个两层博弈模型。为便于计算，将此问题分为下层子问题和上层子问题。下层子问题包括U_A,U_W，而上层子问题则基于下层子问题的解来求解U_J。

首先求解下层子问题。A 只需保证$\gamma_{\text{worst}}\geqslant\beta$并取最大值，$\partial P_D/\partial c$可以写成

$$\frac{\partial P_D}{\partial c}=\frac{P_{\text{A}}^{\text{M}}}{c^2}\frac{e^{-\frac{1}{P_T+\sigma_0^2}}}{(P_T+\sigma_0^2)^{\frac{D}{2}+1}}\left[\eta_1^{\frac{D}{2}}c^{-\eta_1}-\eta_0^{\frac{D}{2}}c^{-\eta_0}\right] \tag{15}$$

类似地，可得

$$\frac{\partial P_F}{\partial \eta_1}=-\frac{1}{\Gamma\left(\frac{D}{2}\right)}\left[\left(\frac{\eta_1}{\sigma_0^2}\right)^{\frac{D}{2}-1}e^{-\frac{-\eta_1}{\sigma_0^2}}\phi_0+\left(\frac{\eta_1}{\sigma_1^2}\right)^{\frac{D}{2}-1}e^{-\frac{-\eta_1}{\sigma_1^2}}\phi_1\right] \tag{16}$$

显然，最大化P_D的策略为$c^*=c^{th}$。

其次，可以通过解以下问题来获得η_1^{th}：

$$P_F=\frac{1}{\Gamma\left(\frac{D}{2}\right)}\left[\Gamma\left(\frac{D}{2},\frac{\eta_1^{th}}{\sigma_0^2}\right)\phi_0+\Gamma\left(\frac{D}{2},\frac{\eta_1^{th}}{\sigma_1^2}\right)\phi_1\right]=\alpha \tag{17}$$

因此，通过选择$\eta_1=\eta_1^{th}$来最大化P_D。当$c>vP_A^m/P_J^m$时，有$\partial P_D/\partial\eta_1<0$，且$\partial P_D/\partial\eta_0>0$，即$\eta_1^*$为满足$c>vP_A^m/P_J^m$的任意值。对于任意$\eta_0^*$，只要能满足$\frac{1}{\Gamma(D/2)}\left[\Gamma(D/2,\frac{\eta_0^*}{\sigma_0^2}\phi_0+\Gamma\left(D/2,\frac{\eta_0^*}{\sigma_1^2}\right)\phi_1\right]<\alpha$，则最大化$P_D$。至此可以获取$(\eta_0^*,\eta_1^*)$。

接下来求解上层问题。由于下层中的c^*,η_0^*,η_1^*已给定，且$\frac{\partial P_D}{\partial v}=0$，$\frac{\partial P_{F0}}{\partial v}=0$，因此有

$$\frac{\partial P_F}{\partial v}=P_{F0}\frac{\partial\varphi_0}{\partial v}+P_{F1}\frac{\partial\varphi_1}{\partial v}+\varphi_1\frac{\partial P_{F1}}{\partial v} \tag{18}$$

其中 $\frac{\partial\varphi_0}{\partial v}=-p\frac{1}{M-c}-(1-p)\frac{1}{M}$，$\frac{\partial\varphi_1}{\partial v}=p\frac{1}{M-c}+(1-p)\frac{1}{M}$当$\frac{\partial P_F}{\partial v}\leqslant 0$且$v=M$时，上层策略的解为$v_{th}=M$；其余情况通过求解$\frac{\partial P_F}{\partial v}=0$可获得$v_{th}$。

在面临监察者主动干扰的威胁下，发射机 A 在保证满足约束条件$\gamma_{\text{worst}}\geqslant\beta$的条件下，通过将其全部功率分散在$c^*=c_{th}$条信道上进行传输，能够最大程度的降低被监察者发现并干扰的概率。同时，协作干扰机通过选择干扰信道数目制造最大的不确定性，增大监察者的虚警概率，为监察者制造最大程度的频谱不确定性，以掩护合法系统数据传输。

4 仿真结果

相关仿真参数如表 1 所示。

表 1 仿真参数设置

参数	说明	数值
M	总信道数	10个
P_{A}^{M}	最大功率	20 dBm
P_{J}^{M}	干扰机最大功率	5~25 dBm
P_{W}^{M}	监察者最大功率	15 dBm
β	接收端最小信噪比阈值	1
μ	检测阶段时隙占比	30%
D	检测符号数	100
σ_0^2	噪声功率	−110 dBm

离散均匀传输功率(discrete uniform transmission power, DUTP)方案[14]核心思想是发射机从离散功率等级集合中均匀随机选择发射功率，通过功率随机化增加监察者的检测不确定性。作为结构化功率控制策略的代表，其性能受限于固定的离散等级设计，无法动态响应监察者的干扰行为，因此本研究策略具有自适应性优势。随机传输功率方案[15]通过发射功率在连续范围内完全随机跳变，利用功率域的随机性干扰监察者的检测。该方案代表无约束随机化策略，虽

提升隐蔽性但忽略通信质量保障(如信噪比(signal-to-noise ratio, SNR)约束)。最优停止信道探索方案[16]核心思想是发射机采用序贯观测方式,利用最优停止理论动态确定信道探索次数,通过权衡探索开销与信道增益来最大化期望吞吐量。假时隙传输方案[17]核心思想是通过构建合法用户与干扰机间的双矩阵博弈模型,利用假时隙传输策略避开干扰机的感知干扰时序,通过求解纳什均衡获得最优抗干扰策略。与本研究联合优化隐蔽性和通信可靠性的模型形成方法层面对比,这些方案是隐蔽通信抗干扰领域的典型方案,分别覆盖结构化离散控制、完全随机化、提升吞吐量、欺骗干扰机感知的设计,因此作为基准方案进行性能评估与对照。

图 2 展示了虚警概率随干扰机最大功率P_J^M的变化情况。随着P_J^M的增加,上行信号可以更好地被隐藏。本研究将基于双层博弈的方案与离散均匀传输功率方案[14]和随机传输功率方案[15]进行比较。图 3 展示了平均速率随信道数量的变化情况。由于 A 的

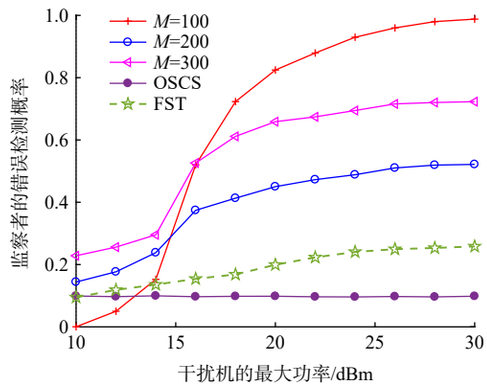


图 2 虚警概率随干扰机最大功率的变化

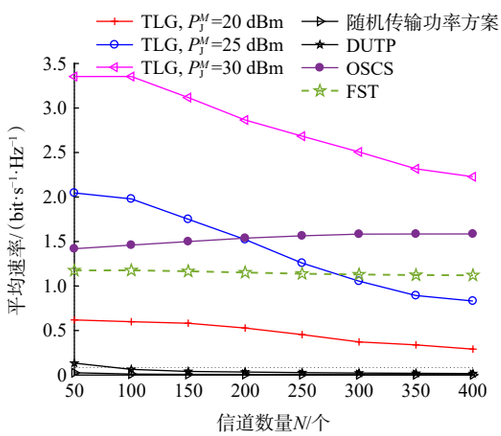


图 3 平均速率随信道数量的变化

策略 c 随着信道数量的增加而扩展,分配到每个信道的 P_T 减少。因此,隐蔽速率下降。图 4 展示了平均速率随干扰机最大功率P_J^M的变化情况。随着干扰功率的增大的增加,对 W 的迷惑性增强,漏检概率增加。因此,干扰攻击的效果减弱,传输速率增加。

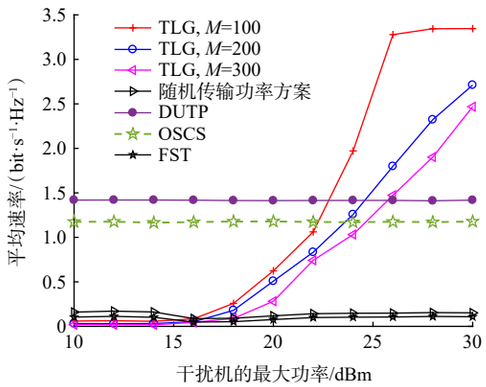


图 4 平均速率随干扰机最大功率的变化

5 结论

研究了面临干扰攻击威胁的隐蔽通信问题。将监察者的联合检测-干扰行为纳入隐蔽通信框架,创新性地将监察者的检测问题表述为三元假设检验,并将其检测阈值作为其博弈策略变量进行内生优化,从而在统一框架下刻画了“检测-干扰-反检测-反干扰”的完整对抗链条。通过构建双层博弈模型,本研究获得了发射机、监察者和干扰机策略的解决方案。仿真表明相比基线方案,在监察者最大干扰功率 25 dBm 时,传输速率最多提升 41%。能够为 5G/6G(第 5/6 代移动通信技术)高安全通信(如军事物联网、隐私保护 D2D(设备直连通信)传输)提供抗干扰隐蔽传输新思路。未来可探索动态信道环境下的在线博弈策略、多监察者协作场景的扩展模型,并引入深度学习增强策略求解的实时性。

参考文献(References)

[1] Jiang X, Li P, Zou Y L, et al. Physical layer security for cognitive multiuser networks with hardware impairments and channel estimation errors[J]. IEEE Transactions on Communications, 2022, 70(9): 6164-6180.

[2] Shahzad K, Zhou X Y. Covert wireless communications under

quasi−static fading with channel uncertainty[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 1104−1116.

[3] Bash B A, Goeckel D, Towsley D. Limits of reliable communication with low probability of detection on AWGN channels[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 1921−1930.

[4] Shahzad K, Zhou X Y, Yan S H. Covert communication in fading channels under channel uncertainty[C]//Proceedings of IEEE 85th Vehicular Technology Conference (VTC Spring). Piscataway, NJ: IEEE, 2017: 1−5.

[5] Sobers T V, Bash B A, Guha S, et al. Covert communication in the presence of an uninformed jammer[J]. IEEE Transactions on Wireless Communications, 2017, 16(9): 6193−6206.

[6] Zheng T X, Wang H M, Ng D W K, et al. Multi−antenna covert communications in random wireless networks[J]. IEEE Transactions on Wireless Communications, 2019, 18(3): 1974−1987.

[7] Li Z, Chen R, Shi J, et al. A game−theoretic approach to achieve covert communication in cognitive radio systems[J]. IEEE Transactions on Vehicular Technology, 2023, 72(10): 13011−13023.

[8] Wang M L, Xu Z, Xia B, et al. Active intelligent reflecting surface assisted covert communications[J]. IEEE Transactions on Vehicular Technology, 2023, 72(4): 5401−5406.

[9] Duan Z X, Yang X, Gong Y Y, et al. Covert communication in uplink NOMA systems under channel distribution information uncertainty[J]. IEEE Communications Letters, 2023, 27(5): 1282−1286.

[10] Lu X B, Yan S H, Yang W W, et al. Covert communication with time uncertainty in time−critical wireless networks[J]. IEEE Transactions on Wireless Communications, 2023, 22(2): 1116−1129.

[11] Ma W Y, Niu Z A, Wang W, et al. Covert communication with uninformed backscatters in hybrid active/passive wireless networks: Modeling and performance analysis[J]. IEEE Transactions on Communications, 2022, 70(4): 2622−2634.

[12] Che B H, Shi H, Yang W W, et al. Covert wireless communication against jamming−assisted proactive detection[J]. IEEE Wireless Communications Letters, 2023, 12(8): 1304−1308.

[13] Zhang L Y, Ding G R, Wu Q H, et al. Spectrum sensing under spectrum misuse behaviors: A multi−hypothesis test perspective[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(4): 993−1007.

[14] Yan S H, He B, Zhou X Y, et al. Delay−intolerant covert communications with either fixed or random transmit power[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(1): 129−140.

[15] Arghavani A, Dey S, Ahlén A. Covert outage minimization in the presence of multiple wardens[J]. IEEE Transactions on Signal Processing, 2023, 71: 686−700.

[16] He W H, Wang J L, Chen J, et al. Against inactive and reactive wardens: Covert transmission with optimal channel exploration[J]. IEEE Transactions on Communications, 2025, 73(10): 9815−9829.

[17] Zhang J S, Wu X F. An anti−jamming game between dynamically−sensing jammer and legitimate user with faking−slot transmission[J]. IEEE Transactions on Vehicular Technology, 2024, 73(7): 10287−10300.

Game-theoretic defense framework against jamming-assisted surveillance in covert communications

WU Jinxing, DI Xing, YIN Chuan, SONG Ruizhen, LI Tielin

Chinese Flight Test Establishment, Xi'an 710089, China

Abstract To address transmission exposure and link jamming in covert communications when an active warden is capable of both signal detection and intentional jamming, a covert communication strategy against warden jamming based on a bilevel game is proposed. The transmitter randomly selects a subset of the available channels to transmit uplink signals, while the receiver employs maximal-ratio combining for signal reception. The warden distinguishes idle channels, artificial-noise channels, and uplink-signal channels through ternary hypothesis testing and subsequently performs targeted jamming according to the detection results. To increase the warden's detection uncertainty, a cooperative jammer randomly selects a subset of the available channels not occupied by the uplink transmission to transmit artificial noise. On this basis, the transmitter, warden, and cooperative jammer respectively aim to minimize the detection probability of the uplink signal, maximize the detection probability, and maximize the detection-error probability. A tripartite bilevel game model is formulated subject to constraints on the communication signal-to-noise ratio, false-alarm probability, and transmit power. The number of transmission channels, the warden's detection thresholds, and the number of artificial-noise channels are jointly optimized. Simulation results demonstrate that the proposed strategy effectively increases the warden's detection uncertainty, reduces the probability that the uplink transmission is successfully detected and effectively jammed, and improves the transmission performance of the legitimate communication link. The proposed approach provides a theoretical reference for highly secure wireless communications and anti-jamming covert transmission under active detection and jamming threats.

Keywords covert communication; game theory; physical layer security; artificial noise; ternary hypothesis testing; channel allocation



（责任编辑 王微）