面向物联网的迪斯科式智能超表面下隐蔽通信检测与性能分析

黄欢[1]，孙路瑶[1]，张泓亮[2]
（1. 苏州大学电子信息学院，江苏 苏州 215006；2. 北京大学电子学院，北京 100871）

摘　要：随着物联网中敏感数据规模持续扩大，隐蔽通信因能够隐藏“通信存在”而成为重要的安全机制。在此背景下，分析了监听者 Willie 部署迪斯科式可重构智能超表面（DRIS， disco reconfigurable intelligent surface）条件下物联网（IoT， Internet-of-Things）隐蔽通信的检测与性能问题。由于 DRIS 反射系数随机时变，接收端等效信道在相干时间内不再近似恒定，从而引入主动信道老化（ACA， active channel aging）并导致信道状态信息失配。为此，设计了适用于时变 DRIS 的 Willie 检测规则；在非等概先验概率下，以总检测差错概率衡量检测性能，以信号-干扰-噪声比（SJNR， signal-to-jamming-plus-noise ratio）衡量通信性能，并推导了最优检测阈值及相关理论表达式。仿真结果表明：在发射功率为 5 dBm 时，相比无 DRIS 方案，DRIS 可使 Willie 的总检测差错概率降低约 63.4%，同时使 Bob 侧可达速率下降约 41.9%；固定 RIS 虽可使可达速率提升约 5.7%，但其总检测差错概率却比无 DRIS 方案高 8.43 倍。结果表明，DRIS 会同时增强 Willie 的检测能力并破坏合法隐蔽链路，对 IoT 隐蔽通信构成严重安全威胁。

关键词：物联网；隐蔽通信；可重构智能表面；信号检测；信道老化
中图分类号：TN915.08
文献标志码：A
doi：10.11959/j.issn.2096−3750.XXXX.

Detection and performance analysis of covert communications with disco reconfigurable intelligent surfaces for IoT

HUANG Huan[1], SUN Luyao[1], ZHANG Hongliang[2]
1. School of Electronic and Information Engineering, Soochow University, Suzhou 215006, China
2. School of Electronics, Peking University, Beijing 100871, China

Abstract: With the rapid growth of sensitive data in the Internet of Things (IoT), covert communication has become an important security mechanism by hiding the very existence of wireless transmissions. In this context, the detection and communication performance of IoT covert communications were analyzed when a disco reconfigurable intelligent surface (DRIS) was deployed by the warden Willie. Owing to the randomly time-varying reflection coefficients of the DRIS, the effective channel at the receiver was no longer approximately constant within one coherence block, thereby inducing active channel aging (ACA) and causing channel state information mismatch. To address this scenario, a detection rule for Willie tailored to time-varying DRIS-assisted channels was developed. Under non-equiprobable prior probabilities, the total detection error probability was used to characterize the detection performance, while the signal-to-jamming-plus-noise ratio (SJNR) was used to evaluate the communication performance. The optimal detection threshold and the corresponding analytical expressions were further derived. Numerical results showed that, at a transmit power of 5 dBm, compared with the no-DRIS scheme, the DRIS reduced Willie's total detection error probability by approximately 63.4% while de-

收稿日期：XXXX−XX−XX；修回日期：XXXX−XX−XX
通信作者：张泓亮，hongliang.zhang92@gmail.com
基金项目：国家自然科学基金重点项目（No.62531008）；国家自然科学基金（No.62401387，No.62371011）；江苏省自然科学基金（No.BK20240768）
Foundation Items: The Key Program of the National Natural Science Foundation of China (No. 62531008), The National Natural Science Foundation of China (No.62401387, No.62371011), The Natural Science Foundation of Jiangsu Province (No.BK20240768)

creasing Bob's achievable rate by about 41.9%. Although a fixed RIS improved the achievable rate by approximately 5.7%, its total detection error probability was 8.43 times that of the no-DRIS scheme. These results indicate that DRIS can simultaneously enhance Willie's detection capability and impair the legitimate covert link, thereby posing a serious security threat to IoT covert communications.

Key words: Internet-of-Things, covert communication, reconfigurable intelligent surface, signal detection, channel aging

0 引言

物联网（IoT, Internet-of-Things）在现代生活中扮演着越来越重要的角色，广泛应用于医疗健康、交通、工业设备、智能家居等多个领域。数以亿计的智能设备彼此间通过通信与协作完成各种复杂任务。这一发展不仅为经济增长带来新机遇，也带来了各类安全风险[1-4]。在物联网系统中，安全性与隐私保护对于用户至关重要，特别是在系统提供关键服务时，如智能汽车[5]、医疗保健[6]、工业[7]等领域。然而，传统的加密技术和网络安全方法无法全面应对物联网环境中的各种安全挑战。当IoT节点希望在不被攻击者发现的情况下进行通信时，单纯依靠加密技术来防止窃听远远不够。即便信息经过加密，相关元数据（如流量模式）仍有可能泄露敏感内容[8-9]。

相较于传统的密码学与物理层安全（PLS, physical-layer security）机制，隐蔽通信侧重于隐藏“通信存在”这一事实，从而为无线通信系统提供更高层次的隐私保护[10-11]。当监听者Willie未能觉察到通信行为时，一般不会进行信号解码与信息提取。文献[11]在加性高斯白噪声（AWGN, additive white Gaussian noise）信道下给出基准结论：当信道使用次数为n，则在未知发射端Alice与监听者Willie之间噪声功率的情况下，可在实现任意低概率检测的同时传输$o(\sqrt{n})$比特信息。其中，$o(\sqrt{n})$表示相对于$\sqrt{n}$的非渐近紧上界。此外，若噪声功率的下界已知，则可传输至多$O(\sqrt{n})$比特信息，此时$O(\sqrt{n})$为$\sqrt{n}$的渐近紧上界。

继文献[11]之后，相关研究相继引入了非正交多址(NOMA, non-orthogonal multiple access)与Turbo编码技术，在保证传输性能的同时有效提升了系统的隐蔽性[12]。文献[13-14]研究了借助干扰器或人工噪声以增大接收信号的功率波动，从而增加监听者Willie的决策不确定性。进一步地，文献[15-16]证明了中继节点的引入能产生相似的波动增强效果，以此破坏Willie的检测能力[17]。此外，文献[18]提出了一种直接利用小尺度衰落所引发的接收功率变化来实现隐蔽通信的方案。

随着IoT设备以无线链路为主的信息交互方式日益普及，且在敏感信息采集、传输与处理方面的需求不断增长，将隐蔽通信引入IoT系统已成为该领域关注的研究热点。当前针对物联网隐蔽通信的研究主要聚焦于三大方面：信号与干扰利用、协作架构与能力扩展以及新频段与智能环境应用。在信号与干扰利用方面，文献[19-22]探究了通过利用网络内生的聚合干扰或频谱掩模等策略来天然地隐藏传输行为；同时，通过采用非适当高斯信令（IGS, improper Gaussian signaling）等先进信号处理技术，以及信道反转功率控制（CIPC, channel inversion power control）来解决接收端信道信息获取问题，有效提升了系统的隐蔽速率。在协作架构与能力扩展方面，文献[23-25]引入了中继机制克服远距离传输的限制，并通过全双工网关或无人机作为协作节点发射人工噪声来主动压制窃听者，甚至应用平均场理论对大规模系统进行建模优化。此外，随着技术向更高频段发展，相关研究已延伸至太赫兹通信，并探索了结合无人机等新型智能环境技术来优化隐蔽传输的可靠性和能量效率[26]。

近年来，可重构智能表面（RISs, reconfigurable intelligent surfaces）被视为提升无线通信性能的关键技术[27-30]。RIS由大量反射单元构成，其反射系数可通过PIN二极管或变容二极管进行灵活调控[31]。将RIS引入无线网络，可在不显著增加功耗与成本的前提下，显著提升系统性能[32-33]。值得注意的是，现有研究还将RIS用于反向散射通信等低功耗IoT体制的鲁棒设计，例如RIS辅助异构反向散射通信的鲁棒优化已得到探讨[34]。目前，RIS在隐蔽通信中的应用已在文献[35-39]中得以探索。这些研究主要聚焦于如何利用单个或多个RIS，在结合NOMA[35]、人工噪声[36]、有限块长编码[37]或无人机通信[38-39]等技术的系统中，有效增强通信的隐

蔽性。此外，针对表面结构的扩展也已受到关注，例如STAR-RIS等具备透射–反射双功能的架构可进一步提升空间调控维度与覆盖灵活性[40]。

现有关于IoT隐蔽通信系统的研究多围绕增强隐蔽性展开，无论是否引入RIS，通常假设接收端等效信道在一个相干时间内保持不变或近似不变。此假设在多数场景下成立，但在面对反射系数随机时变的迪斯科式可重构智能表面（DRIS, disco RIS）[41]或具有非互易连接结构的RIS[42]时，接收端等效信道在相干时间内不再保持近似恒定。文献[43]进一步提出，可利用DRIS在无需合法用户信道状态信息（CSI, channel state information）或额外发射功率的条件下，发起全无源干扰攻击。由于DRIS的反射系数具有随机时变特性（类似“迪斯科球”），通过引入主动信道老化（ACA, active channel aging），使已获取的CSI与当前等效信道之间产生偏差[44-45]，且这种攻击方式极难被传统频谱监测手段发现。

更重要的是，DRIS代表了一种超越传统方案的攻击范式，其通过颠覆性的工作机制实现了对隐蔽通信系统的协同攻击。与传统RIS需依赖CSI以优化相位来增强通信性能不同，DRIS主动摒弃CSI与优化算法，采用完全随机、时变的反射模式，将同一硬件平台从“性能增强器”重构为“信道破坏器”。而与需要消耗自身功率发射干扰信号的传统主动干扰（AJ, active jammer）相比[46-48]，DRIS作为无源干扰器，仅通过反射并扰动环境中的合法信号即可实施干扰，无需主动发射干扰信号，因而相较传统有源干扰器具有更低的能耗开销。

这种低成本、低门槛的物理层攻击对实际IoT隐蔽通信场景构成了直接威胁。例如，在工业IoT中，一个伪装成普通设备的DRIS可被秘密部署于关键区域，通过ACA效应持续干扰传感器与控制器之间的状态上报链路，可能导致关键告警信息丢失，引发安全事故；同时，它还能显著提升攻击者对隐蔽传输事件的检测概率，从而窃取生产节奏、设备故障模式等敏感商业情报。在智能家居中[49]，微型DRIS可以静默地探测健康监测仪、安防传感器等设备的无线活动，即使通信内容已加密，攻击者仍能通过分析被扰动的信道特征推断用户的居家状态、作息规律等深度隐私信息。现有基于加密和应用层的安全机制对此类物理层攻击完全无效。

文献[50]首次探讨了DRIS在隐蔽通信对抗中的应用，监听者Willie通过引入DRIS，可在不消耗额外发射功率且无需任何CSI的条件下，提升其自身监测性能并干扰可能的隐蔽通信。然而，该研究仅考虑了等概的二元假设模型：Alice和Bob之间进行隐蔽通信或者静默的先验概率相同，未能充分揭示在更符合实际通信统计特性的非等概场景下，DRIS对IoT隐蔽通信系统的完整影响机理与双重威胁。因此，本文进一步在非等概先验概率设置下开展检测规则与性能分析，以更贴合IoT业务中“发射/静默”非对称发生概率，并更全面刻画DRIS对隐蔽通信的暴露与干扰效应。

本文旨在探讨在IoT隐蔽通信场景下，DRIS引入ACA及其对检测性能与通信性能的影响。为此，本文考虑更符合实际的隐蔽通信模型：Alice和Bob之间进行通信的先验概率为P_{C}，静默的先验概率为P_{S}，且$P_{\mathrm{C}} + P_{\mathrm{S}} = 1$。本文主要贡献如下：

(1)建立了存在DRIS下，IoT隐蔽通信系统的模型，其中DRIS由于其随机时变的反射系数，引入了ACA。监听者Willie通过部署DRIS，可以在无需知晓Alice与Bob的CSI，也无需消耗额外功率的情况下，干扰合法链路的隐蔽通信性能，并同时降低其检测差错概率。为量化DRIS的影响，本文为Willie设计了一种检测规则。进一步，本文采用非等概的先验概率来设定Alice发射隐蔽信息与保持静默两种状态，并以总检测差错概率（即虚警率（FAR, false alarm rate）与漏检率（MDR, missed detection rate）的加权和）作为Willie检测性能的度量。同时，定义信号-干扰-噪声比（SJNR, signal-to-jamming-plus-noise ratio）作为评估Alice与Bob间隐蔽通信质量的指标。

(2)为定量评估时变DRIS引入的ACA对IoT隐蔽通信系统性能的影响，本文首先推导了DRIS信道的统计特性。基于该统计结果与所提检测规则，给出了Willie的最优检测阈值，该阈值充分考虑了DRIS的时变特性以及不等先验概率场景。在此基础上，推导了Willie的FAR与MDR的闭式表达式，进而给出了总检测差错概率的理论表达式。同时，通过对SJNR的渐近分析，揭示了DRIS对合法通信链路的影响机制。仿真结果验证了理论分析的正确性。

(3)基于上述理论分析，揭示了DRIS对IoT隐

蔽通信系统的双重影响。研究结果表明：DRIS 在降低 Willie 总检测差错概率的同时，也会对 Alice 与 Bob 之间的合法通信造成显著干扰；即使 Willie 发生漏检，此干扰依然存在。更为关键的是，由于 DRIS 的存在，提升 Alice 的发射功率并不能有效改善其隐蔽通信的性能，反而会加剧 DRIS 引入的 ACA 效应，从而进一步恶化 Alice 与 Bob 之间的通信质量，并增加 Alice 被 Willie 侦测到的风险。此外，研究还发现，即使 DRIS 的反射系数仅采用 1 比特量化，其也能有效提升 Willie 的检测精度并干扰合法隐蔽链路，系统性地证实了 DRIS 在隐蔽通信中的严重安全隐患。

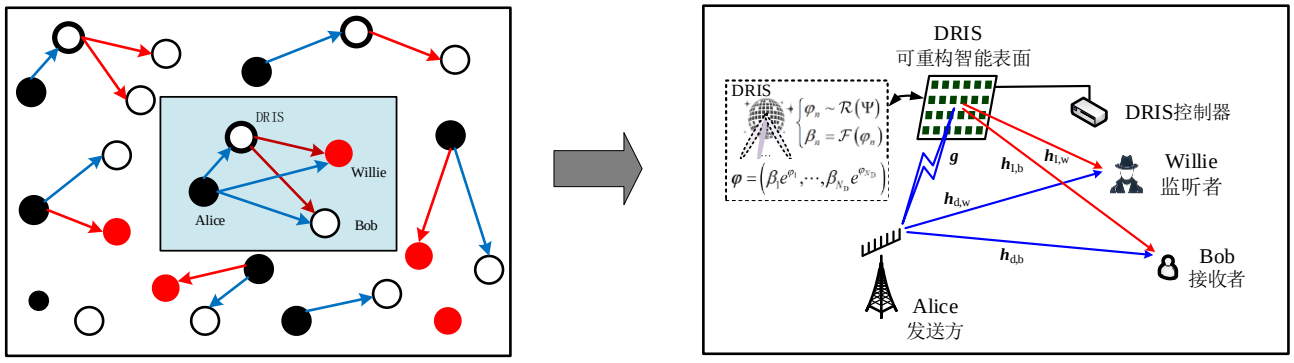

图 1　IoT 系统中存在 DRIS（具有时变随机的反射系数）情况下的隐蔽通信示意图

本文后续结构安排如下：第 1 节构建了存在 DRIS 的 IoT 隐蔽通信系统模型，并分析其对无线信道的影响，同时确立了以总检测差错概率作为监听者 Willie 的检测性能指标，以 SJNR 作为 Alice 与 Bob 的传输性能指标。第 2 节推导了 DRIS 信道的统计特性，进而确定了在时变 DRIS 引入的 ACA 影响下，Willie 用于判决通信状态的最优检测阈值；据此，进一步给出了 Willie 处 FAR 与 MDR 的闭式解析表达式，从而得到总检测差错概率的理论表达式，并对 Bob 处的 SJNR 进行了渐近分析。第 3 节通过仿真对比，验证了理论分析的正确性，并系统评估了 DRIS 的影响。最后，结论部分对全文研究工作进行总结。

符号说明：本文使用粗体小写字母表示向量（如$\boldsymbol{g}$），使用斜体字母表示标量（如N_{D}）。运算符$(\cdot)^{T}$和$(\cdot)^{H}$分别表示转置和共轭转置，符号$|\cdot|$表示绝对值。统计期望用$\mathbb{E}[\cdot]$表示。

1　系统模型

第 1.1 节首先提出一个存在 DRIS 的隐蔽通信场景。随后，第 1.2 节对涉及的无线信道进行建模。第 1.3 节阐述了监听者 Willie 检测 Alice 与 Bob 间隐蔽通信的检测规则，定义了 FAR 与 MDR，同时给出了总检测差错概率的数学表达式。最后，第 1.4 节将 SJNR 定义为通信性能指标，用于评估 DRIS 的部署对 Alice 与 Bob 间隐蔽传输的影响。

1.1　DRIS 存在下的隐蔽通信

图 1 示意性地展示了存在 DRIS 的隐蔽通信系统模型。在该系统中，Alice 的目标是向 Bob 秘密传输信息，同时规避非法监听者 Willie 的侦测。本研究核心探讨的问题是：在 DRIS 不与通信双方（Alice 与 Bob）进行任何协调的前提下，如何确定 Willie 正确识别二人是否保持沉默的概率。鉴于此，本文假设 Willie 无法获取 Bob 的 CSI 及其位置信息。

为提升对 Alice 传输行为的检测能力，监听者 Willie 采用反射系数可二进制量化的 DRIS。该 DRIS 由可编程 PIN 二极管单元组成，其相移与幅度可能的取值分别表示为：$\boldsymbol{\Psi}=\{\phi_1,\phi_2,\cdots,\phi_{2^b}\}$以及$\boldsymbol{\Omega}=\{\alpha_1,\alpha_2,\cdots,\alpha_{2^b}\}$。

与文献[41,43-45]类似，假设第n个 DRIS 单元（$n=1,\cdots,N_{\mathrm{D}}$）的反射系数$\varphi_{\mathrm{n}}(t)$和$\beta_{\mathrm{n}}(t)$是随机时变并且独立同分布的。据此，DRIS 的无源波束赋形矩阵可表示为$\boldsymbol{\Phi}(t)=diag\left(\varphi(t)\right)$，其中$\varphi(t)=\left[\beta_1(t)e^{\varphi_1(t)},\cdots,\beta_{N_{\mathrm{D}}}(t)e^{\varphi_{N_{\mathrm{D}}}(t)}\right]$为 DRIS 反射向量。在实际系统中，振幅$\beta_{\mathrm{n}}(t)$通常是相移$\varphi_{\mathrm{n}}(t)$的函数，即$\beta_{\mathrm{n}}(t)=\mathcal{F}\left(\varphi_{\mathrm{n}}(t)\right)\in\Omega$[27]。本文理论分析基于 DRIS 反射系数可精确控制的理想假设。第 3 节的仿真分析进一步表明，在适度硬件误差下，所得结论仍具有鲁棒性。参考文献[45]中的相关设定表明，DRIS

反射系数在每个信道相干时间内仅需随机更新少数几次，即可引发ACA。

本文模型构建于文献[36]所提出的隐蔽通信框架之上。在信道相干时间内，监听者Willie接收到的第m个采样信号可建模为式(1)。本文采用准静态假设，即相干区间内直达链路近似恒定[17]，而DRIS反射系数可在相干区间内发生有限次随机切换，从而在相干区间内诱发ACA效应。

$$y_{\mathrm{w}}(m)=\begin{cases}\dfrac{h_{\mathrm{d}}^{\mathrm{w}}s(m)}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}+\dfrac{h_{\mathrm{D}}^{\mathrm{w}}(m)s(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}}+n_{\mathrm{w}}(m), & \textit{通信}\\ n_{\mathrm{w}}(m), & \textit{静默}\end{cases} \tag{1}$$

其中，$s(m)$为Alice发送的隐蔽通信符号，$n_{\mathrm{w}}(m)\sim\mathcal{CN}\left(0,\delta_{\mathrm{w}}^2\right)$为AWGN。与文献[11,13-14]类似，假设$s(m)$服从零均值、功率为$P_0$的复高斯分布，即$s(m)\sim\mathcal{CN}\left(0,P_0\right)$，其中$P_0$为Alice的传输功率。此外，本文默认Alice在不同采样时刻发送的符号$s(m)$在采样维度上相互独立。$h_{\mathrm{d}}^{\mathrm{w}}$为Alice与Willie之间的直接链路信道。$h_{\mathrm{D}}^{\mathrm{w}}$为在第$m$个采样时刻，经DRIS反射的级联信道，该信道可建模为

$$h_{\mathrm{D}}^{\mathrm{w}}(m)=\boldsymbol{g}\mathrm{diag}\left(\boldsymbol{\varphi}(m)\right)\boldsymbol{h}_{\mathrm{I}}^{\mathrm{w}} \tag{2}$$

其中，$\boldsymbol{g}\in\mathbb{C}^{1\times N_D}$为Alice与DRIS之间的信道，$\boldsymbol{h}_{\mathrm{I}}^{\mathrm{w}}\in\mathbb{C}^{1\times N_{\mathrm{D}}}$为DRIS与Willie之间的信道。式中$\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}$、$\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}$和$\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}$分别为$h_{\mathrm{d}}^{\mathrm{w}}$，$\boldsymbol{g}$和$\boldsymbol{h}_{\mathrm{I}}^{\mathrm{w}}$的大尺度衰落系数，其路径损耗因子依次为$v_{\mathrm{d}}^{\mathrm{w}}$，$v_{\mathrm{g}}$和$v_{\mathrm{I}}^{\mathrm{w}}$。为简化分析，假设Alice与Willie的位置固定，故上述大尺度衰落系数可视为常数。此外，若Willie在信道相干时间内采集$M\geqslant 2$个采样点，则其接收信号可表示为向量形式：$\boldsymbol{y}_{\mathrm{w}}=\left[y_{\mathrm{w}}(1),y_{\mathrm{w}}(2),\cdots,y_{\mathrm{w}}(M)\right]^T$。

Bob在第m个采样时刻接收到的信号可建模为

$$y_{\mathrm{b}}(m)=\underbrace{\frac{h_{\mathrm{d}}^{\mathrm{b}}s(m)}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{b}}}{2}}}}_{\textit{直接链路}}+\underbrace{\frac{h_{\mathrm{D}}^{\mathrm{b}}(m)s(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{b}}}{2}}}}_{\textit{基于DRIS的链路}}+n_{\mathrm{b}}(m) \tag{3}$$

其中，$h_{\mathrm{d}}^{\mathrm{b}}$为Alice与Bob之间的直接链路信道，$h_{\mathrm{D}}^{\mathrm{b}}(m)$为第$m$个采样时刻经DRIS反射的级联信道，$n_{\mathrm{b}}(m)\sim\mathcal{CN}\left(0,\delta_{\mathrm{b}}^2\right)$为AWGN。$\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{b}}}{2}}$和$\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{b}}}{2}}$分别为信道$h_{\mathrm{d}}^{\mathrm{b}}$和$h_{\mathrm{I}}^{\mathrm{b}}$的大尺度衰落系数，其对应的路径损耗因子依次为$v_{\mathrm{d}}^{\mathrm{b}}$和$v_{\mathrm{I}}^{\mathrm{b}}$。

此处，级联信道$h_{\mathrm{D}}^{\mathrm{b}}(m)$可进一步表示为

$$h_{\mathrm{D}}^{\mathrm{b}}(m)=\boldsymbol{g}\mathrm{diag}\left(\boldsymbol{\varphi}(m)\right)\boldsymbol{h}_{\mathrm{I}}^{\mathrm{b}} \tag{4}$$

其中，$\boldsymbol{h}_{\mathrm{I}}^{\mathrm{b}}\in\mathbb{C}^{1\times N_{\mathrm{D}}}$为DRIS与Bob之间的信道。本文以单对Alice－Bob隐蔽链路为核心，旨在刻画DRIS随机时变反射引入的级联分量对Willie检测门限与统计量的影响，从而揭示ACA机理。对于密集IoT场景，设备密度提升可等效为聚合干扰增强（噪声底抬升/附加干扰项），在式(1)与式(4)中加入相应干扰项并更新阈值与速率表达即可推广。网络级密度效应的定量评估将结合聚合干扰与业务活跃模型在后续工作中展开。

1.2　信道模型

本文考虑如下场景：DRIS部署在Alice的附近，而监听者Willie与接收端Bob均位于远处。在本文所考虑的隐蔽通信场景中，Alice位置固定，因此本文聚焦于DRIS靠近Alice部署的情形。该设定与现有RIS部署研究结论一致，即RIS靠近发射端或接收端时，对系统链路的影响更为显著[51]。据此，本文分析未知Bob信息条件下DRIS部署对Willie检测性能及Alice－Bob合法链路性能的影响。

进一步地，尽管将DRIS部署在靠近Alice的位置可能增加其被发现的风险，但RIS具有无源特性，即其本身不进行信号的发射、接收或处理[31]，因此可通过环境伪装的方式实现隐蔽部署，例如嵌入玻璃结构、安装于墙体表面或集成到现有基础设施中。由此，本文假设DRIS可在隐蔽通信发生前预先部署，并在后续阶段自主运行。其中，Alice-Bob与Alice-Willie的直达信道$h_{\mathrm{d}}^{\mathrm{b}}$、$h_{\mathrm{d}}^{\mathrm{w}}$，以及DRIS-Bob与DRIS-Willie的信道$\boldsymbol{h}_{\mathrm{I}}^{\mathrm{b}}$、$\boldsymbol{h}_{\mathrm{I}}^{\mathrm{w}}$均遵循远场假设进行建模[20,22,24-25]，其信道系数被视为相互独立同分布的复高斯随机变量：

$$h_{\mathrm{d}}^{\mathrm{b}},h_{\mathrm{d}}^{\mathrm{w}}\sim\mathcal{CN}\left(0,1\right) \tag{5}$$

$$\boldsymbol{h}_{\mathrm{I}}^{\mathrm{b}},\boldsymbol{h}_{\mathrm{I}}^{\mathrm{w}}\sim\mathcal{CN}\left(\mathbf{0}_{N_{\mathrm{D}}},\mathbf{I}_{N_{\mathrm{D}}}\right) \tag{6}$$

其中，$0_{N_{\mathrm{D}}}$为N_{D}维零向量，$\mathbf{I}_{N_{\mathrm{D}}}$为$N_{\mathrm{D}}$阶单位矩阵。

通常，实际中RIS需要配置大量反射单元以补偿其级乘的大尺度衰落造成的路径损耗[41,44-45]。因此，Alice与DRIS之间的信道$\boldsymbol{g}$采用近场模型进行建模[53]

$$\boldsymbol{g}=\sqrt{\frac{\varepsilon_{\mathrm{g}}}{1+\varepsilon_{\mathrm{g}}}}\,\boldsymbol{g}^{\mathrm{LOS}}+\sqrt{\frac{1}{1+\varepsilon_{\mathrm{g}}}}\,\boldsymbol{g}^{\mathrm{NLOS}} \tag{7}$$

其中，ε_{g}为信道$\boldsymbol{g}$的莱斯因子。在式(7)中，非视距(NLOS, non-line-of-sight)分量$\boldsymbol{g}^{\mathrm{NLOS}}$的各元素服从瑞

利衰落分布[52]；而视距(LOS, line of sight)分量$\boldsymbol{g}^{\mathrm{LOS}}$的元素可表示为[53]

$$\left[\boldsymbol{g}^{\mathrm{LOS}}\right]_r = e^{-j\frac{2\pi}{\lambda}(d_r - d_0)}, r = 1,\cdots,N_{\mathrm{D}} \tag{8}$$

其中，λ为隐蔽信号的波长，d_r和d_0分别为Alice天线至第r个DRIS单元的距离，以及该天线至DRIS中心（坐标原点）的距离。

1.3 Willie处判决准则

在隐蔽通信中，监听者Willie通过监听无线信道以判别Alice与Bob是否通信。具体而言，Willie根据式(1)中的采样结果来推断以下两种事件的发生：Alice与Bob正在通信（$\mathcal{H}_1$），或Alice保持静默（$\mathcal{H}_0$）。其检测性能通常由两类错误概率来评价：FAR，即$\mathbb{P}(\mathcal{H}_1|\mathcal{H}_0)$，表示Alice未通信时Willie误判为通信的概率;以及MDR，$\mathbb{P}(\mathcal{H}_0|\mathcal{H}_1)$，表示Alice实际通信时Willie误判为静默的概率。

现有隐蔽通信研究普遍基于接收端等效信道在相干时间内保持不变或近似不变的假设。在此条件下，Willie的接收信号向量$\boldsymbol{y}_{\mathrm{w}}$各元素满足独立同分布，因此可采用总接收功率作为检测统计量以判别通信状态[14-18]。然而，DRIS的引入使接收端等效信道在相干时间内不再保持近似恒定。具体而言，Willie在一个检测窗口内采集的多个样本可对应不同的DRIS反射状态，因此即便在同一相干时间内$\boldsymbol{y}_{\mathrm{w}}$的各元素统计特性也不再相同，从而不再满足传统独立同分布假设。因此，本文为Willie设计了如下的检验统计量：

$$\mathcal{S} = \left\{ \boldsymbol{y}_{\mathrm{w}} \middle| \bigcup_{i_1 < \cdots i_N} \left|y_{\mathrm{w}}(i_1)\right|^2 \geqslant \varepsilon(i_1) \cap \cdots \cap \left|y_{\mathrm{w}}(i_N)\right|^2 \geqslant \varepsilon(i_N) \right\} \tag{9}$$

其中，M表示Willie在一个检测窗口内采集的样本总数，$1 \leqslant i_1 < \cdots < i_N \leqslant M$，$\varepsilon(m)$为第$m$个检测分量的判决门限。式(9)中交集表示所选$N$个检测分量同时超过其对应门限的联合事件，并集表示对所有可能的N元索引组合取并。因此，式(9)对应于一种N-out-of-M判决规则，即当M个检测分量中至少有N个超过各自门限时，判定观测向量$\boldsymbol{y}_{\mathrm{w}}$落入检测区域$S$。据此，Willie的检测问题可表述为

$$\mathcal{H}_1: \boldsymbol{y}_{\mathrm{w}} \in \mathcal{S} \tag{10}$$

$$\mathcal{H}_0: \boldsymbol{y}_{\mathrm{w}} \notin \mathcal{S} \tag{11}$$

鉴于检测门限$\varepsilon(m)$的时变性，其设计必须计及DRIS的影响以确保检测精度。对应地，加权FAR与MDR分别表示为：

$$P_{\mathrm{F}} = \mathbb{P}(\mathcal{H}_0)\mathbb{P}(\mathcal{H}_1|\mathcal{H}_0) = P_{\mathrm{S}}\mathbb{P}(\mathbf{y}_{\mathrm{w}} \in \mathcal{S}|\mathcal{H}_0) \tag{12}$$

$$P_{\mathrm{M}} = \mathbb{P}(\mathcal{H}_1)\mathbb{P}(\mathcal{H}_0|\mathcal{H}_1) = P_{\mathrm{C}}\mathbb{P}(\mathbf{y}_{\mathrm{w}} \notin \mathcal{S}|\mathcal{H}_1) \tag{13}$$

为了量化Willie的检测可靠性，本文进一步定义其总检测差错概率为P_{E}，如式(14)所示。

$$P_{\mathrm{E}} = P_{\mathrm{M}} + P_{\mathrm{F}} \tag{14}$$

其中P_{C}为Alice处于通信状态的先验概率，即系统中Alice选择发射隐蔽信息的概率。P_{S}为Alice处于静默状态的先验概率，即Alice不发射隐蔽信息的概率，且$P_{\mathrm{C}} + P_{\mathrm{S}} = 1$。

1.4 Bob处的信号与干扰加噪声比

鉴于DRIS通过时变信道$h_{\mathrm{D}}^{b}(t)$对Bob产生干扰效应，本文采用文献[45]定义的SJNR对该干扰进行表征。需要说明的是，本文场景不同于文献[54]中的协作式回散射通信。文献[54]中附加回散射项可作为额外多径分量被接收机利用，而本文中DRIS反射状态由Willie随机控制且对Bob未知，Bob也不具备针对该随机时变反射的同步训练与实时跟踪机制，因此其引入的级联分量在Bob端更合理地表现为未知时变扰动。基于此，本文采用SJNR而非SNR来刻画Bob侧通信性能。

$$\eta_{\mathrm{b}} = \frac{\dfrac{P_0\mathbb{E}\left[\left|h_{\mathrm{d}}^{\mathrm{b}}s(m)\right|^2\right]}{\mathcal{L}^{v_{\mathrm{d}}^{\mathrm{b}}}}}{\dfrac{P_0\mathbb{E}\left[\left|h_{\mathrm{D}}^{\mathrm{b}}(m)s(m)\right|^2\right]}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{f}}^{\mathrm{b}}}} + \delta_{\mathrm{b}}^2}} \tag{15}$$

其中，Bob的可达速率为$R_{\mathrm{b}} = \log_2(1 + \eta_{\mathrm{b}})$。且本文方法可进一步推广至多DRIS场景，其中各DRIS独立采用随机时变反射系数，从而进一步增强Alice与Bob之间的主动信道老化效应，而不会削弱对Bob的干扰影响。

如式(15)所示，在不消耗额外发射干扰功率且无需Bob的CSI的情况下，DRIS仍能对Alice与Bob间的潜在隐蔽传输造成干扰。具体地，由于DRIS反射向量$\varphi(t)$由Willie随机控制且对通信双方未知，导致的级联干扰信道$h_{\mathrm{D}}^{\mathrm{b}}(m)$在信道相干时间内也是时变的，使得$h_{\mathrm{D}}^{\mathrm{b}}(m)s(m)$在接收端表现为类噪声干扰。DRIS通过引入ACA，进而降低了Bob处的SJNR。由此可见，Willie部署DRIS可在提升自身检测性能的同时，恶化合法链路的通信

质量。

2　隐蔽通信性能的渐近分析

第2.1节首先推导了DRIS级联信道的统计特性，以定量分析时变DRIS所引入ACA对系统的影响；在此基础上，为监听者Willie设计了考虑DRIS时变特性的检测阈值，用于判决Alice是否正在通信。第2.2节在给定该阈值的条件下，推导了Willie总检测差错概率的闭式表达式。第2.3节则通过对SJNR进行渐近分析，揭示了DRIS对合法链路传输性能的影响。

2.1　存在DRIS时的检测错误概率

为确定式(9)中的检测阈值，首先需推导Alice与Willie间级联DRIS信道$h_{\mathrm{D}}^{\mathrm{w}}(t)$的统计特性。

命题1：当DRIS的反射单元数$N_{\mathrm{D}} \to \infty$时，随机时变的级联信道$h_{\mathrm{D}}^{\mathrm{w}}(t)$依分布收敛于复高斯分布，即

$$\frac{h_{\mathrm{D}}^{\mathrm{w}}(t)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}} \xrightarrow{\mathrm{d}} \mathcal{CN}\left(0, \frac{N_{\mathrm{D}}\bar{\alpha}}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{d}}^{\mathrm{w}}}}\right) \tag{16}$$

其中，$\bar{\alpha} = \mathbb{E}[\left|\beta_{\mathrm{n}}(t)\right|^2] = \sum_{i=1}^{2^{\mathrm{b}}} P_i \alpha_i^2$，$P_i$为相位偏移$\varphi_r(t)$取第$i$个离散值的概率，即$P_i = \mathbb{P}(\varphi_r(t) = \phi_i)$。本文假设各DRIS单元所选择的离散相位服从均匀分布。

证明：见附录A。

为确定Willie的最优检测阈值ε，需推导其接收信号的分布。假设$\mathcal{H}_1$下，Willie接收到的第m个样本$y_{\mathrm{w}}(m)$可表示为

$$y_{\mathrm{w}}(m) = \frac{h_{\mathrm{d}}^{\mathrm{w}} s(m)}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}} + \frac{h_{\mathrm{D}}^{\mathrm{w}}(m) s(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}} + n_{\mathrm{w}}(m) \tag{17}$$

直接链路信道$h_{\mathrm{d}}^{\mathrm{w}}$在信道相干区间内保持恒定。基于命题1，可得如下结论

$$c_{\mathrm{w}}(m) = \frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}} + \frac{h_{\mathrm{D}}^{\mathrm{w}}(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}} \xrightarrow{\mathrm{d}} \mathcal{CN}\left(\frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}, \frac{N_{\mathrm{D}}\bar{\alpha}}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{d}}^{\mathrm{w}}}}\right) \tag{18}$$

然而，在式(17)中，隐蔽消息$s(m)$同样服从复高斯分布，且与$c_{\mathrm{w}}(m)$相互独立。两个相互独立的复高斯随机变量的乘积不再服从高斯分布[55]。对于两个相互独立的随机变量X和Y，其概率密度函数（PDF, probability density function）分别为$f_{\mathrm{X}}(x)$和$f_{\mathrm{Y}}(y)$，则$Z = XY$的PDF可由下式计算

$$f_{\mathrm{Z}}(z) = \int_{-\infty}^{+\infty} f_{\mathrm{X}}(x) f_{\mathrm{Y}}\left(\frac{z}{x}\right) \frac{1}{|x|} dx \tag{19}$$

根据式(19)，随机变量$e_{\mathrm{w}}(m)$的PDF由下式给出

$$\begin{aligned} & f_{E_{\mathrm{w}}}(e_{\mathrm{w}}(m)|\mathcal{H}_1) \\ &= \int_{-\infty}^{+\infty} \frac{1}{\frac{\pi N_{\mathrm{D}}\bar{\alpha}}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{w}}}}} \mathrm{e}^{-\frac{\left|c_{\mathrm{w}}(m) - \frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}\right|^2}{\frac{N_{\mathrm{D}}\bar{\alpha}}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{w}}}}}} \frac{1}{\pi P_0} e^{-\frac{\left|\frac{e_{\mathrm{w}}(m)}{c_{\mathrm{w}}(m)}\right|^2}{P_0}} \left|\frac{1}{c_{\mathrm{w}}(m)}\right|^2 \mathrm{d}c_{\mathrm{w}}(m) \\ &= \frac{4|e_{\mathrm{w}}(m)|}{\frac{P_0 N_{\mathrm{D}}\bar{\alpha}}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{w}}}}} \mathrm{e}^{-\kappa_{\mathrm{e}}^2} \sum_{n=0}^{+\infty} \left(\frac{1}{n!}\right)^2 \left(\frac{\kappa_{\mathrm{e}}^2 |e_{\mathrm{w}}(m)|}{\frac{P_0 N_{\mathrm{D}}\bar{\alpha}}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{w}}}}}\right)^{\mathrm{n}} K_n\left(\frac{2|e_{\mathrm{w}}(m)|}{\sqrt{\frac{P_0 N_{\mathrm{D}}\bar{\alpha}}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{w}}}}}}\right) \end{aligned} \tag{20}$$

其中，κ_{e}为$\frac{\left|h_{\mathrm{d}}^{\mathrm{w}}\right|^2 \mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{w}}}}{N_{\mathrm{D}}\bar{\alpha}\mathcal{L}^{v_{\mathrm{d}}^{\mathrm{w}}}}$[43]，$K_{\mathrm{n}}(\cdot)$为$n$阶第二类修正贝塞尔函数。

设Z和V为两个相互独立的随机变量，其PDF分别为$f_{\mathrm{Z}}(z)$和$f_{\mathrm{V}}(v)$。则随机向量$W = Z + V$的PDF由下式给出

$$f_{\mathrm{W}}(w) = \int_{-\infty}^{+\infty} f_{\mathrm{Z}}(z) f_{\mathrm{V}}(w - z) dz \tag{21}$$

在式(17)中，$n_{\mathrm{w}}(m)$的PDF可以表示为

$$f_{N_{\mathrm{w}}}(n_{\mathrm{w}}(m)) = \frac{1}{\pi\delta_{\mathrm{w}}^2} \mathrm{e}^{-\frac{|y_{\mathrm{w}}(m)|^2}{\delta_{\mathrm{w}}^2}} \tag{22}$$

$$\begin{aligned} & f_{Y_{\mathrm{w}}}(y_{\mathrm{w}}(m)|\mathcal{H}_1) \\ &= \int_{\mathbb{C}} f_{N_{\mathrm{w}}}(y_{\mathrm{w}}(m) - e_{\mathrm{w}}(m)) f_{E_{\mathrm{w}}}(e_{\mathrm{w}}(m)|\mathcal{H}_1) \mathrm{d}e_{\mathrm{w}}(m) \\ &= \int_{\mathbb{C}} \frac{1}{\pi\delta_{\mathrm{e}}^2} e^{-\frac{|y_{\mathrm{w}}(m) - e_{\mathrm{w}}(m)|^2}{\delta_{\mathrm{e}}^2}} \frac{2|e_{\mathrm{w}}(m)|}{\pi \frac{P_0 N_{\mathrm{D}}\bar{\alpha}}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{w}}}}} K_0\left(\frac{|e_{\mathrm{w}}(m)|}{\sqrt{\frac{P_0 N_{\mathrm{D}}\bar{\alpha}}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{w}}}}}}\right) \mathrm{d}e_{\mathrm{w}}(m) \end{aligned} \tag{23}$$

将式(20)和式(22)代入(21)，可得式(23)。其中，$\int_{\mathbb{C}}$为复平面上的积分。然而，式(23)中的积分难以直接求解以获得闭式解。

由于Willie可知第m个采样时刻的等效信道$h_{\mathrm{D}}^{\mathrm{w}}(m)$中$\varphi(m)$的取值。因此，在给定$\varphi(m)$的条件下，$e_{\mathrm{w}}(m)$的条件PDF可由式(20)简化为式(24)。

$$f_{E_{\mathrm{w}}}(e_{\mathrm{w}}(m)|\mathcal{H}_1,h_{\mathrm{D}}^{\mathrm{w}}(m)) \sim \mathcal{CN}\left(0,\delta_{\mathrm{e}}^2(m)\right)$$

$$= \frac{1}{\pi P_0\left|\frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}+\frac{h_{\mathrm{D}}^{\mathrm{w}}(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}}\right|^2}\exp\left(-\frac{\left|e_{\mathrm{w}}(m)\right|^2}{P_0\left|\frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}+\frac{h_{\mathrm{D}}^{\mathrm{w}}(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}}\right|^2}\right) \tag{24}$$

$$f_{Y_{\mathrm{w}}}\left(y_{\mathrm{W}}(m)|\mathcal{H}_1,h_{\mathrm{D}}^{\mathrm{w}}(m)\right) \sim \mathcal{CN}\left(0,\delta_{\mathrm{e}}^2(m)+\delta_{\mathrm{w}}^2\right)$$

$$= \frac{1}{\pi\left(\delta_{\mathrm{w}}^2+P_0\left|\frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}+\frac{h_{\mathrm{D}}^{\mathrm{w}}(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}}\right|^2\right)}\exp\left(-\frac{\left|y_{\mathrm{w}}(m)\right|^2}{\delta_{\mathrm{w}}^2+P_0\left|\frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}+\frac{h_{\mathrm{D}}^{\mathrm{w}}(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}}\right|^2}\right) \tag{25}$$

另一方面，在假设$\mathcal{H}_0$下，Willie接收到的第m个采样点$y_{\mathrm{w}}(m)$仅由AWGN构成，因此其PDF与零均值高斯分布的AWGN完全一致

$$f_{Y_{\mathrm{w}}}(y_{\mathrm{w}}(m)|\mathcal{H}_0) \sim \mathcal{CN}(0,\delta_{\mathrm{w}}^2) = \frac{1}{\pi\delta_{\mathrm{w}}^2}e^{-\frac{|y_{\mathrm{w}}(m)|^2}{\delta_{\mathrm{w}}^2}} \tag{26}$$

联立式(25)和(26)，可得命题2中的检测阈值$\varepsilon(m)$。

命题2: 考虑监听者Willie针对式(10)与式(11)所描述的二元假设检验问题进行检测，其最优检测阈值$\varepsilon(m)$（$m=1,\cdots,M$）基于似然比检验（LRT, likelihood ratio test）确定，其闭式表达式如式(27)。

$$\varepsilon(m) = \frac{\left(\delta_{\mathrm{w}}^2+P_0\left|\frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}+\frac{h_{\mathrm{D}}^{\mathrm{w}}(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}}\right|^2\right)\delta_{\mathrm{w}}^2}{P_0\left|\frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}+\frac{h_{\mathrm{D}}^{\mathrm{w}}(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{C}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}}\right|^2} \times \tag{27}$$

$$\left(\ln\left(\delta_{\mathrm{w}}^2+P_0\left|\frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}+\frac{h_{\mathrm{D}}^{\mathrm{w}}(m)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}}\right|^2\right)-\ln\delta_{\mathrm{w}}^2+\ln\left(\frac{P_{\mathrm{S}}}{P_{\mathrm{C}}}\right)\right)$$

证明：见附录B。

由命题2可知，DRIS的引入将直接影响检测规则式(9)中检测阈值$\varepsilon(m)$的取值。若无DRIS，则式(27)中的检测门限将退化为如下固定形式

基于独立复高斯随机变量之和仍服从复高斯分布的性质，Willie接收信号条件PDF可简化如下。

$$\varepsilon = \frac{\left(\delta_{\mathrm{w}}^2+\frac{P_0|h_{\mathrm{d}}^{\mathrm{w}}|^2}{\mathcal{L}^{v_{\mathrm{d}}^{\mathrm{w}}}}\right)\delta_{\mathrm{w}}^2}{\frac{P_0\left|h_{\mathrm{d}}^{\mathrm{w}}\right|^2}{\mathcal{L}^{v_{\mathrm{d}}^{\mathrm{w}}}}} \times \left(\ln\left(\delta_{\mathrm{w}}^2+\frac{P_0|h_{\mathrm{d}}^{\mathrm{w}}|^2}{\mathcal{L}^{v_{\mathrm{d}}^{\mathrm{w}}}}\right)-\ln\delta_{\mathrm{w}}^2+\ln\left(\frac{P_{\mathrm{S}}}{P_{\mathrm{C}}}\right)\right) \tag{28}$$

2.2 Willie检测的误差概率分析

本节旨在定量分析时变DRIS所引入的ACA对监听者Willie检测决策的影响。具体地，基于命题2所确定的最优检测阈值$\varepsilon(m)$，首先推导了总检测差错概率中理论FAR与MDR的表达式，并最终在定理1中给出了二者闭式解析解。

定理1：FAR和MDR可分别表示为：

$$P_{\mathrm{F}} = \mathbb{P}(\mathbf{y}_{\mathrm{w}} \in \mathcal{S}|\mathcal{H}_0)$$

$$= \sum_{T=N}^{M}\sum_{i_1<\cdots<i_T}\left(\prod_{j=i_1}^{i_T}e^{-\frac{\varepsilon(j)}{\delta_{\mathrm{w}}^2}}\prod_{i\neq i_1\neq\cdots\neq i_T}\left(1-e^{-\frac{\varepsilon(i)}{\delta_{\mathrm{w}}^2}}\right)\right) \tag{29}$$

和

$$P_{\mathrm{M}}=\mathbb{P}(\mathbf{y}_{\mathrm{w}}\notin\mathcal{S}|\mathcal{H}_0)=\frac{\prod_{m=1}^{M}\left(1-\exp\left(-\frac{\varepsilon(m)}{\delta_{\mathrm{w}}^2+\frac{P_0|h_{\mathrm{d}}^{\mathrm{w}}|^2}{\mathcal{L}^{v_{\mathrm{d}}^{\mathrm{w}}}}+\frac{P_0|h_{\mathrm{D}}^{\mathrm{w}}(m)|^2}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{w}}}}}\right)\right)}{2^{\mathrm{M}}}+\sum_{T=1}^{N-1}\sum_{i_1<\cdots<i_T}\left(\prod_{j=i_1}^{i_T}\exp\left(\frac{-\varepsilon(j)}{\delta_{\mathrm{w}}^2+P_0\left|\frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}+\frac{h_{\mathrm{D}}^{\mathrm{w}}(j)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}}\right|^2}\right)\times\prod_{i\neq i_1\neq\cdots\neq i_T}\left(1-\exp\left(-\frac{\varepsilon(i)}{\delta_{\mathrm{w}}^2+P_0\left|\frac{h_{\mathrm{d}}^{\mathrm{w}}}{\mathcal{L}^{\frac{v_{\mathrm{d}}^{\mathrm{w}}}{2}}}+\frac{h_{\mathrm{D}}^{\mathrm{w}}(i)}{\mathcal{L}^{\frac{v_{\mathrm{g}}}{2}}\mathcal{L}^{\frac{v_{\mathrm{I}}^{\mathrm{w}}}{2}}}\right|^2}\right)\right)\right)\tag{30}$$

证明：见附录C。

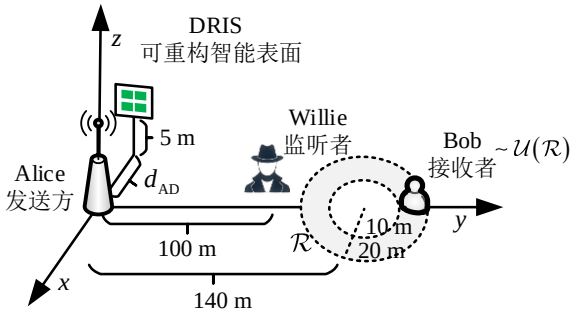

图2　存在DRIS的隐蔽通信场景示例，其中Bob随机位于以（0m, 140m）为圆心、半径从10m到20m的环形区域$\mathcal{R}$内。

由定理1可知，DRIS在隐蔽通信中展现出若干关键性质。首先，Alice的发射功率P_0越大，Willie的总检测差错概率反而越低。这意味着，提高发射功率非但不能有效提升Alice与Bob间的通信速率（此性能受限于DRIS引入的ACA），反而会增大通信行为被Willie侦测的风险。值得注意的是，如式(30)与(31)所示，Willie借助DRIS所获得的检测性能提升，与DRIS相移的具体取值无关。因此，即便仅采用1比特量化的DRIS反射系数，亦能显著增强其检测精度。

2.3　Alice与Bob的通信性能

Willie部署的DRIS具有双重影响：一方面提升其检测性能，另一方面降低Alice与Bob之间的隐蔽传输质量。更具体地，即使Willie漏检了隐蔽传输，DRIS的时变特性仍会持续向Bob引入额外的ACA干扰，从而恶化其接收性能。为量化这一影响，定理2给出了Bob端SJNR的闭式表达式。

定理2：当反射单元数$N_{\mathrm{D}}\to\infty$时，Bob处的可达速率依分布收敛于

$$R=\log_2\left(1+\frac{\frac{P_0}{\mathcal{L}^{v_{\mathrm{d}}^{\mathrm{b}}}}}{\frac{P_0N_{\mathrm{D}}\bar{\alpha}}{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{b}}}}+\delta_{\mathrm{b}}^2}\right),\ N_{\mathrm{D}}\to\infty\tag{31}$$

证明：见附录D。

定理2揭示了，提高发射功率并不能使Bob处的可达速率R无限增长；当$P_0\to\infty$时，R将渐近收敛于一个由大尺度衰落与DRIS参数决定的常数上界$\log_2\left(1+\frac{\mathcal{L}^{v_{\mathrm{g}}}\mathcal{L}^{v_{\mathrm{I}}^{\mathrm{b}}}}{\mathcal{L}^{v_{\mathrm{d}}^{\mathrm{b}}}N_{\mathrm{D}}\bar{\alpha}}\right)$。与之形成对比的是，根据定理1，Willie的总检测差错概率随P_0的增加而显著降低。需特别指出的是，DRIS产生上述影响的机理，既不依赖于Alice与Bob之间的CSI，也无需消耗任何额外的发射功率。

3　仿真结果与分析

本节通过数值仿真验证DRIS对隐蔽通信的影响，并评估第2节理论分析的有效性。默认仿真参数设置如图2所示。单天线Alice位于坐标(0, 0, 5)米处，单天线Bob随机分布于以(0, 140, 0)米为圆心、半径10至20米的环形区域内。监听者Willie位于(0, 100, 0)米，并利用DRIS对Alice与Bob间的通信进行监控。该DRIS配备有2048个反射单元（$N_{\mathrm{D,h}}$=64,$N_{\mathrm{D,v}}$=32），部署在($-d_{\mathrm{AD}}$米, 0米, 5米)位置，其中Alice与DRIS中心之间的距离d_{AD}设置为1.5米。DRIS采用1比特量化的反射系数，其相移与幅度分别取自集合$\Psi=\{\pi/6,7\pi/6\}$和$\Omega=\mathcal{F}(\Theta)=\{0.8,1\}$[33]，且两种相移被等概率选用。据此，由命题1可计算得$\bar{\alpha}=0.82$。假设Willie在信道相干时间内的检测样本数$M=5$，且检测规则式(9)中的$N=2$。大尺度LOS和NLOS衰落系数基于3GPP传播模型[56]和相关仿真参数在表1定义，噪声功率谱密度为$\sigma_{\mathrm{c}}^2=-170+10\log_{10}(BW)$dBm，系统带宽为

BW = 180kHz。

表1　无线信道仿真参数

仿真参数	取值
视距衰落	$35.6 + 22\log_{10}(d)(dB)$
非视距衰落	$32.6 + 36.7\log_{10}(d)(dB)$
DRIS单元数	NN = 2048
检测样本数	M = 5

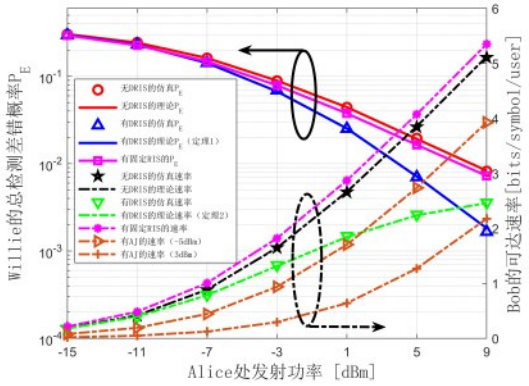

图3　总检测差错概率（左纵轴）以及可达速率（右纵轴）随发射功率的变化关系

图3展示了不同基准方案下，Willie的总检测差错概率（左纵轴）与Bob的可达速率（右纵轴）随Alice发射功率变化的曲线。对比方案包括无DRIS、固定相位RIS、DRIS以及发射功率分别为-5 dBm和3 dBm的传统AJ方案。一般而言，随着$\mathcal{H}_0$与$\mathcal{H}_1$之间“差异”的增大，隐蔽性会下降；这种差异通常可用（KL, Kullback–Leibler）散度等度量来衡量[11]。由于主动干扰信号在$\mathcal{H}_0$与$\mathcal{H}_1$两种假设下均存在，因此AJ并不会显著降低检测错误概率。基于此，我们仅展示AJ对通信性能指标可达速率的影响。结果表明，Willie通过引入DRIS可显著降低其总检测差错概率，固定RIS则介于无RIS与DRIS之间。其根本原因在于DRIS随机时变反射引入的级联分量会增大$\mathcal{H}_0$与$\mathcal{H}_1$下接收统计量的差异，且该差异随Alice发射功率增加而进一步扩大，从而提升可分性并降低Willie的总检测差错概率。同时，与固定RIS增强系统性能不同，DRIS所引入的ACA效应对Alice与Bob之间的隐蔽通信造成严重干扰。值得注意的是，DRIS所造成的干扰效果与3 dBm的高功率AJ相当，在部分中低发射功率区间甚至优于-5 dBm的低功率AJ。与传统需消耗额外功率的主动干扰方案不同，Willie部署DRIS既无需获取Alice-Bob链路的CSI，也不消耗任何额外发射功率。理论曲线与蒙特卡洛仿真结果高度吻合，验证了定理1与定理2的正确性。

从图中可进一步看出，随着Alice发射功率的提高，Willie的检测性能进一步提升，其对合法链路的干扰也更为显著。然而，在DRIS所引入的ACA作用下，单纯增加Alice的发射功率并不能有效改善隐蔽通信性能，反而会带来两方面不利影响：一方面增大了通信行为被Willie侦测的风险，另一方面也导致合法链路遭受更严重的干扰。相较于反射系数固定不变的固定RIS，以及需主动发射信号、消耗功率的AJ方案，DRIS凭借其反射系数的随机时变特性，在无需CSI、完全被动工作的条件下，实现了更优的系统性攻击效能。其中，对抗方Willie引入固定相位RIS相较于引入DRIS，不仅无法降低Willie的总检测差错概率，反而会提升Alice与Bob之间的可达速率。下文将分别针对低发射功率与高发射功率两种情况分析不同因素对隐

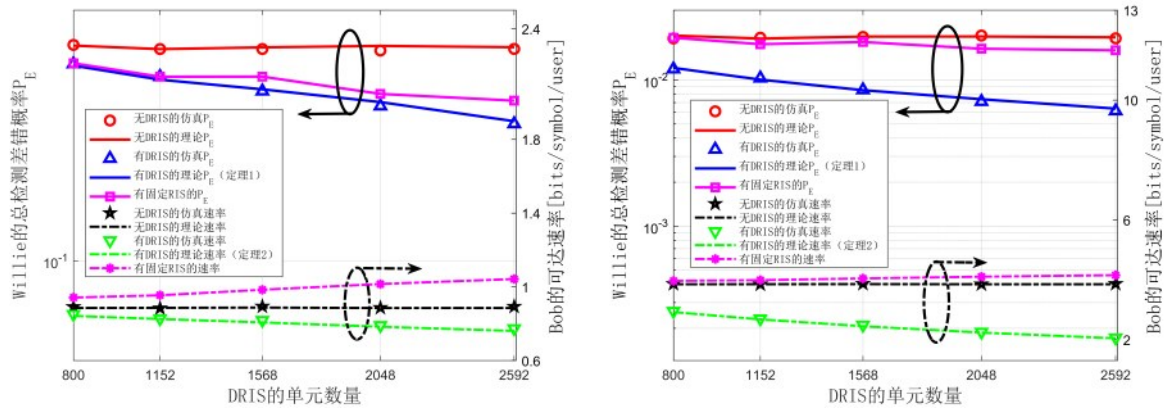

图4　总检测差错概率（左纵轴）以及可达速率（右纵轴）随DRIS单元数量变化关系；(a)为低发射功率(-7 dBm)，(b)为高发射功率(5 dBm)

蔽通信性能的影响规律，且固定RIS与DRIS物理条件设置一致。

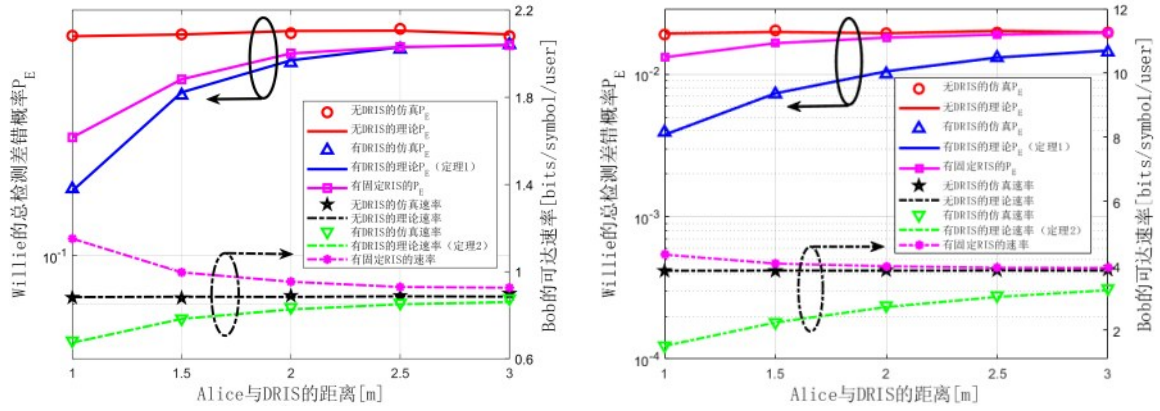

图6　总检测差错概率（左纵轴）以及可达速率（右纵轴）随Alice与DRIS的距离变化关系；(a)为低发射功率（-7 dBm），(b)为高发射功率（5 dBm）

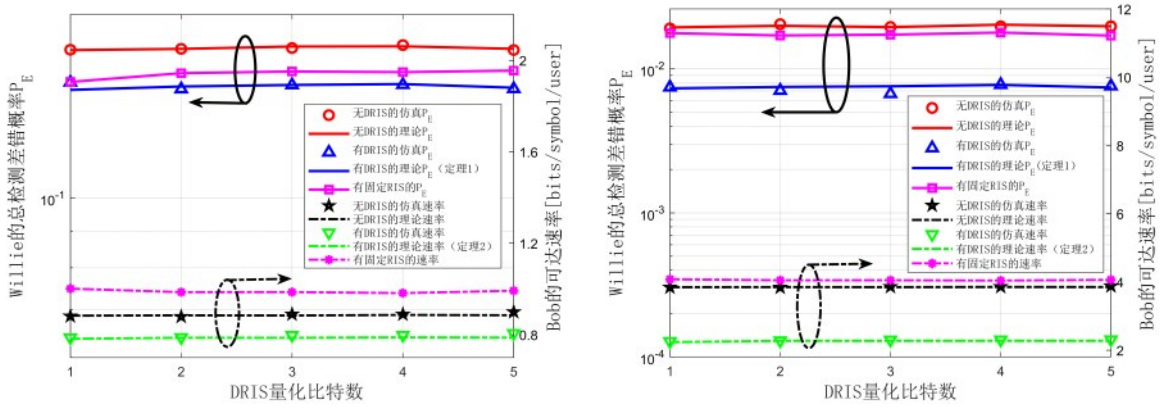

图5　总检测差错概率（左纵轴）以及可达速率（右纵轴）随DRIS量化比特数变化关系；(a)为低发射功率（-7 dBm），(b)为高发射功率（5 dBm）

首先，图4展示了不同基准方案下，Willie的总检测差错概率（左纵轴）与Bob的可达速率（右纵轴）随DRIS反射单元数量的变化关系。其中，图4(a)和(b)分别对应Alice采用低发射功率（-7 dBm）与高发射功率（5 dBm）的情形。与定理1的结论一致，随着DRIS反射单元数量的增加，Willie的总检测差错概率呈下降趋势，且下降速率受Alice发射功率的影响。图4(a)和(b)的结果进一步表明，较高的Alice发射功率有助于Willie获得更高的检测精度。随着反射单元数量的增加，DRIS对系统性能的影响也更为显著。同时，图4(a)和(b)显示Bob的可达速率随DRIS反射单元数量的增加而下降。然而与DRIS相反，固定RIS随反射单元数量增加，可达速率逐渐增加。这说明Willie能够通过配置大规模DRIS在降低自身检测差错概率的同时，有效恶化Alice与Bob间的隐蔽传输性能。与定理1和2相符，当DRIS反射单元数量趋于无穷时，Willie的总检测差错概率与Bob在DRIS干扰下的可达速率均将渐近收敛于零。

图5研究了DRIS响应量化产生的影响。基于文献[51]构建了具有2^b个相移值的b比特量化DRIS模型，其相移值集合定义为$\boldsymbol{\Psi}=\left\{\frac{-\pi}{2},\frac{-\pi}{2}+\frac{\pi}{2^{b-1}},\cdots,\frac{3\pi}{2}-\frac{\pi}{2^{b-1}}\right\}$。进一步根据[56]，第$n$个DRIS单元($n=1,2,\cdots,N_D$)的时变相移与振幅建模为：

$$\begin{aligned}\beta_n(t)&=\mathcal{F}\left(\varphi_n(t)\right)\\&=(1-\alpha_{\min})\left(\frac{\sin\left(\varphi_n(t)-\phi\right)+1}{2}\right)^{\mu}+\alpha_{\min}\end{aligned}\tag{32}$$

其中，$\varphi_n(t)\in\Psi$为第n个DRIS单元的相移，$\alpha_{\min}=$

$min\{\Omega\}$为DRIS的最小振幅，μ与ϕ为由RIS具体实现方式决定的常数。参照文献[57]的设置，取$\alpha_{\min}$ = 0.8，μ = 1.6，ϕ = 0。在大多数RIS研究中，提升量化比特数通常可带来更显著的系统性能增益。然而与先前研究相反，图5显示提高DRIS的量化分辨率对Willie的总检测差错概率以及Bob的可达速率影响均较为有限。基于命题，DRIS的级联信道统计特性并不依赖于其反射系数的具体取值，而是取决于反射幅度平方的期望。尽管提高量化比特数为DRIS提供了更多可选的幅度取值，但根据式(32)可知，这并不会显著改变$\bar{\alpha}$的数值。鉴于采用更高量化精度的DRIS并不能增强对隐蔽通信的干扰，本文选用1比特量化作为默认基线。该设置更贴合IoT低成本、低功耗部署：量化比特数越高，DRIS控制信令与硬件实现复杂度越高，进而增加配置开销与能耗[58]。综合图4与图5的结果可知，仅需采用具备大规模反射单元的1比特DRIS，即可有效提升监听者Willie的检测精度，同时显著恶化Alice与Bob之间的隐蔽通信质量。

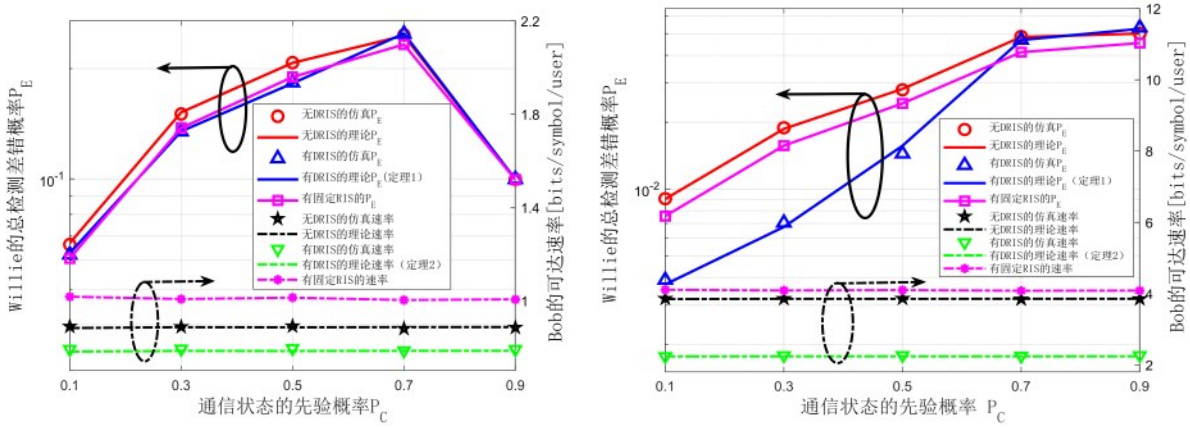

图8　总检测差错概率（左纵轴）以及可达速率（右纵轴）随通信状态的先验概率变化关系；(a)为低发射功率（-7 dBm），(b)为高发射功率（5 dBm）

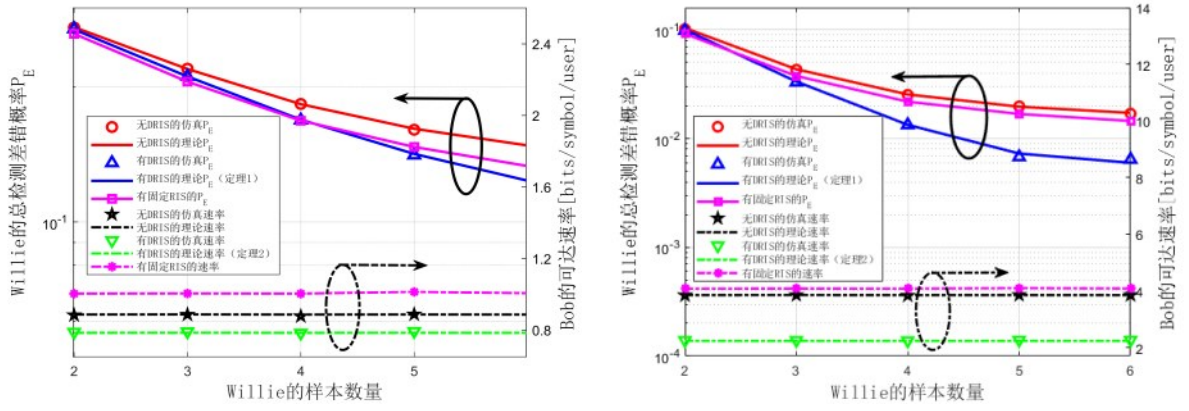

图7　总检测差错概率（左纵轴）以及可达速率（右纵轴）随Willie的样本数量变化关系；(a)为低发射功率（-7 dBm），(b)为高发射功率（5 dBm）

图6展示了在低发射功率（-7 dBm）与高发射功率（5 dBm）条件下，Willie的总检测差错概率以及Bob的可达速率随Alice与DRIS（固定RIS）间距离的变化关系。可以看出，随着Alice与固定RIS间距离的增大，其对通信性能的增益逐渐降低。其原因在于Alice与固定RIS间距离增大将加剧级联路径损耗，使Bob端反射有效功率下降，从而削弱链路增益。随着Alice与DRIS间距离的增大，DRIS对Willie检测性能及Bob通信速率的干扰效果均逐渐减弱。换言之，若监听者Willie意图有效监控Alice与Bob之间的隐蔽通信并最大化DRIS的攻击效果，应将DRIS部署于尽可能靠近Alice的

位置。

图7展示了Willie检测所用样本数量与Bob可达速率以及总检测差错概率之间的关系。可以看出，样本数量对Bob的通信性能无明显影响，但无论是否部署DRIS及固定RIS，该参数均会显著影响Willie的总检测差错概率。随着样本数量的增加，Willie的总检测差错概率显著下降。需要注意的是，样本数的取值受限于信道相干时间内可获取的最大样本数。上述结果表明，在信道相干时间约束下，增加检测样本数量可显著改善Willie处检测差错概率。

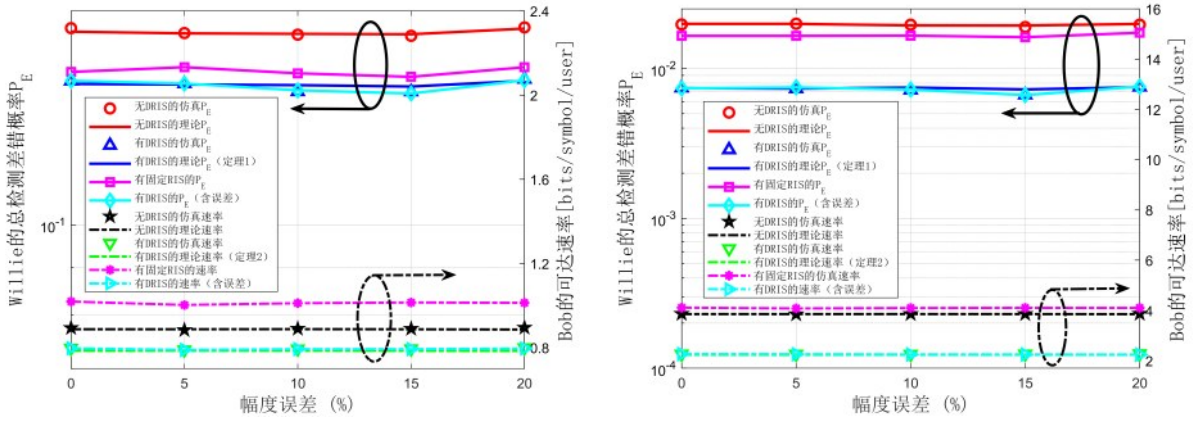

图9　总检测差错概率（左纵轴）以及可达速率（右纵轴）随幅度误差变化关系；(a)为低发射功率(-7 dBm)，(b)为高发射功率(5 dBm)

图8展示了低、高发射功率下Willie的总检测差错概率及Bob可达速率随P_C的变化关系。结果表明，随着P_C增大，总检测差错概率在中等P_C区间呈上升趋势，并在较大P_C范围内逐渐趋于平缓；在低功率情形下，曲线在大P_C端进一步出现回落。上述现象源于非等先验条件下最优检测门限随P_C增大而降低，使检测器更偏向判决“存在通信”，从而虚警相关的加权错误项更易占主导；当P_C进一步增大时，检测错误概率逐步进入饱和区间（虚警趋近上界、漏检趋近下界），导致总检错概率对P_C的敏感性降低并表现为平台化，而低功率下门限更易触及物理下界，从而导致末端回落。另一方面，Bob可达速率随P_C基本保持稳定，表明在固定发射功率与信道统计不变的设置下，先验概率主要影响Willie的检测过程而不改变Bob端的速率。方案对比还表明，DRIS在提升Willie检测能力的同时引入ACA，显著降低Bob可达速率；固定相位RIS不产生同等强度的时变ACA，其速率性能优于DRIS。

图9展示了在相位误差$\sigma_\phi = 5^\circ$，幅度误差σ_a从0到20%时，Willie的总检测差错概率及Bob可达速率随σ_a的变化关系。可以观察到，在所考虑的幅度误差标准差范围内，各方案的性能曲线整体变化较为平缓。对于Willie而言，DRIS理想与含误差DRIS两种情形下的总检测差错概率基本重合，表明在$\sigma_\phi = 5^\circ$且幅度扰动为乘性小幅波动并满足无源幅度约束的条件下，反射系数不确定性对能量统计量的整体分布影响有限，从而不会显著改变基于阈值判决的检测性能。对于Bob而言，可达速率随幅度误差的变化同样不明显，说明DRIS引入的等效ACA干扰功率在该误差水平下仅发生轻微波动，系统通信性能保持稳定。总体而言，图9验证了在典型硬件环境幅度扰动范围内，所采用的检测规则及相应的通信性能评估对DRIS反射系数误差具有较好的鲁棒性。

4　结束语

在本文中，我们提出了一种新的面向IoT系统中隐蔽通信的检测方案，能够在无需获取Alice-Bob的CSI且不引入额外发射功率的条件下，有效提升监听者Willie对隐蔽通信的检测能力，并实现对Alice-Bob链路的无源干扰。理论分析与仿真结果表明，该方法具有以下重要特性：

1)监听者Willie采用的检测规则充分考虑了时变DRIS的动态特性。结果表明，该DRIS在有效降低Willie总检测差错概率的同时，也会对Alice与

Bob 间的合法通信造成显著干扰；即使 Willie 发生漏检，此干扰依然存在。

2)结果表明，在 DRIS 引入的 ACA 干扰下，提升 Alice 的发射功率并不能有效改善其隐蔽通信的性能，反而会加剧 DRIS 引入的 ACA 效应，从而进一步恶化 Alice 与 Bob 之间的通信质量，并增加 Alice 被 Willie 侦测到的风险。

3)结果表明，采用 1 比特量化的 DRIS 即可显著提升监听者 Willie 的检测精度，并有效恶化 Alice 与 Bob 间的隐蔽通信性能。为最大化 DRIS 的攻击效果，应将 DRIS 部署于 Alice 的邻近区域，以增强其对合法链路的干扰强度。

本文表明，即使在无 CSI 且不引入额外发射功率的条件下，由监听者 Willie 非法部署的 DRIS 仍会对合法隐蔽通信系统构成严重威胁，这一发现揭示了无线通信物理层安全中亟待关注的关键问题。针对上述威胁，后续可进一步研究信号分类、异常检测及自适应波束赋形等缓解措施，以提升隐蔽通信系统的对抗鲁棒性。本文主要针对准静态场景开展分析，而在更一般的移动性条件下，多普勒扩展、相干时间缩短与 DRIS 随机时变反射之间的耦合作用可能进一步改变系统性能，这一问题仍需在显式时变信道模型框架下作深入研究。

参考文献：

[1] 李赞, 廖晓闽, 石嘉, 等. 面向认知物联网的隐蔽通信智能功率控制[J]. 物联网学报, 2020, 4(1): 52-58.
LI Z, LIAO X M, SHI J, et al. Intelligent power control for covert communication in cognitive Internet of Things[J]. Chinese Journal on Internet of Things, 2020, 4(1): 52-58.

[2] YANG Y, WU L, YIN G, et al. A survey on security and privacy issues in Internet-of-Things[J]. IEEE Internet of Things Journal, 2017, 4(5): 1250-1258.

[3] MUKHERJEE A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints[J]. Proceedings of the IEEE, 2015, 103(10): 1747-1761.

[4] FERNANDES E, RAHMATI A, EYKHOLT K, et al. Internet of Things security research: A rehash of old ideas or new intellectual challenges?[J]. IEEE Security & Privacy, 2017, 15(4): 79-84.

[5] KUUTTI S, FALLAH S, KATSAROS K, et al. A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications[J]. IEEE Internet of Things Journal, 2018, 5(2): 829-846.

[6] CATARINUCCI L, et al. An IoT-aware architecture for smart healthcare systems[J]. IEEE Internet of Things Journal, 2015, 2 (6): 515-526.

[7] XU L D, HE W, LI S C. Internet of Things in industries: A survey [J]. IEEE Transactions on Industrial Informatics, 2014, 10(4): 2233-2243.

[8] 张志飞, 刘峰, 葛祎阳, 等. 一种基于深度可分离卷积和注意力机制的入侵检测方法[J]. 物联网学报, 2023, 7(1): 49-59.
ZHANG Z F, LIU F, GE Y Y, et al. An intrusion detection method based on depthwise separable convolution and attention mechanism[J]. Chinese Journal on Internet of Things, 2023, 7(1): 49-59.

[9] 丁凯, 黄宜都, 陶铭, 等. 基于联邦强化学习的面向边缘网络的入侵检测方法研究[J]. 物联网学报, 2024, 8(4): 140-155.
DING K, HUANG Y D, TAO M, et al. Research on intrusion detection method for edge networks based on federated reinforcement learning[J]. Chinese Journal on Internet of Things, 2024, 8 (4): 140-155.

[10] CHEN X, AN J, XIONG Z, et al. Covert communications: A comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2023, 25(2): 1173-1198.

[11] 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.

[12] TOPAL O A, KARABULUT-KURT G. Covert communication in cooperative NOMA networks[C]//Proceedings of the 2020 28th Signal Processing and Communications Applications Conference (SIU). Piscataway: IEEE Press, 2020: 1-4.

[13] 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.

[14] LI K, KELLY P A, GOECKEL D. Optimal power adaptation in covert communication with an uninformed jammer[J]. IEEE Transactions on Wireless Communications, 2020, 19(5): 3463-3473.

[15] HU J, YAN S, ZHOU X, et al. Covert communication achieved by a greedy relay in wireless networks[J]. IEEE Transactions on Wireless Communications, 2018, 17(7): 4766-4779.

[16] LIN M, LIU C, WANG W. Relay-assisted uplink covert communication in the presence of multi-antenna warden and uninformed jamming[J]. IEEE Transactions on Communications, 2024, 72(4): 2124-2137.

[17] SUN R, YANG B, MA S, et al. Covert rate maximization in wireless full-duplex relaying systems with power control[J]. IEEE Transactions on Communications, 2021, 69(9): 6198-6212.

[18] HU J, SHAHZAD K, YAN S, et al. Covert communications with a full-duplex receiver over wireless fading channels[C]//Proceedings of the 2018 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2018: 1-6.

[19] LIU Z, LIU J, ZENG Y, et al. Covert wireless communications in IoT systems: Hiding information in interference[J]. IEEE Wireless Communications, 2018, 25(6): 46-52.

[20] WANG D, QI P, ZHANG N, et al. Covert wireless communication with spectrum mask in Internet of Things networks[J]. IEEE Transactions on Communications, 2021, 69(12): 8402-8415.

[21] WANG D, FU Q, SI J, et al. Improper Gaussian signaling based covert wireless communication in IoT networks[C]//Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE Press, 2021: 1-6.

[22] HU J, YAN S, ZHOU X, et al. Covert communications without channel state information at receiver in IoT systems[J]. IEEE Internet of Things Journal, 2020, 7(11): 11103-11114.

[23] GAO C, YANG B, JIANG X, et al. Covert communication in relay-assisted IoT systems[J]. IEEE Internet of Things Journal, 2021, 8(8): 6313-6323.

[24] WANG B, et al. Relay-assisted finite blocklength covert communications for Internet of Things[J]. IEEE Internet of Things Journal, 2024, 11(24): 39984-39993.

[25] FENG S, LU X, SUN S, et al. Mean-field artificial noise assistance and uplink power control in covert IoT systems[J]. IEEE Transactions on Wireless Communications, 2022, 21(9): 7358-7373.

[26] LIU Z, LIU J, ZENG Y, et al. Covert wireless communication in IoT network: From AWGN channel to THz band[J]. IEEE Internet of Things Journal, 2020, 7(4): 3378-3388.

[27] ZHANG H, ZENG S, DI B, et al. Intelligent omni-surfaces for full-dimensional wireless communications: Principles, technology, and implementation[J]. IEEE Communications Magazine, 2022, 60(2): 39-45.

[28] HUANG C, HU S, ALEXANDROPOULOS G C, et al. Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends[J]. IEEE Wireless Communications, 2020, 27(5): 118-125.

[29] WU Q, ZHANG R. Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming[J]. IEEE Transactions on Wireless Communications, 2019, 18(11): 5394-5409.

[30] WU Q, ZHANG S, ZHENG B, et al. Intelligent reflecting surface aided wireless communications: A tutorial[J]. IEEE Transactions on Communications, 2021, 69(5): 3313-3351.

[31] CUI T, QI M, WAN X, et al. Coding metamaterials, digital metamaterials and programmable metamaterials[J]. Light: Science & Applications, 2014, 3, e218.

[32] HUANG C, ZAPPONE A, ALEXANDROPOULOS G C, et al. Reconfigurable intelligent surfaces for energy efficiency in wireless communication[J]. IEEE Transactions on Wireless Communications, 2019, 18(8): 4157-4170.

[33] HUANG C, MO R, YUEN C. Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(8): 1839-1850.

[34] XU Y, et al. RIS-assisted heterogeneous backscatter communications: A robust design[J]. IEEE Transactions on Communications, 2025, 73(12): 13214-13225.

[35] LV L, WU Q, LI Z, et al. Covert communication in intelligent reflecting surface-assisted NOMA systems: Design, analysis, and optimization[J]. IEEE Transactions on Wireless Communications, 2022, 21(3): 1735-1750.

[36] WANG C, XIONG Z, ZHENG M, et al. Covert communications via two-way IRS with noise power uncertainty[J]. IEEE Transactions on Communications, 2024, 72(8): 4803-4815.

[37] WU Y, CHEN X, LIU M, et al. IRS-assisted covert communication with equal and unequal transmit prior probabilities[J]. IEEE Transactions on Communications, 2024, 72(5): 2897-2912.

[38] WANG C, CHEN X, AN J, et al. Covert communication assisted by UAV-IRS[J]. IEEE Transactions on Communications, 2023, 71 (1): 357-369.

[39] WANG Q, GUO S, WU C, et al. STAR-RIS aided covert communication in UAV air-ground networks[J]. IEEE Journal on Selected Areas in Communications, 2025, 43(1): 245-258.

[40] XIAO H, et al. Simultaneously transmitting and reflecting RIS (STAR-RIS) assisted multi-antenna covert communication: Analysis and optimization[J]. IEEE Transactions on Wireless Communications, 2024, 23(6): 6438-6452.

[41] HUANG H, DAI L, ZHANG H, et al. DISCO might not be funky: Random intelligent reflective surface configurations that attack[J]. IEEE Wireless Communications, 2024, 31(5): 76-82.

[42] WANG H, HAN Z, SWINDLEHURST A L. Channel reciprocity attacks using intelligent surfaces with non-diagonal phase shifts [J]. IEEE Open Journal of the Communications Society, 2024, 5: 1469-1485.

[43] HUANG H, ZHANG Y, ZHANG H, et al. Illegal intelligent reflecting surface based active channel aging: When jammer can attack without power and CSI[J]. IEEE Transactions on Vehicular Technology, 2023, 72(8): 11018-11022.

[44] HUANG H, ZHANG Y, ZHANG H, et al. Disco intelligent reflecting surfaces: Active channel aging for fully-passive jamming attacks[J]. IEEE Transactions on Wireless Communications, 2024, 23(1): 806-819.

[45] HUANG H, DAI L, ZHANG H, et al. Anti-jamming precoding against disco intelligent reflecting surfaces based fully-passive jamming attacks[J]. IEEE Transactions on Wireless Communications, 2024, 23(8): 9315-9329.

[46] BESSON O, STOICA P, KAMIYA Y. Direction finding in the presence of an intermittent interference[J]. IEEE Transactions on Signal Processing, 2002, 50(7): 1554-1564.

[47] LANCE E, KALEH G K. A diversity scheme for a phase-coherent frequency-hopping spread-spectrum system[J]. IEEE Transactions on Communications, 1997, 45(9): 1123-1129.

[48] JEUNG J, JEONG S, LIM J. Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN[C]//Proceedings of the 2011 IEEE Military Communications Conference

(MILCOM). Piscataway: IEEE Press, 2011: 1231-1236.

[49] LUO Y, CHENG L, HU H, et al. Context-rich privacy leakage analysis through inferring apps in smart home IoT[J]. IEEE Internet of Things Journal, 2021, 8(4): 2736-2750.

[50] HUANG H, ZHANG H, CAI Y, et al. Simultaneously exposing and jamming covert communications via disco reconfigurable intelligent surfaces[J]. IEEE Journal on Selected Areas in Communications, 2026, 44: 1708-1721.

[51] ZHANG S, ZHANG R. Intelligent Reflecting Surface Aided Multi-User Communication: Capacity Region and Deployment Strategy[J]. IEEE Transactions on Communications, 2021, 69(9): 5790-5806.

[52] TSE D, VISWANATH P. Fundamentals of wireless communication[M]. Cambridge: Cambridge University Press, 2005.

[53] CUI M, DAI L. Channel estimation for extremely large-scale MIMO: Far-field or near-field?[J]. IEEE Transactions on Communications, 2022, 70(4): 2663-2677.

[54] LONG R Z, LIANG Y C, GUO H Y, et al. Symbiotic radio: A new communication paradigm for passive Internet of Things[J]. IEEE Internet of Things Journal, 2020, 7(2): 1350-1363.

[55] O'DONOUGHUE N, MOURA J M F. On the product of independent complex Gaussians[J]. IEEE Transactions on Signal Processing, 2012, 60(3): 1050-1063.

[56] Further Advancements for E-UTRA Physical Layer Aspects (Release 9), document 3GPP TS 36.814, 2010.

[57] ABEYWICKRAMA S, ZHANG R, WU Q, et al. Intelligent reflecting surface: Practical phase shift model and beamforming optimization[J]. IEEE Transactions on Communications, 2020, 68 (9): 5849-5863.

[58] TANG J, CUI M, XU S, et al. Transmissive RIS for B5G communications: Design, prototyping, and experimental demonstrations [J]. IEEE Transactions on Communications, 2023, 71(11): 6605-6615.