无线隐蔽通信容量限与实现技术综述

陈炜宇[1]，骆俊杉[1]，王方刚[2]，丁海洋[3]，王世练[1]，夏国江[4]

（1. 国防科技大学电子科学学院，湖南 长沙 410073；2. 北京交通大学轨道交通控制与安全国家重点实验室，北京 100044；
3. 国防科技大学信息通信学院，湖北 武汉 430019；4. 北京宇航系统工程研究所，北京 100076）

摘 要：梳理无线隐蔽通信与相关概念的区别和联系，聚焦基于假设检验理论和信息论的无线隐蔽通信研究，介绍了基本研究模型与具体模型分类，分容量限和实现技术两部分对现有工作进行综述。前者依据极限速率的量级，将极限速率揭示工作分均方根速率和非零正速率两类进行综述；后者依据应用场景的不同，对无线隐蔽通信系统性能分析与实现方案优化工作进行分类和综述。最后，探讨了具有高价值的潜在研究方向。

关键词：无线隐蔽通信；低检测概率通信；物理层安全；信息安全

中图分类号：TN92

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022153

Survey of capacity limits and implementation techniques in wireless covert communication

CHEN Weiyu[1], LUO Junshan[1], WANG Fanggang[2], DING Haiyang[3], WANG Shilian[1], XIA Guojiang[4]

1. College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China
2. State Key Lab of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China
3. College of Information and Communication, National University of Defense Technology, Wuhan 430019, China
4. Beijing Institute of Astronautical Systems Engineering, Beijing 100076, China

Abstract: The differences and connections between wireless covert communication (WCC) and related concepts were clarified. The WCC research based on hypothesis testing theory and information theory was focused. The basic research model and the categories of specific models were introduced. The existing works were classified and reviewed in two parts, namely, capacity limits and implementation techniques. The former part reviewed the works that reveal the limit rate, and divided them into two categories as per the order of the limit rate: squared root rate and positive rate. The latter part reviewed the works that analyze the performance of WCC systems and optimize the implementation schemes, and classified them as per their application scenarios. Finally, potential research directions were discussed.

Keywords: wireless covert communication, low probability of detection communication, physical-layer security, information security

0 引言

随着 5G 商用和大数据时代的到来，海量隐私数据将由无线通信系统传输，无线信道的开放性对这些数据的安全提出了挑战，且这一挑战会随着无处不在的连接和孪生城市等愿景逐步落地而更加

收稿日期：2022−04−25；**修回日期：**2022−06−13

通信作者：骆俊杉，ljsnudt@foxmail.com

基金项目：国家自然科学基金资助项目（No.61871387, No.61871471, No.62171445）；中央高校基本科研业务费专项资金资助项目（No.2020JBM081）；国防科技大学研究基金资助项目（No.ZK20-40）；轨道交通控制与安全国家重点实验室自主课题资助项目（No.RCS2022ZT011）；陕西高校青年创新团队基金资助项目

Foundation Items: The National Natural Science Foundation of China (No.61871387, No.61871471, No.62171445), The Fundamental Research Funds for the Central Universities (No.2020JBM081), The NUDT Research Fund (No.ZK20-40), The State Key Laboratory of Rail Traffic Control and Safety (No.RCS2022ZT011), Youth Innovation Team of Shaanxi Universities

严峻。一直以来，基于密码学的上层加密技术是保护数据安全最主要的手段，利用没有密钥就难以求解的复杂数学问题进行数据加密，需要近乎不可达的算力才能破解，然而，这类技术正面临越来越大的挑战，主要包括以下几个方面。

① 计算能力特别是量子计算的发展使这些数学问题能够在越来越短的时间内被破解。

② 计时攻击、能量攻击、电磁攻击等边信道攻击方法绕开了明密文之间的复杂数学逻辑，直接提取中间信息[1]。

③ 分发和管理密钥需要额外开销，尤其在去中心化的随遇接入高动态网络中，分发和管理密钥是困难的。

④ 大量物联网设备采用相同的密码协议，使单一密码协议被破解的损失更大。

物理层安全技术通过增加和利用合法信道与窃听信道的差异性以及无线信道的随机性，从根本上确保信息对于非法窃听者的不可解译性，有效弥补了上述密码学安全技术的不足[2]。然而，隐私数据不仅包括通信内容，隐藏通信行为本身具有重要意义，包括以下几个方面。

① 通信行为是否发生、通信时间特征、通信发生的地点、发射机的移动轨迹等也是重要隐私。

② 不被发现的通信行为不会被干扰或解译。

③ 在某些通信场景中发现即摧毁，隐藏通信行为能够有效保护战略目标。

为此，区别于传统物理层安全技术，面向无线信道的、位于物理层的、安全层面更前沿的低检测概率（LPD, low probability of detection）通信技术近年来得到广泛关注[3]。其目标是在提高发射机（通常记为 Alice）向接收机（通常记为 Bob）的可靠信息传输速率的同时，保证监察者（通常记为 Willie）无法正确判断是否存在通信行为。

1) 与相关概念的区别和联系

一些文献将 LPD 和低截获概率（LPI, low probability of interception）等同。LPI 也位于物理层，严格来说包含防通信行为检测、防信号特征提取、防通信内容窃取 3 个研究层面。因此，LPD 属于 LPI，但反过来 LPI 技术不一定是 LPD 技术，如跳频技术通过捷变频率使第三方无法跟踪接收，但在任意时刻仍属于能量集中的窄带信号，易被发现。

LPD 通信在大多数文献中也称为隐蔽通信，本文剩余部分也使用隐蔽通信这一表述。事实上，更广义的隐蔽通信还包括以下技术。

① 隐写技术，是指以合法消息的特征不发生显著变化为前提将信息隐藏在其中。广义上包括在应用层将信息隐藏在视频、图像、音频、文本中；在链路层将信息隐藏在某些位或字段上；在物理层将隐蔽信号叠加在合法信号上同时发出，对合法信号做微小改动以承载隐蔽信息，将信息隐藏在纠错码的冗余比特中等手段。这些隐写技术在可公开的通信行为中隐藏额外的通信行为，而在本文所聚焦的隐蔽通信中，Alice 无可公开的通信行为，甚至是否存在有通信意图的发射机也不为 Willie 所知。

② 隐蔽信道，是指利用系统中本不被用于通信的资源传输隐蔽信息，同时保证系统近乎正常运行而不被发现。其最初被用于庞大的单一系统，随后扩展到计算机网络中[4]。隐蔽信道分为时间隐蔽信道和存储隐蔽信道，它们分别基于对资源的使用时间和本不应承载有效信息的字段传递信息。隐蔽信道所研究的是大型计算机内部或计算机网络中的隐蔽通信，而本文所关注的是无线信道中的隐蔽通信。

2) 传统隐蔽通信研究的局限性与本文的主要内容

以直接序列扩频、chirp 扩频等为代表的扩展频谱通信技术于 20 世纪初被提出，至今仍是最有效的隐蔽通信技术手段。其原理为将信号功率分摊到较宽的频带范围，使信号功率谱被噪声掩盖。由于扩展频谱通信在国防领域的重要性，早已出现针对性的检测技术[5-6]。Heidari-Bateni 等[7-8]提出以混沌序列作为扩频码，利用其非周期性进一步提高隐蔽性，相应的检测技术已于 2015 年被提出[9]。

在传统隐蔽通信研究与应用过程中，主要基于相关域、能量域及各变换域的分析实现通信信号检测，攻守双方虽然通过不断提出新通信体制和新检测技术提高隐蔽或检测能力，但对隐蔽通信性能的分析始终没有统一可靠的标准。关于这些工作的综述可参考文献[6,10-11]。

2013 年，Bash 等[12]将对通信行为的检测问题建模为二元假设检验问题，开创性地结合假设检验理论和信息论分析隐蔽通信的容量，建立了理论坚实且广泛适用的隐蔽通信分析框架。文献[12]的工作暂时没有启发出新的隐蔽通信技术手段，但掀起了对不同场景下无线隐蔽通信容量限和现有技术手段的性能分析与实现方案优化的研究热潮。本文将针对这些由假设检验理论和信息论支撑的无线

隐蔽通信研究工作进行综述，相关综述包括中文文献[13-14]和英文文献[15]。其中，文献[13]将现有工作分为基础理论研究、隐蔽系统研究、隐蔽技术应用三部分进行综述；文献[14]除了分标准通信、辅助通信、中继通信、其他等四类场景综述无线隐蔽通信，还涵盖了各层级的隐写技术；文献[15]分无线隐蔽通信、图像隐写、视频隐写、音频隐写、文本隐写、基于网络协议的隐蔽通信、基于区块链的隐蔽通信等七部分进行综述，涵盖物理层、应用层、网络层。相较于上述工作，本文聚焦于物理层的无线隐蔽通信，分容量限和实现技术两部分深入介绍该领域的经典工作和新的重要发现。

1　无线隐蔽通信研究模型

1.1　研究模型、常用隐蔽性能指标与研究思路

无线隐蔽通信模型如图 1 所示。在无线隐蔽通信模型中，Alice 通过无线信道向 Bob 发送信息，Willie 侦听并判断 Alice 是否在通信（或是否有发射机在通信）。Alice 的目标包括保证 Bob 接收信号质量和使 Willie 无法正确判断。

Willie 所面对的是一个二元假设检验问题，其接收信号可表示为

$$y_{\mathrm{w}}(i)=\begin{cases} I(i)+N(i), & \mathcal{H}_0 \\ S(i)+I(i)+N(i), & \mathcal{H}_1 \end{cases} \tag{1}$$

其中，$S(i)$、$I(i)$和$N(i)$分别表示 Willie 在第i个符号时间内接收到的信号、干扰和噪声，$\mathcal{H}_0$表示 Alice 未进行通信，$\mathcal{H}_1$表示 Alice 进行了通信。由于 Willie 仅需要进行二元判决，而 Bob 需要判断 Alice 所发码字是众多可能码字中的哪一个，无先验信息优势难以实现隐蔽通信，因此 Alice 和 Bob 通常需要提前共享一定长度的密钥，从而得以约定秘密的通信时间和码本，后者指合法码字集及码字与消息符号的对应关系。

Willie 基于其所关心的全部接收信号进行联合判决，以$\mathcal{D}_0$表示判定无通信行为，$\mathcal{D}_1$表示判定有通信行为，通常以错误检测概率$\mathbb{P}_e$，即虚警概率与漏检概率的先验概率加权和$\Pr(\mathcal{D}_1\mid\mathcal{H}_0)\Pr(\mathcal{H}_0)+\Pr(\mathcal{D}_0\mid\mathcal{H}_1)\Pr(\mathcal{H}_1)$量化 Willie 的检测性能，该值越接近于$\min\{\Pr(\mathcal{H}_0),\Pr(\mathcal{H}_1)\}$，隐蔽性能越好。对于先验概率未知的情况，通常假设$\Pr(\mathcal{H}_0)=\Pr(\mathcal{H}_1)=0.5$。

也可以将虚警概率与漏检概率直接求和作为隐蔽性能指标或隐蔽性能约束，这是因为$\mathbb{P}_e\geqslant\big(\Pr(\mathcal{D}_1\mid\mathcal{H}_0)+\Pr(\mathcal{D}_0\mid\mathcal{H}_1)\big)\min\{\Pr(\mathcal{H}_0),\Pr(\mathcal{H}_1)\}$。保守考虑，通常假设 Willie 使用最优检测器，其性能满足[16]

$$\Pr(\mathcal{D}_1\mid\mathcal{H}_0)+\Pr(\mathcal{D}_0\mid\mathcal{H}_1)=1-\mathcal{V}_T(\mathbb{P}_0,\mathbb{P}_1) \tag{2}$$

其中，$\mathcal{V}_T(\mathbb{P}_0,\mathbb{P}_1)=\frac{1}{2}\left\|p_0(y_{\mathrm{w}})-p_1(y_{\mathrm{w}})\right\|_1$表示 Willie 所关心的全部接收信号在$\mathcal{H}_0$下的联合概率分布$\mathbb{P}_0$与$\mathcal{H}_1$下的联合概率分布$\mathbb{P}_1$的总变分距离，$p_0(y_{\mathrm{w}})$和$p_1(y_{\mathrm{w}})$分别表示概率分布$\mathbb{P}_0$和$\mathbb{P}_1$的概率密度函数。因此，总变分距离也是常用的隐蔽性能指标。

由于总变分距离的表达式过于复杂，许多研究进一步使用 Pinsker 不等式获取关于错误检测概率的下界并以其为隐蔽约束[17]，如式(3)和式(4)所示。

$$\mathcal{V}_T(\mathbb{P}_0,\mathbb{P}_1)\leqslant\sqrt{\frac{D(\mathbb{P}_0\,\|\,\mathbb{P}_1)}{2}} \tag{3}$$

$$\mathcal{V}_T(\mathbb{P}_0,\mathbb{P}_1)\leqslant\sqrt{\frac{D(\mathbb{P}_1\,\|\,\mathbb{P}_0)}{2}} \tag{4}$$

其中，$D(\mathbb{P}_0\,\|\,\mathbb{P}_1)=\int p_0(y_{\mathrm{w}})\ln\frac{p_0(y_{\mathrm{w}})}{p_1(y_{\mathrm{w}})}\mathrm{d}y_{\mathrm{w}}$为由$\mathbb{P}_0$到$\mathbb{P}_1$的相对熵，也称为 KL（Kullback-Leibler）散度。需要注意的是，由于相对熵的非对称性，由$D(\mathbb{P}_0\,\|\,\mathbb{P}_1)$和$D(\mathbb{P}_1\,\|\,\mathbb{P}_0)$作为隐蔽约束得到的结果一般不同。

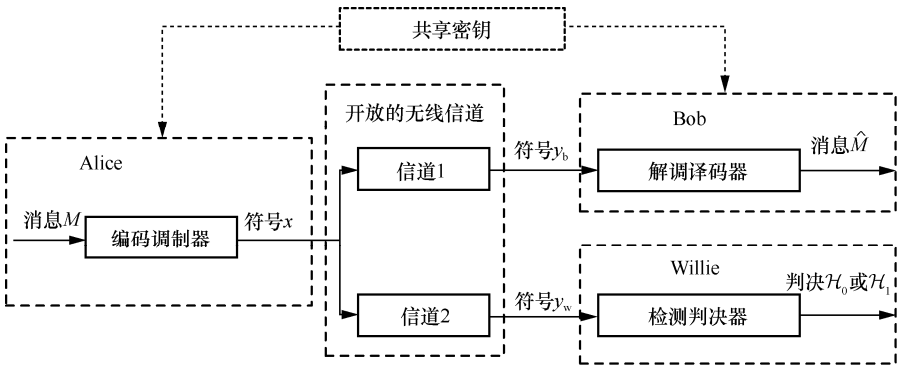


图 1　无线隐蔽通信模型

由式(2)～式(4)及总变分距离和相对熵的定义可知，要取得良好的隐蔽性要求 $\mathbb{P}_0$ 和 $\mathbb{P}_1$ 的差异较小，因而要求泄露至 Willie 的信号功率足够小，限制了发射功率，使可靠传输速率降低。为此，从使 $\mathbb{P}_1$ 接近 $\mathbb{P}_0$ 的角度出发，可利用波束成形、低功率中继转发、可重构智能表面等技术抑制信号泄露，规避 Bob 接收功率降低的问题。另一方面，从使 $\mathbb{P}_0$ 接近 $\mathbb{P}_1$ 的角度出发，可利用辅助节点或全双工接收机释放的人工噪声、周围环境中的随机通信行为、噪声功率随温度的自然变化等，强化和利用 Willie 对背景噪声和干扰的不确定性，使 Willie 无法辨别可疑的接收信号是由通信行为导致的还是由于噪声和干扰发生了变化。相关研究将在后文中做详细介绍。

1.2 模型的具体分类

可根据离散时间和连续时间、离散信道和连续信道 2 种分类方式对现有研究进行分类。其中，离散时间模型基于离散时刻上的抽样点进行分析，而离散信道是指输入、输出符号取自离散有限范围。依靠离散模型的简洁性更易于得到重要研究结论，而连续模型能够捕捉实际系统中更多的实现细节及其带来的隐蔽性能影响，结果更严谨，分析难度往往也更高。例如，离散时间模型可以认为是经过完美的 sinc 函数匹配滤波和位定时等步骤后从连续时间模型简化而来的，但忽略了不完美的信号处理和不同来源信号异步到达的影响，以及过采样可能提供的检测增益，使基于离散时间模型得到的结论并不总适用于连续时间模型[18]。如不加说明，后文所提及的文献均为离散时间连续信道模型。

还可以按实值信号模型和复值信号模型分类。由于在通信理论中复数的实部和虚部可以独立承载信息，基于更简易的实值信号模型得到的结论通常不失一般性，可以直接推广至复值信号模型。但对于存在多个相关信源的情形，由于不同信源到同一节点的相移通常不同，需采用复值信号模型[19]。

除使用多发射天线或可重构智能表面通过波束成形完全避免信号泄露这一情况之外，需要利用 Willie 对其接收信号的不确定性实现隐蔽。根据不确定性的来源，可将其分为瞬时噪声不确定性、噪声功率不确定性、信道不确定性、干扰不确定性、通信时间不确定性等。正如本文将论述的，瞬时噪声不确定性提供了基础隐蔽性，但其能支撑的可靠隐蔽速率非常有限，利用其他的不确定性可以达到更高的速率。值得注意的是，各种不确定性可以同时存在，只是不同研究有不同侧重。

无限码长和有限码长是另一重要分类方式。对于前者，一次传输的符号总数 n 充分大，此时通常以 Bob 无差错接收作为基本要求。而对于低时延通信场景，需采用有限码长模型，此时不可能实现无差错接收，需要在传输速率、可靠性、隐蔽性间进行折中，常用吞吐量（即正确接收的信息量）作为 Bob 的性能指标。无限码长模型常用渐近符号[20]表示结论，本文涉及的渐近符号总结如下。

1) 函数 $f(n)$ 用 $\mathcal{O}\big(g(n)\big)$ 表示，则 $f(n)$ 关于 n 的渐近阶数小于或等于函数 $g(n)$，即存在常数 $m,n_0>0$，使对于任意的 $n\geqslant n_0$，满足 $0\leqslant f(n)\leqslant mg(n)$。尽管 $\mathcal{O}(\cdot)$ 符号的定义中并不要求 $f(n)$ 与 $g(n)$ 同阶，但其在隐蔽通信领域中用于描述同阶函数[12]。

2) 函数 $f(n)$ 用 $o\big(g(n)\big)$ 表示，则 $f(n)$ 关于 n 的渐近阶数小于函数 $g(n)$，即对于任意常数 $m>0$，存在常数 $n_0>0$，使对于任意的 $n\geqslant n_0$，满足 $0\leqslant f(n)<mg(n)$。该定义隐含 $\lim\limits_{n\to\infty}\dfrac{g(n)}{f(n)}\to\infty$。尽管 $o(\cdot)$ 符号的定义中只要求 $f(n)$ 的阶数小于 $g(n)$，但为了描述容量界，该符号在隐蔽通信领域中用于描述不可达到的阶数上确界，例如若 n 个符号可传输的最大信息量为 $\mathrm{o}(n)$ bit，则信息量关于 n 的渐近阶数可无限接近 $g(n)=n$ 的阶数，但无法达到或超过该阶数。

3) 函数 $f(n)$ 用 $\omega\big(g(n)\big)$ 表示，则 $f(n)$ 关于 n 的渐近阶数大于 $g(n)$，即对于任意常数 $m>0$，存在常数 $n_0>0$，使对于任意的 $n\geqslant n_0$，满足 $0\leqslant mg(n)<f(n)$。该定义隐含 $\lim\limits_{n\to\infty}\dfrac{f(n)}{g(n)}\to\infty$。

2 无线隐蔽通信容量限

本节依据 n 个符号可传输的信息量为 $\mathcal{O}(\sqrt{n})$ 或 $\mathcal{O}(n)$ bit，分均方根速率和非零正速率两部分介绍不同场景下无线隐蔽通信的容量限。本节介绍的结论不依赖于 Alice 和 Bob 具体的通信方案，而是当 Willie 采用最优检测时，在隐蔽约束下能够达到的无差错传输速率极限。

2.1 均方根速率

Bash 等[12]的开创性工作指出，如果 Alice 与 Bob 提前共享大小为 $\mathcal{O}(\sqrt{n}\mathrm{lb}n)$ bit 的码本，码本构造方法为 Willie 所知但内容不为 Willie 所知，仅依

靠瞬时噪声不确定性，Alice 可以在加性白高斯噪声（AWGN, additive white Gaussian noise）信道中基于 n 个符号向 Bob 隐蔽且无差错地传输 $\mathcal{O}(\sqrt{n})$ bit。这里，隐蔽定义为对于给定的隐蔽容限 $\delta>0$，满足 $\Pr(\mathcal{D}_1|\mathcal{H}_0)+\Pr(\mathcal{D}_0|\mathcal{H}_1)>(1-\delta)$。反之，文献[12]指出，如果试图传输 $\omega(\sqrt{n})$ bit，不可能同时实现无差错接收和隐蔽传输。该结论被称为均方根定律（SRL, squared root law）。后续在不同模型下证明均方根定律的适用性的工作大多遵循与该文献相同的证明框架，即构造一种 Alice 与 Bob 间的通信方案，使即使 Willie 采用最佳检测器，Alice 仍可无差错且隐蔽地传输 $\mathcal{O}(\sqrt{n})$ bit；再构造一种 Willie 的检测方案，使 Alice 在传输 $\omega(\sqrt{n})$ bit 时，隐蔽约束带来的功率约束必然导致 Bob 的接收误码率无法趋近于零。适用均方根定律的重要工作及其核心贡献总结如表 1 所示，本节将详细介绍这些工作。

文献[21]指出多输入多输出（MIMO, multiple-input multiple-output）AWGN 信道的隐蔽通信速率极限可表示为每 n 个符号传输 $\mathcal{O}\left(\min\{N_\mathrm{a},N_\mathrm{b}\}\sqrt{\frac{n}{\min\{N_\mathrm{a},N_\mathrm{w}\}}}\right)$ bit，其中，N_a、N_b 和 N_w 分别是 Alice、Bob 和 Willie 的天线数，可见 MIMO 系统仍服从均方根定律，但增加通信双方天线数可线性增加隐蔽通信速率极限。

基于离散无记忆信道（DMC, discrete memoryless channel）进行分析，特别是基于二元输入 DMC 和二元对称信道（BSC, binary symmetric channel），更易于揭示更深层次的规律，为连续信道的分析指明方向。文献[22]考察了 Alice-Willie 信道错误概率大于 Alice-Bob 信道的 BSC，揭示了在此种情况下不需要密钥就可以隐蔽且无差错地传输 $\mathcal{O}(\sqrt{n})$ bit，并给出了 $\sqrt{n}$ bit 前的常数的最大可达值，该值被称为一阶隐蔽通信容量。文献[22]开启了 2 个重要研究方向，一是刻画密钥量，二是刻画一阶隐蔽通信容量。

关于密钥量的刻画，文献[23]证明了实现 DMC 最大隐蔽信息量 $\mathcal{O}(\sqrt{n})$ 所需的最少密钥量可表示为 $\mathcal{O}(\sqrt{n})$，且如果 Alice-Bob 信道优于 Alice-Willie 信道则不需要密钥，并将上述结论推广至 AWGN 信道。此处信道更优的定义为，有通信行为和无通信行为对应的接收信号概率分布之间的相对熵更大。对应于 AWGN 信道中，该定义表示接收信噪比越小，则噪声越能主导接收信号的概率分布，即有通信信号时接收的概率分布与无通信信号时的概率分布的相对熵越小，因此可推断若 Bob 的接收信噪比高于 Willie，则不需要密钥。

关于一阶隐蔽通信容量的刻画，文献[24]推导了相对熵约束下 DMC 和 AWGN 信道的一阶隐蔽容量。针对瑞利快衰落信道，文献[25]在相对熵约束下推导了一阶隐蔽容量和所需密钥量，由于 Bob 和

表 1　　**适用均方根定律的重要工作及其核心贡献总结**

文献	核心贡献	信道模型
文献[12]	均方根定律	AWGN
文献[21]	天线数对隐蔽通信速率极限的影响	MIMO AWGN
文献[22]	不需要密钥，一阶隐蔽容量	BSC（Bob 信道优于 Willie）
文献[23]	最小所需密钥量关于符号数的阶数	DMC/AWGN
文献[24]	相对熵约束下的一阶隐蔽容量	DMC/AWGN
文献[25]	相对熵约束下的一阶隐蔽容量	瑞利快衰落
文献[26]	相对熵约束下的一阶隐蔽密钥生成容量	DMC
文献[27]	不同隐蔽指标约束下的一阶、二阶隐蔽容量	二元输入 DMC
文献[28]	一阶容量可达的低复杂度编码方案（多进制）	二元输入 DMC
文献[29]	一阶容量可达的低复杂度编码方案（二进制）	二元输入 DMC
文献[30]	一阶容量可达的低复杂度编码方案	AWGN
文献[31]	相对熵约束下的一阶容量域	二元输入 DMC 多址接入信道
文献[32]	相对熵约束下的一阶容量域	DMC/AWGN 广播信道
文献[33]	相对熵约束下的一阶容量域	DMC/AWGN 多收发对互扰信道

Willie 所接收到的每一个符号都受到相位服从独立均匀分布的信道系数的影响，他们仅依靠接收信号幅度信息进行译码或检测。文献[26]则在相对熵约束下考察了 DMC 的隐蔽密钥生成容量，证明了在 Bob 可以在另一个公开无差错信道上广播信息的条件下，一阶隐蔽密钥生成容量等于一阶隐蔽通信容量。

值得注意的是，由于不同隐蔽性能指标并不等价，在不同指标约束下得到的容量表达式往往不同。为此，文献[27]在错误检测概率、总变分距离、相对熵 3 种隐蔽性能指标约束下，推导二元输入 DMC 的一阶、二阶隐蔽容量，并分别给出了所需密钥量。具体地，3 种约束下的最优渐近隐蔽信息量均可写为 $an^{\frac{1}{2}}-b(\epsilon)n^{\frac{1}{4}}+\mathcal{O}(\ln n)$ 的形式，其中，参数 $a>0$，且 a 与隐蔽容限、Alice 通信时与不通信时 Bob 接收符号的概率分布差异、Alice 通信时与不通信时 Willie 接收符号的概率分布差异有关，而参数 $b(\epsilon)>0$ 除与上述因素有关，还随着最大误码容限 ϵ 的降低而增大。

如何以更低复杂度的编码方式达到一阶隐蔽容量对于推动隐蔽通信走向实用十分重要，这一问题在首次推导容量的文献中往往被忽略。为此，文献[28]针对二元输入 DMC，提出一种以脉冲位置调制（PPM, pulse-position modulation）为内码，以随机编码为外码的低复杂度编码方式。其中，为达到相对熵约束下的一阶隐蔽容量，PPM 符号的阶数需随普通符号数 n 的增加而增加，在 PPM 符号基础上的随机编码是非二进制编码。文献[29]为进一步降低复杂度，以多级编码为外码替代随机编码，把在 PPM 符号上的编码转化为在多个二进制输入信道上的编码，并允许进一步采用极化码等低复杂度二进制编码方案，同样能够达到一阶隐蔽容量。文献[30]将上述思路拓展到 AWGN 信道中，提出了基于 PPM 和多级编码的可以达到 AWGN 信道一阶隐蔽容量的低复杂度编码方案，首次基于稀疏非零码元而非基于随着 n 的增加而接近于零的功率实现 AWGN 信道的一阶隐蔽容量。

以上研究针对点对点通信，除此之外，均方根定律还广泛适用于多对一、一对多、多对多通信。文献[31]考虑二元输入 DMC 多址接入信道，其中多个发射机同时向接收机 Bob 隐蔽传输信息，推导了整个系统在相对熵约束下的一阶容量域和各发射机需要和 Bob 共享的密钥量，其结果表明各发射机一阶容量值此消彼长，且如果某一发射机到 Bob 的信道相对于该发射机到 Willie 的信道更优，则该发射机不需要与 Bob 共享密钥，此处信道更优的定义为，仅存在该发射机时，有通信行为和无通信行为对应的接收信号概率分布之间的相对熵更大。文献[32]考虑广播信道，推导了单 Alice 多 Bob AWGN 广播信道和满足一定条件的单 Alice 双 Bob DMC 广播信道在相对熵约束下的一阶容量域，其结果表明一阶容量域的边界为各链路单独存在时的容量的凸组合，其上每一个点都可以基于时分多址分配时间资源来达到。需要注意的是，在无隐蔽约束的一般广播信道中，时分多址通常不是最优的。文献[33]考虑多个 Alice-Bob 对，每一个 Bob 仅需要接收其对应的 Alice 的信息，对于有多个非合作 Willie 的二元输入 DMC，推导了相对熵约束下的一阶容量域和达到容量域所要求的各 Alice-Bob 对共享的密钥量，结果表明，各 Alice-Bob 对的容量此消彼长，如果某一 Alice-Bob 对的信道在相对熵意义上优于该 Alice 到所有 Willie 的信道中最优的那个，则该 Alice-Bob 对不需要密钥。对于一般的 DMC 和 AWGN 信道，假设仅存在单个 Willie，该文献也推导了一阶容量域，但没有分析密钥量。在该文献的所有可达性证明中，各 Bob 仅需将其他 Alice 的干扰当作噪声处理，即其最优接收策略如同没有其他 Alice 存在。这是因为隐蔽约束迫使各 Alice 采用极少非零符号或极小发射功率，从而互干扰的影响相对于噪声影响可以忽略。

2.2 非零正速率

将 $\mathcal{O}(\sqrt{n})$ bit 平均到 n 个符号上，可以得到均方根定律对应的隐蔽通信速率实际上渐近为 0。许多研究进一步探索利用 Willie 处更多的不确定性实现非零正速率（简称正速率），即每 n 个符号 $\mathcal{O}(n)$ bit。实现正速率的不同途径如表 2 所示。

表 2 实现正速率的不同途径

文献	正速率来源	信道模型
文献[34]	Willie 对噪声功率的不确定性	AWGN
文献[35]	Willie 对干扰功率的不确定性	AWGN/准静态瑞利衰落信道
文献[18]	Willie 对干扰功率的不确定性	AWGN（连续时间）
文献[36]	干扰源充分逼近 Willie	AWGN
文献[37]	Alice 具有信道信息优势/Alice 已知干扰序列	DMC/AWGN
文献[38]	Willie 对传输时间的不确定性	AWGN
文献[39]	掌握关于 Willie 的信道信息且有零空间/充分大的发射天线数	MIMO AWGN

由于温度变化等原因，无法避免噪声功率的不确定性，文献[34]假设 Willie 仅掌握噪声功率的统计分布，但不知检测过程中噪声功率的准确值，证明了 AWGN 信道中噪声功率不确定性能够带来正速率。该文献分别考虑噪声功率服从以 dB 为单位的均匀分布和正态分布 2 种情况，求解符号数 n 充分大时，隐蔽约束所导致的 Alice 平均发射功率的最大允许值，所得结果在 2 种分布下均为与 n 无关的常数，因此能够实现与 n 无关的非零隐蔽通信速率，其研究结果还表明，隐蔽约束要求越严苛（δ 接近于 0）极限速率值越接近于 0。

自然存在的噪声功率不确定性有限。文献[35]考虑干扰不确定性，证明了 AWGN 和准静态瑞利衰落信道 2 种情况下，额外布设的干扰机能够带来正速率。该文献并未要求干扰机知道 Alice 何时通信，对于 AWGN 信道，通过设计干扰机在不同的 Alice 可能通信的时隙内发射不同功率的高斯信号，达到了等同于不确定的噪声功率的效果。对于准静态瑞利衰落信道，设计干扰机采用固定功率干扰，利用 Willie 对信道系数的不确定性造成不确定的干扰功率，也证明了 Alice 可以采用常数功率。其中对于准静态瑞利衰落信道这一情况，由于该文献假设一次传输时间内对应的准静态衰落块的个数是有限的，无论采用多小的传输速率，总有一定概率因为信道增益过小导致误码，所以在该情况下得到了 n 个符号能无差错传输 $o(n)$ bit 而非 $\mathcal{O}(n)$ bit 的结论。

文献[18]揭示了文献[35]的成果不能推广至连续时间模型。具体地，在文献[35]所考虑的离散时间模型下，采用其所构造的通信策略与干扰策略，功率计被证明是 Willie 的最优检测器，即使 Willie 采用最优检测仍能实现正速率隐蔽通信。考虑连续时间模型，文献[18]利用 Alice 和干扰机所发信号到达 Willie 的时间差，构造了干扰消除级联功率计的 Willie 检测策略，使原通信策略与干扰策略所能达到的隐蔽通信速率极限为均方根速率。不过，文献[18]重新构造了一种通信与干扰策略，其核心思想是引入传输时间与干扰时间的随机性，从而打破 Willie 消除干扰的可能，新策略被证明在 Willie 采用最优检测时仍能达到正速率，即每 T s 传输 $\mathcal{O}(WT)$ bit，其中 $T\to\infty$，带宽 W 是有限值。

文献[36]考虑 AWGN 信道中服从密度为 m 的泊松点过程（PPP, Poisson point process）的大量干扰节点对隐蔽通信速率的增益。假设单位面积方形内有多个位置服从独立均匀分布的 Willie 进行联合检测，Alice 和 Bob 分别位于方形对边的中点，该文献提出的策略为对于每一个 Willie，开启距其最近的干扰节点，发射固定功率人工噪声。区别于文献[18,35]，由于假设 Willie 和干扰节点是互知位置的，Willie 并没有对干扰功率的不确定性。然而，文献[36]证明了在路径损耗系数 $\alpha=2$ 且 Willie 个数 $N_{\mathrm{w}}>1$ 时，n 个符号可传输的隐蔽信息量为 $\mathcal{O}\left(\min\left\{m\sqrt{n}\left(N_{\mathrm{w}}\ln N_{\mathrm{w}}\right)^{-2},n\right\}\right)$ bit，对于其他情况，可传输 $\mathcal{O}\left(\min\left\{m^{\frac{\alpha}{2}}\sqrt{n}N_{\mathrm{w}}^{-\alpha},n\right\}\right)$ bit。由文献[36]可知，如果干扰源充分逼近 Willie（密度 m 足够大，并开启距 Willie 最近的干扰机），是可以仅依靠其对瞬时噪声与干扰的不确定性突破均方根定律的。

文献[37]揭示了 Alice 利用信道信息优势实现正速率的可能性。具体地，该文献考察了信道状态（转移概率）逐符号变化的 DMC，Bob 和 Willie 均不掌握信道在某个符号周期中的具体状态，该文献分别针对 Alice 实时掌握最新信道状态而做出因果反应和提前掌握整个传输过程中的信道状态而做出非因果反应 2 种情况，推导了相对熵约束下隐蔽容量的上下界，证明了依赖上述信道信息优势，在一些情况下可以实现正速率。进一步，该工作考察恒定功率人工噪声干扰下的 AWGN 信道，指出若 Alice 实时或提前掌握干扰序列，则正速率可达，并给出了相应需要的密钥量，还揭示了如果 Willie 噪声功率大于 Bob 则不需要密钥。由文献[37]可知，若 Alice 已知干扰序列，则不需要 Willie 对干扰功率有不确定性也能实现正速率。

上述研究假设 Willie 准确知道 Alice（如果通信）通信时间的起始与结束时刻，而实际中 Alice 和 Bob 可能预先安排了不为 Willie 所知的通信时段，该通信时段相对于总的可能通信的时间可能很短。针对上述特点，文献[38]证明了传输时间不确定性可以提供正速率。具体地，假设实际通信时隙为 $T(n)$ 个时隙中的一个，其中 $T(n)$ 随每个时隙可传输的符号数 n 的增加而增加，则仅利用所选中的时隙可隐蔽且可靠地传输 $\mathcal{O}\left(\min\left\{\sqrt{n\ln T(n)},n\right\}\right)$ bit。且如果 $T(n)$ 随 n 的增加速度小于文献中给出的值，则 Alice 和 Bob 不需要事先约定选择哪个时隙，因为此时 Bob 能够无差

错地将没有信息传输的情况译码为空码字。反之，仅需要在 Willie 处采用功率检测计，Alice 就无法隐蔽且可靠地传输 $\omega(\sqrt{n\ln T(n)})$ bit 。需要注意的是，不需要证明无法传输 $\omega(n)$ bit ，因为传输 $\omega(n)$ bit 要求有无穷大的功率。

除增加和利用不确定性外，文献[39]指出在 AWGN 信道中利用发射天线阵能够实现正速率的 2 种情况。在有限发射天线数下，达到正速率需要 Alice 掌握 Willie 信道信息并有零空间可利用。如果使用充分多的发射天线，不需要 Willie 的信道信息也能实现正速率，且随着发射天线数的增加，隐蔽通信容量将越来越接近无隐蔽约束的普通 MIMO 通信容量，这得益于大规模发射天线的窄波束。

3 无线隐蔽通信实现技术

本节依据不同应用场景对无线隐蔽通信实现技术研究进行综述，这些研究工作在假设检验理论和信息论的支撑下进行性能分析与方案优化，为隐蔽通信工程实践提供了坚实的理论依据。

3.1 有限码长隐蔽通信

一些隐蔽通信场景要求低传输时延。前述隐蔽通信容量限的研究均假设一次传输所使用的符号数足够多（无限码长），该假设为推导提供了便利，但不适用于时延受限（有限码长）系统。

文献[40]首次考虑有限码长隐蔽通信，针对 AWGN 信道，该文献假设每次传输使用至多 N 个服从功率为 P 的独立复高斯分布的符号，一次传输过程中 P 不变，Willie 仅掌握 P 的统计分布。考虑 P 取自固定值、均匀分布、离散分布 3 种情况，联合优化功率值和码长，最大化隐蔽吞吐量。其重要结论为，虽然使用更多的符号更易暴露，但使用全部 N 个符号并结合功率控制得到的隐蔽吞吐量是最高的。此外，功率分布随机性越大吞吐量越高，但取值不多的离散分布足以接近均匀分布的性能。

值得注意的是，使用尽可能多的符号数不总是最优的。文献[41]揭示了在准静态瑞利衰落信道中，使用允许的最小符号数可能是最优的。具体地，假设 Alice 采用高斯码本，文献[41]首先证明了在高错误检测概率区，Willie 掌握 Alice-Willie 的瞬时信道信息的准确度对其最优检测性能没有影响，因此该文献在随后的工作中合理保守地假设 Willie 能够完美估计信道信息，而 Bob 有信道估计误差。给定传输速率，在最大码长、最小码长、最大功率、Willie 错误检测概率等约束下，以码长和发射功率为优化变量最大化吞吐量，给出了数值最优和低复杂度理论解，二者接近。其重要结论在于，至少从该文献考虑的参数来看，选用允许的最小码长是最优的，其原因在于 AWGN 信道中 Bob 接收的不可靠性来自噪声，使用更多的符号可以减小噪声影响，而在准静态瑞利衰落信道中不可靠性还来自信道，并不能通过更多的符号数消除其影响，当信道衰落影响大于噪声时，使用更少的符号数有益于隐蔽。

更多关于有限码长隐蔽通信的工作将在后文结合其他实现技术介绍。

3.2 多天线发射

前述隐蔽通信容量限相关工作[21,39]已从理论上揭示了多天线对隐蔽通信的增益。在发射机对体积和成本不敏感的隐蔽通信场景中，可利用多天线的波束成形能力集中信号能量，减少能量泄露。

文献[42]考察了有限码长多输入单输出（MISO, multiple-input single-output）隐蔽通信系统在相对熵约束下的波束成形和功率控制策略，最大化接收信噪比。假设 Alice 采用高斯码本且掌握关于 Bob 的完美信道信息，其研究结果表明：对于完美掌握关于 Willie 信道信息的情况，可以实现零相对熵，也可以允许部分信号泄露以换取更高的 Bob 处的信噪比；对于掌握关于 Willie 的不准确信道信息的情况，若超过某发射功率值则无论采用何种波束成形策略，都不可能满足隐蔽约束；对于仅掌握 Willie 统计信道信息的情况，证明了 Alice-Willie MISO 信道系数统计不相关时的最优波束成形策略是最大比传输。

面向噪声功率不确定性掩护下的无限码长 MISO 隐蔽通信系统，文献[43]考察了在瑞利衰落信道中的吞吐量最大化问题，其中假设 Alice 依靠 Bob 发送的导频掌握 Alice-Bob 瞬时信道信息，但仅掌握 Alice-Willie 统计信道信息，因而直接采用最大比发送波束成形，而优化变量包括发射功率和传输速率。文献[44]则针对 Willie 位置未知的情形，面向三维莱斯信道提出了隐蔽区域的概念，具体定义为满足隐蔽约束、中断概率约束、功率约束前提下的最大吞吐量大于给定要求的 Willie 位置的集合，该文献通过数值手段直观揭示了各系统参数对隐蔽区域的空间分布的影响。上述文献考虑多天线对隐蔽性能的增强，文献[45]则揭示了 Willie 天线数的增加将大幅降低隐蔽吞吐量。

3.3　全双工接收

对于接收机距离潜在监察者较近且接收机不需要隐蔽的场景，采用全双工架构释放干扰可以有效提高监察者的干扰不确定性，且得益于自干扰消除技术的发展[46]，相较于额外布设干扰节点而言其对接收性能的损害更小。

考虑瑞利衰落信道和无限码长，文献[47]假设 Willie 掌握完美信道信息，令 Alice 码本与全双工 Bob 的干扰信号都服从高斯分布，在一个时隙内干扰功率不变但功率值随机取自均匀分布，达到类似于文献[35]布设额外干扰节点带来干扰功率不确定性的效果。值得一提的是，不同于以往假设 Alice 在某时隙传输的先验概率为某一固定值的做法，该文献将 Alice 传输的先验概率与 Bob 干扰功率的取值范围一起作为优化变量，在给定的有效传输速率要求下最大化 Willie 的错误检测概率，揭示了将先验概率作为可控量对隐蔽性能有增益。

同样令 Alice 码本和全双工 Bob 的干扰信号都服从高斯分布，文献[48]考虑 AWGN 信道和有限码长，其中 Bob 的干扰功率恒定。以相对熵为隐蔽约束，在给定传输速率和码字长度下优化 Alice 和 Bob 的发射功率，最大化吞吐量，证明了如果 Bob 的噪声功率大于自干扰系数乘以 Willie 的噪声功率，最优 Bob 干扰功率为最大允许值，否则为 0。需要注意的是，如果其他系统设定不变，将有限码长改为无限码长，则因为干扰功率固定，Willie 可以相应地调整检测门限，不论干扰功率多大对检测性能都没有影响。

3.4　频谱共享网络中的隐蔽通信

如果环境中存在其他发射机在相同频段上的通信行为，即使这些发射机无意帮助 Alice，也能够提高 Willie 对干扰的不确定性。利用这一特点，可以在频谱复用度高的网络（如物联网、认知网络）中为隐私设备提供不需要额外干扰源的低功耗隐蔽通信方案。

文献[49]将外部随机通信行为的发生建模为 PPP，其关键假设包括：所有发射机采用高斯码本，除 Alice 外所有发射机采用相同的发射功率，且在 Alice 可能传输的时隙中保持发射状态不变。该文献分别考虑无衰落和瑞利衰落下的隐蔽吞吐量最大化问题，揭示了以下规律：①无噪声时 PPP 密度和外部发射机功率对最优吞吐量没有影响，即干扰的增加对 Bob 和 Willie 的影响刚好抵消；②有噪声时增大 PPP 密度和外部发射机功率可以提高吞吐量；③进一步可以推论，增大 PPP 密度和外部发射机功率到一定程度后将不再有影响，因为此时干扰远大于噪声。

文献[50]研究采用集中式或分布式多天线的 Alice 在 PPP 网络干扰掩护下的隐蔽通信性能。具体地，考虑准静态瑞利衰落信道，有多个地理位置不为 Alice 所知的单天线 Willie，Willie 仅掌握 Alice 位置并采用功率计执行独立检测，Alice 采用最大比传输或分布式波束成形策略。以多个 Willie 中至少有一个的最优判决门限在随机信道、随机干扰源位置与数量、随机 Willie 位置的具体实现下能够正确判决的概率为隐蔽约束，最大化吞吐量，优化变量为 Alice 的发射功率和传输速率。由于表达式过于复杂，最优解只能通过数值搜索得到，数值结果表明集中式多天线性能优于分布式。

上述两项研究中，Alice 与其他发射机不具有同等地位，文献[51]则考察了等功率高斯码本 PPP 分布发射机中任意一个发射机的隐蔽容量。具体地，该文献首先考虑瑞利衰落信道中各发射机采用全向天线的情况，此时 PPP 分布和信道衰落给 Willie 带来了严重的干扰功率不确定性，在假定 Willie 采用功率计和以相对熵作为隐蔽约束的前提下，证明了如果 Alice 和 Willie 的距离满足 $\omega\left(n^{\frac{1}{2\alpha}}\right)$，则不论发射功率多大，一定能实现隐蔽通信，其中 α 为路径损耗系数。由于表达式过于复杂，该文献仅给出了当 $\alpha=4$ 时，隐蔽信息量可表示为 $\mathcal{O}(\mathrm{lb}\sqrt{n})$。随后，该文献考虑太赫兹 AWGN 信道，各发射机采用定向天线，针对 Willie 位于 Alice 和 Bob 之间的极端情况，通过数值结果说明了通过镜面反射或漫散射绕开 Willie 是可能实现隐蔽通信的。

上述研究中，Alice 与其他发射机无主次之分。文献[52]则考察了基站−用户通信掩护下的终端直通（D2D, device-to-device）通信隐蔽吞吐量最大化问题，其中，D2D 通信复用上行频谱，多天线全双工基站在接收上行信号的同时在上行频段发射人工噪声以掩护 D2D 通信。文献[53]考察认知网络中次用户的隐蔽通信，不同于上述文献所采用的传统优化框架，该文献以生成对抗网络（GAN, generative adversarial network）为工具优化主用户与次用户的功率，对抗 Willie 所可能采取的门限策略。

3.5 无人机参与的隐蔽通信

无人机具有高机动性和视距空地、空空信道优势，在隐蔽通信系统中作为发射机、接收机、监察者、转发节点或干扰节点均可根据需要进行机动，调整信道优劣[54]。

由于空地、空空信道通常有视距分量，以无人机作为发射机隐蔽难度大，合理设计发射功率、飞行轨迹尤为重要。文献[55]研究噪声功率不确定性掩护下的无人机空地视距隐蔽通信，其中假设合理的时间离散化处理能够保证每个时隙内无人机位置近乎不变，且每个时隙能够承载充分大的符号数，无人机在固定高度二维移动，对 Willie 和 Bob 的位置估计存在高斯分布误差。文献[55]在关于位置误差的平均错误检测概率和中断概率、无人机起点终点位置和速度、峰值和平均发射功率等约束下，优化飞行轨迹和每个离散位置的发射功率与传输速率，最大化平均信息传输速率。

文献[56]针对无人机抵近以 Willie 为中心的区域执行任务，并向 Bob 回传信息的场景，合理假设无人机位于 Bob 和 Willie 连线上方的以 Willie 为中心的二维扇形区域。在相对熵隐蔽约束、扇形区域约束、最大发射功率约束下，优化无人机悬停位置和发射功率，最大化接收信噪比。文献[56]将可悬停区域划分成多个子区域，每个子区域内的最优解更易于找到。文献[57]则从监察者角度研究空中无人机通信行为的检测问题，提出基于波束扫描，结合无人机位于扫描区时的接收与位于其他区域时的接收进行联合判决，以最小化错误检测概率为目标，优化在二维平面上的扇形扫描区数量，其数值结果表明扫描区的划分不应过多或过少。

在上述工作中无人机作为发射机。文献[58]则考察多用户地空隐蔽通信，其中每个时隙只有一个用户进行上行传输，而其他用户均作为 Willie，全双工无人机 Bob 释放均匀分布功率干扰提供隐蔽。该文献在隐蔽约束下联合优化无人机在固定高度上的二维轨迹、最大干扰功率、用户时隙分配，最大化最小用户速率，提出利用惩罚连续凸近似的方法处理由时隙分配二进制约束构成的混合整数非凸优化问题。文献[59]则考虑位于地面的 Alice 和 Bob 距离过远而需要无人机中继的情况，其中 Willie 也是无人机，对地面 Alice 和无人机中继的通信行为进行检测。该文献以端到端吞吐量最大化为优化目标，在隐蔽约束下联合优化 Alice、无人机中继的发射功率及分配给 Alice 和无人机中继的有限符号数。

3.6 多跳中继

远距通信需要较大的发射功率，而经由多个中继进行多跳转发能够有效降低所需发射功率，从而提高隐蔽性。

文献[60]研究 AWGN 信道中以大量备选转发节点为基础的多跳隐蔽路由问题，其中多个 Willie 对全通信过程进行侦听后进行联合检测。分别考察各转发节点采用与 Alice 相同的秘密高斯码本和采用独立秘密高斯码本 2 种情况，在相对熵隐蔽约束下分别以最大化吞吐量和最小化通信时延为目标提出路径和各跳功率的联合优化算法。其结果表明，多跳路由相较于单跳能够大幅提高性能，采用独立码本相较于相同码本能够大幅提高性能。值得注意的是，由于长密钥可基于短密钥通过密码算法生成，因此采用独立码本带来的开销并不会太大。

文献[61]考察无人机监视下的地面多跳译码转发隐蔽通信。注意到，转发跳数越多，虽然可以采用越低的发射功率来同时保证隐蔽性和可靠性，但在相同时频资源上的有效传输时间越少。另一方面，大的发射功率能支撑大的通信速率，但距离无人机近的节点采用大功率容易暴露。因此该文献以转发跳数、各跳功率、传输速率为优化变量，在相对熵隐蔽约束和总功率约束下最大化吞吐量，提供了最优解的数值解法。

3.7 可重构智能表面增强的隐蔽通信

可重构智能表面（RIS, reconfigurable intelligent surface）是由一定数量的可编程反射单元组成的厚度微小但具有一定面积的表面，可灵活改变反射信号的电磁特性，也被称为智能反射表面（IRS, intelligent reflecting surface）[62]。RIS 打破了无线通信领域中无线信道环境不受控制、只优化发射机和接收机的传统，可以有效增强 Bob 接收信号质量并抵消泄露至窃听者或监察者处的信号，为提高无线通信安全性和隐蔽性均提供了全新的技术手段[63-64]。由于 RIS 具有易于布置、低成本和低功耗的突出优势，特别适用于辅助物联网中隐私设备的隐蔽通信。

文献[65]考虑 RIS 辅助的单输入单输出无限码长隐蔽通信，由于未知 Willie 的瞬时信道信息，RIS 仅用于增强 Bob 接收，噪声功率不确定性被用于提高隐蔽性。该文献在瑞利衰落信道下以满足 Willie 错误检测概率约束为前提，联合优化 Alice 的发射功率和 RIS 反射系数的幅度和相位，最小化中断概

率。其数值结果验证了 RIS 的能量集中能力可以大幅降低隐蔽约束下的中断概率。对于同样的场景，文献[66]考虑 Alice 传输的先验概率对于遍历容量的影响，联合优化先验概率、Alice 的发射功率及 RIS 的反射相位，其数值结果表明优化传输先验概率相较于通常研究中将其固定为 0.5 的做法能够有效提升容量。文献[67]则并不假设 Willie 对噪声功率有不确定性，针对有限码长情况，分别对掌握关于 Willie 的完美信道信息和统计信道信息 2 种情况最大化隐蔽容量，证明了当掌握完美信道信息且 Alice-RIS-Willie 信道总增益大于 Alice-Willie 信道增益时，Willie 处的接收信号可以被完全抵消。上述工作均说明了即使 Alice 和 RIS 仅掌握关于 Willie 的统计信道信息，RIS 仍能提供较大隐蔽性能增益，需注意这是在 Willie 和 Bob 的信道服从独立瑞利分布情况下得出的结论，此时 RIS 到达 Willie 的信号相位随机叠加，而 RIS 到达 Bob 的信号可以同相叠加，因此这一性能增益将随 Bob 和 Willie 信道相关性提高而减小。

文献[68]考虑 RIS 辅助的 MISO 通信，分别针对掌握关于 Willie 的完美信道信息、不准确信道信息、统计信道信息 3 种情况，联合优化发射波束成形和 RIS 的反射相位，在噪声功率不确定性的掩护下优化隐蔽容量。其数值结果表明，使用 RIS 并不总是提高隐蔽容量，例如 Willie 靠近 RIS 时可能反而降低隐蔽容量。同样针对 MISO 场景，文献[69]考虑 Alice 与 Bob 之间无直射路径而必须经由 RIS 完成通信的情形，在全双工 Bob 所发干扰信号的掩护下，以中断概率和错误检测概率为约束最大化传输速率，所提算法可直接推广至 Willie 具有多天线的情况。文献[70]首次考虑 RIS 辅助的 MIMO 通信，其中 Willie 也配有多天线，假设掌握关于 Willie 的完美信道信息，在噪声功率不确定性的掩护下，联合优化发射相关矩阵和 RIS 反射系数，求解隐蔽容量最大化问题。

4　潜在研究方向

4.1　非理想条件的影响

如前文所述，文献[18]考虑不同来源信号到达的时间差，揭示了基于离散时间模型得到的结论不一定适用于连续时间模型，前者隐含了不同来源信号的符号时间完全对齐这一理想条件。目前绝大多数研究均基于离散时间模型，其中隐含的理想条件还包括精准的位定时、无码间串扰等，亟待开展更多工作探究这些理想条件不被满足时造成的影响。

进一步研究需审视更多现有模型中隐含的理想条件，并评估这些条件不被满足时造成的影响。例如，在隐蔽约束下 Alice 的发射功率需要足够低，而当接收功率过低时，锁相环受噪声影响无法正常工作，因而无法获取接收符号的绝对相位信息。此外，许多工作通过额外布设干扰节点提供掩护，过强的干扰也会影响锁相环对期望信号的捕获。然而，目前除专门研究非相干接收隐蔽通信的工作[25,71]外，默认绝对相位信息是可以获取的。

4.2　最优码本的设计与有限字符集的影响

由于高斯分布信号在 AWGN 信道中能够最大化互信息，且易于分析，因此被广泛采用，然而即使是对于 AWGN 信道，高斯码本在隐蔽通信中的最优性并未得到证明。文献[17]证明了在 AWGN 信道中，仅依靠瞬时噪声不确定性，高斯码本可以最小化 $D\left(\mathbb{P}_1 \| \mathbb{P}_0\right)$，因此在以 $D\left(\mathbb{P}_1 \| \mathbb{P}_0\right)$ 为隐蔽约束时高斯码本最优。在以 $D\left(\mathbb{P}_0 \| \mathbb{P}_1\right)$ 为隐蔽约束时，文献[17]在理论上证明了高斯非最优，并利用数值手段证明了更优码本的存在。此外，文献[17]还证明了在选用高斯码本时，$D\left(\mathbb{P}_0 \| \mathbb{P}_1\right) \leqslant D\left(\mathbb{P}_1 \| \mathbb{P}_0\right)$。综合上述结论可知，如果以 $\min\left\{D\left(\mathbb{P}_0 \| \mathbb{P}_1\right), D\left(\mathbb{P}_1 \| \mathbb{P}_0\right)\right\}$ 为约束，高斯码本不是最优的。不过，由于采用相对熵为约束与直接采用错误检测概率为约束仍有差距，尚不能确定高斯码本在 AWGN 信道中并非最优。因此，不同信道及不同不确定性掩护下的最优码本尚待研究。

即使高斯分布信号对于隐蔽通信而言是最优的，实际中连续的无穷多种符号取值是不可实现的，不可避免地需要讨论有限字符集对隐蔽通信的影响，可借鉴传统物理层安全领域针对有限字符集的研究工作[72]。

4.3　无源隐蔽通信

无源通信包括环境反向散射通信[73]和基于 RIS 的反射调制通信[74]，利用环境中已经载有信息的电磁波，通过改变反射信号幅度和相位实现信息调制，不需要产生本地载波，具有高频谱效率和高能量效率。由于无源通信方式复用外辐射源信号的频谱，且载有信息的反射信号与外辐射源自然产生的多径信号具有相似的特征，因此无

源通信方式本身就具有隐蔽性。文献[19]揭示了即使 Willie 知道 Alice 使用环境反向散射通信技术，通信过程仍可以是隐蔽且可靠的。具体地，在 AWGN 信道中，仅依靠瞬时噪声不确定性，传输速率服从均方根定律。

上述工作仅考虑了 AWGN 信道和瞬时噪声不确定性，在可达性证明中保守假设 Willie 可以完美恢复外辐射源信息并消除其干扰的影响，未充分利用外辐射源信号波动对无源寄生信号的遮盖，进一步的研究有望得到超越均方根定律的更好结果。

4.4 隐蔽信道估计

绝大多数现有工作隐含或显式地假设了 Bob 掌握 Alice-Bob 信道的信道信息，这要求 Alice 发出导频，或需要在对称信道中由 Alice 向 Bob 反馈信道估计结果，这将可能致使 Alice 的通信行为暴露。在现有工作基础上，需进一步研究如何获取信道信息而不被 Willie 发现，以及这一过程对隐蔽通信速率的影响。

少数工作提供了一些解决路径。其中，面向对称信道，文献[75]提出利用信道倒置功率控制（CIPC, channel inversion power control）绕开 Alice 发导频或反馈信道信息的要求。在 CIPC 中，假设 Bob 不需要隐蔽且可周期性发出导频信号，Alice 知道信道信息后调整所发符号的相位和幅度以保证接收星座固定，使 Bob 不需要知道信道信息即可将接收符号与星座点对应。上述工作中全双工 Bob 释放变功率干扰增加 Willie 的不确定性，文献[76]则基于噪声功率不确定性研究 CIPC 的性能。

另一种绕开信道估计的方法是 Alice 和 Bob 都不发送导频序列，Bob 和 Willie 采用非相干接收。相较于 CIPC，该方法不但同时适用于对称和非对称信道，还避免了 Bob 因发导频信号而暴露。前述揭示了瑞利快衰落信道下的一阶隐蔽容量的文献[25]正是基于非相干接收进行推导的。文献[71]进一步考察了由全双工 Bob 释放等幅干扰信号（此时 Bob 不再隐蔽）的非相干接收隐蔽通信系统，分别考虑瑞利快、慢衰落和干扰幅度固定、干扰幅度均匀分布但一次传输中幅度不变两两组合 4 种情况。对于快衰落固定干扰幅度情况，干扰的影响等同于高斯噪声的影响，因此退化为文献[25]中无干扰的情况，文献[71]证明了当且仅当 Bob 的自干扰功率小于其对 Willie 的干扰功率时，干扰对于相对熵约束下的一阶隐蔽容量是有增益的；对于快衰落均匀分布干扰幅度情况，证明了正速率可达；而对于慢衰落情况，假设 Willie 采用功率计，证明了不论 Alice 发射功率有多大，只要 Bob 的干扰功率足够大，总是可以实现正速率。

不同于上述工作，文献[77]通过导频信号的功率控制实现隐蔽信道估计，其中，Alice 需将有限符号数分配给导频和信息，而 Willie 基于信道估计和信息传输 2 个阶段的接收信号进行联合判决。该文献假设导频和信息均采用秘密高斯码本，Alice-Bob 信道为瑞利衰落信道，Alice-Willie 信道为 AWGN 信道和瑞利衰落信道 2 种情况，仅依靠瞬时噪声功率不确定性，在最小错误检测概率约束下，以导频功率、信息传输功率、符号分配为优化变量，最大化信道估计误差影响下的等效信噪比。主要结论是随着隐蔽要求提高，更多的符号应分配给导频。

此外，采用盲估计算法[78]直接从接收到的信息序列中获取信道信息也是一种规避发送导频序列的方法，可节约功率和带宽资源，但尚未见研究报道其在隐蔽通信中的应用。

4.5 序列变点检测

上述文献均是基于二元假设检验模型的，这要求 Willie 收集完所有可疑接收信号再做判决。然而，在许多情况下 Willie 并不掌握关于 Alice 通信时间的任何先验信息，而是持续地对信道进行侦收，并希望尽快发现 Alice 的通信行为，此时应采用序列变点检测（SCPD, sequential change-point detection）模型进行研究。具体而言，Alice 没有通信时，Willie 的接收信号仅包含噪声和干扰，Alice 开始通信后，Willie 接收信号的统计特性发生变化，并在 Alice 结束通信时恢复至原统计特性，SCPD 就是基于现有所有或部分接收信号，判定变化是否已发生。基于 SCPD 模型不再适用漏检概率和虚警概率评价指标，这是因为不论有无通信行为，只要时间足够长，有意义的 SCPD 检测器终究会告警。对应于二元假设检验模型中的漏检和虚警，在 SCPD 模型下 Willie 希望降低平均检测时延，并提高虚警所需平均运行时间，前者定义为序列统计特性发生变化到告警的时延的期望；后者定义为序列无变化，从开始侦听到虚警的时延的期望。

基于 SCPD 的隐蔽通信研究甚少，处于起步阶段[79-80]。文献[79]开创性地考虑了 SCPD 框架下的隐蔽通信，在 AWGN 信道、高斯码本假设和给定虚警所需平均运行时间下，分别考虑

Shewhart 、 CUSUM （ cumulative sum ）、 Shiryaev-Roberts 这 3 种经典 SCPD 算法，以 Willie 未能在 Alice 结束通信前发现其通信行为的概率大于给定值作为隐蔽约束，优化发射功率和符号数，最大化香农容量和符号数的乘积。上述隐蔽约束意味着 Willie 未及时发现 Alice 的通信行为为检测失败，适用于 Willie 需要对 Alice 的通信行为做出及时反应，如通过干扰阻止 Alice 通信的情景。文献[80]则将隐蔽约束定为让平均检测时延与虚警所需平均运行时间的比值大于一个小于但接近于 1 的值，该定义与二元假设检验框架中的漏检概率与虚警概率之和接近 1 的隐蔽约束有相同逻辑，即要求有、无通信行为 2 种情况下 Willie 的检测结果非常接近，换言之，检测器是无效的。具体地，同样考虑 AWGN 信道，文献[80]分别考虑了 FMAC（finite moving average chart）、Shewhart、CUSUM 这 3 种经典 SCPD 算法，在虚警所需平均运行时间趋于无穷的渐近区域，在新的隐蔽约束下推导了发射功率和符号数的界以及对应的信息容量界。

上述基于 SCPD 模型的隐蔽通信研究基于现有 SCPD 算法进行性能优化或分析。针对隐蔽通信，是否存在未被提出的更优 SCPD 算法，何种 SCPD 算法在何种场景下最优，SCPD 框架下的隐蔽通信极限是什么等问题亟待解决。

4.6　隐蔽通信速率提升

不论是基于二元假设检验模型还是基于 SCPD 模型考虑无线隐蔽通信问题，本质上都要求 Alice 没有通信时 Willie 接收信号的统计特征与 Alice 通信时相近，限制了 Alice 的发射功率，因而限制了通信速率。

未来的工作至少可从两方面着手提高隐蔽通信速率。一是挖掘理论分析中的余量，例如，尽管将相对熵指标作为隐蔽约束分析简单，但其作为错误检测概率指标的下界，导致隐蔽约束过于苛刻，限制了发射功率。此外，可以综合考虑 Willie 处的多种不确定性共同带来的容量增益，而非单一考虑某一种不确定性。二是提出新的实用隐蔽通信技术手段逼近容量限，正如信息论启发了各种性能优越的编码技术，基于二元假设检验模型或 SCPD 模型以及信息论的隐蔽通信理论，也具有启发出新的隐蔽通信技术手段的潜力，但目前未见研究报道。

5　结束语

基于二元假设检验模型或 SCPD 模型以及信息论的无线隐蔽通信研究顺应了未来大数据安全需求。本文梳理了无线隐蔽通信与相关概念的含义、区别及联系，介绍基本研究模型，划分具体模型类别，从均方根速率和非零正速率两方面综述无线隐蔽通信容量限揭示工作，分不同应用场景综述无线隐蔽通信系统性能分析与实现方案优化工作，并对潜在研究方向进行了展望，为本领域研究者全面了解研究现状，把握未来方向提供重要参考。

参考文献：

[1] 王安, 葛婧, 商宁, 等. 侧信道分析实用案例概述[J]. 密码学报, 2018, 5(4): 383-398.
WANG A, GE J, SHANG N, et al. Practical cases of side-channel analysis[J]. Journal of Cryptologic Research, 2018, 5(4): 383-398.

[2] LIU Y L, CHEN H H, WANG L M. Physical layer security for next generation wireless networks: theories, technologies, and challenges[J]. IEEE Communications Surveys & Tutorials, 2017, 19(1): 347-376.

[3] BASH B A, GOECKEL D, TOWSLEY D, et al. Hiding information in noise: fundamental limits of covert wireless communication[J]. IEEE Communications Magazine, 2015, 53(12): 26-31.

[4] ZANDER S, ARMITAGE G, BRANCH P. A survey of covert channels and countermeasures in computer network protocols[J]. IEEE Communications Surveys & Tutorials, 2007, 9(3): 44-57.

[5] DILLARD R A. Detectability of spread-spectrum signals[J]. IEEE Transactions on Aerospace and Electronic Systems, 1979, AES-15(4): 526-537.

[6] 牟青. 直接序列扩频信号的截获分析研究[D]. 成都: 电子科技大学, 2010.
MOU Q. A study on interception and analysis of direct-sequence spread-spectrum signals[D]. Chengdu: University of Electronic Science and Technology of China, 2010.

[7] HEIDARI-BATENI G, MCGILLEM C D. Chaotic sequences for spread spectrum: an alternative to PN-sequences[C]//Proceedings of IEEE International Conference on Selected Topics in Wireless Communications. Piscataway: IEEE Press, 1992 : 437-440.

[8] HEIDARI-BATENI G, MCGILLEM C D. A chaotic direct-sequence spread-spectrum communication system[J]. IEEE Transactions on Communications, 1994, 42(234): 1524-1527.

[9] SEDAGHATNEJAD S, FARHANG M. Detectability of chaotic direct-sequence spread-spectrum signals[J]. IEEE Wireless Communications Letters, 2015, 4(6): 589-592.

[10] 张晓彤. 时宽和波形基联合捷变的 LPD 通信波形设计与性能分析[D]. 哈尔滨: 哈尔滨工程大学, 2020.
ZHANG X T. Design and analysis of LPD communication waveforms based on joint-agility of time-width and waveform bases[D]. Harbin: Harbin Engineering University, 2020.

[11] DIAMANT R, LAMPE L. Low probability of detection for underwater acoustic communication: a review[J]. IEEE Access, 2018, 6:

19099-19112.

[12] 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.

[13] 赵华, 林钰达, 金梁, 等. 隐蔽无线通信综述[J]. 信息工程大学学报, 2020, 21(5): 520-525.
ZHAO H, LIN Y D, JIN L, et al. Covert wireless communication: a review[J]. Journal of Information Engineering University, 2020, 21(5): 520-525.

[14] 戴跃伟, 刘光杰, 曹鹏程, 等. 无线隐蔽通信研究综述[J]. 南京信息工程大学学报(自然科学版), 2020, 12(1): 45-56.
DAI Y W, LIU G J, CAO P C, et al. A survey of wireless covert communications[J]. Journal of Nanjing University of Information Science and Technology (Natural Science Edition), 2020, 12(1): 45-56.

[15] MAKHDOOM I, ABOLHASAN M, LIPMAN J. A comprehensive survey of covert communication techniques, limitations and future challenges[J]. Computers & Security, 2022, 120: 102784.

[16] LEHMANN E L, ROMANO J P. Testing statistical hypotheses[M]. Berlin: Springer, 2005.

[17] YAN S H, CONG Y R, HANLY S V, et al. Gaussian signalling for covert communications[J]. IEEE Transactions on Wireless Commun ications, 2019, 18(7): 3542-3553.

[18] LI K, SOBERS T V, TOWSLEY D, et al. Covert communication in continuous-time systems in the presence of a jammer[J]. IEEE Transactions on Wireless Communications, 2022, 21(7): 4883-4897.

[19] CHEN W Y, DING H Y, WANG S L, et al. On the limits of covert ambient backscatter communications[J]. IEEE Wireless Communications Letters, 2022, 11(2): 308-312.

[20] CORMEN T H, LEISERSON C E, RIVEST R L, et al. Introduction to algorithms[M]. Massachusetts: MIT Press, 2007.

[21] ABDELAZIZ A, KOKSAL C E. Fundamental limits of covert communication over MIMO AWGN channel[C]//Proceedings of IEEE Conference on Communications and Network Security. Piscataway: IEEE Press, 2017: 1-9.

[22] CHE P H, BAKSHI M, JAGGI S. Reliable deniable communication: hiding messages in noise[C]//Proceedings of 2013 IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2013: 2945-2949.

[23] BLOCH M R. Covert communication over noisy channels: a resolvability perspective[J]. IEEE Transactions on Information Theory, 2016, 62(5): 2334-2354.

[24] WANG L G, WORNELL G W, ZHENG L Z. Fundamental limits of communication with low probability of detection[J]. IEEE Transactions on Information Theory, 2016, 62(6): 3493-3503.

[25] TAHMASBI M, SAVARD A, BLOCH M R. Covert capacity of non-coherent Rayleigh-fading channels[J]. IEEE Transactions on Information Theory, 2020, 66(4): 1979-2005.

[26] TAHMASBI M, BLOCH M R. Covert secret key generation[C]//Proceedings of 2017 IEEE Conference on Communications and Network Security. Piscataway: IEEE Press, 2017: 540-544.

[27] TAHMASBI M, BLOCH M R. First- and second-order asymptotics in covert communication[J]. IEEE Transactions on Information Theory, 2019, 65(4): 2190-2212.

[28] BLOCH M R, GUHA S. Optimal covert communications using pulse-position modulation[C]//Proceedings of IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2017: 2825-2829.

[29] KADAMPOT I A, TAHMASBI M, BLOCH M R. Multilevel-coded pulse-position modulation for covert communications over binary-input discrete memoryless channels[J]. IEEE Transactions on Information Theory, 2020, 66(10): 6001-6023.

[30] KADAMPOT I A, TAHMASBI M, BLOCH M R. Codes for covert communication over additive white Gaussian noise channels[C]//Proceedings of IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2019: 977-981.

[31] ARUMUGAM K S K, BLOCH M R. Covert communication over a k-user multiple-access channel[J]. IEEE Transactions on Information Theory, 2019, 65(11): 7020-7044.

[32] TAN V Y F, LEE S H. Time-division is optimal for covert communication over some broadcast channels[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(5): 1377-1389.

[33] CHO K H, LEE S H. Treating interference as noise is optimal for covert communication over interference channels[C]//Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT). Piscataway: IEEE Press, 2020: 816-821.

[34] HE B, YAN S H, ZHOU X Y, et al. On covert communication with noise uncertainty[J]. IEEE Communications Letters, 2017, 21(4): 941-944.

[35] 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.

[36] SOLTANI R, GOECKEL D, TOWSLEY D, et al. Covert wireless communication with artificial noise generation[J]. IEEE Transactions on Wireless Communications, 2018, 17(11): 7252-7267.

[37] LEE S H, WANG L G, KHISTI A, et al. Covert communication with channel-state information at the transmitter[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(9): 2310-2319.

[38] BASH B A, GOECKEL D, TOWSLEY D. Covert communication gains from adversary's ignorance of transmission time[J]. IEEE Transactions on Wireless Communications, 2016, 15(12): 8394-8405.

[39] BENDARY A, ABDELAZIZ A, KOKSAL C E. Achieving positive covert capacity over MIMO AWGN channels[J]. IEEE Journal on Selected Areas in Information Theory, 2021, 2(1): 149-162.

[40] 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.

[41] 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.

[42] YU X C, LUO Y, CHEN W. Covert communication with beamforming over MISO channels in the finite blocklength regime[J]. Science China Information Sciences, 2021, 64(9): 183-197.

[43] 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[J]. 通信学报, 2020, 41(7): 49-58.
LIN Y D, JIN L, ZHOU Y, et al. Performance analysis of covert wireless communication based on beam forming with noise uncertainty[J]. Journal on Communications, 2020, 41(7): 49-58.

[44] 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[J]. 中国科学: 信息科学, 2021, 51(8): 1360-1374.
LIN Y D, JIN L, HUANG K Z, et al. Threat region development of

covert wireless communication based on 3D beamforming[J]. Scientia Sinica (Informationis), 2021, 51(8): 1360-1374.

[45] SHAHZAD K, ZHOU X Y, YAN S H. Covert wireless communication in presence of a multi-antenna adversary and delay constraints[J]. IEEE Transactions on Vehicular Technology, 2019, 68(12): 12432-12436.

[46] EVERETT E, SAHAI A, SABHARWAL A. Passive self-interference suppression for full-duplex infrastructure nodes[J]. IEEE Transactions on Wireless Communications, 2014, 13(2): 680-694.

[47] SHAHZAD K, ZHOU X Y, YAN S H, et al. Achieving covert wireless communications using a full-duplex receiver[J]. IEEE Transactions on Wireless Communications, 2018, 17(12): 8517-8530.

[48] SHU F, XU T Z, HU J S, et al. Delay-constrained covert communications with a full-duplex receiver[J]. IEEE Wireless Communications Letters, 2019, 8(3): 813-816.

[49] HE B, YAN S H, ZHOU X Y, et al. Covert wireless communication with a Poisson field of interferers[J]. IEEE Transactions on Wireless Communications, 2018, 17(9): 6005-6017.

[50] 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.

[51] LIU Z H, LIU J 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.

[52] JIANG Y E, WANG L M, CHEN H H. Covert communications in D2D underlaying cellular networks with antenna array assisted artificial noise transmission[J]. IEEE Transactions on Vehicular Technology, 2020, 69(3): 2980-2992.

[53] 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.

[54] JIANG X, CHEN X Y, TANG J, et al. Covert communication in UAV-assisted air-ground networks[J]. IEEE Wireless Communications, 2021, 28(4): 190-197.

[55] ZHOU X B, YAN S H, HU J S, et al. Joint optimization of a UAV's trajectory and transmit power for covert communications[J]. IEEE Transactions on Signal Processing, 2019, 67(16): 4276-4290.

[56] YAN S H, HANLY S V, COLLINGS I B. Optimal transmit power and flying location for UAV covert wireless communications[J]. IEEE Journal on Selected Areas in Communications, 2021, 39(11): 3321-3333.

[57] HU J S, WU Y P, CHEN R Q, et al. Optimal detection of UAV's transmission with beam sweeping in covert wireless networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(1): 1080-1085.

[58] ZHOU X B, YAN S H, SHU F, et al. UAV-enabled covert wireless data collection[J]. IEEE Journal on Selected Areas in Communications, 2021, 39(11): 3348-3362.

[59] CHEN X Y, SHENG M, ZHAO N, et al. UAV-relayed covert communication towards a flying warden[J]. IEEE Transactions on Communications, 2021, 69(11): 7659-7672.

[60] SHEIKHOLESLAMI A, GHADERI M, TOWSLEY D, et al. Multi-hop routing in covert wireless networks[J]. IEEE Transactions on Wireless Communications, 2018, 17(6): 3656-3669.

[61] WANG H M, ZHANG Y, ZHANG X, et al. Secrecy and covert communications against UAV surveillance via multi-hop networks[J]. IEEE Transactions on Communications, 2020, 68(1): 389-401.

[62] RENZO D M, ZAPPONE A, DEBBAH M, et al. Smart radio environments empowered by reconfigurable intelligent surfaces: how it works, state of research, and the road ahead[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(11): 2450-2525.

[63] 卢汉成, 王亚正, 赵丹, 等. 智能反射表面辅助的无线通信系统的物理层安全综述[J]. 通信学报, 2022, 43(2): 171-184.
LU H C, WANG Y Z, ZHAO D, et al. Survey of physical layer security of intelligent reflecting surface-assisted wireless communication systems[J]. Journal on Communications, 2022, 43(2): 171-184.

[64] LU X, HOSSAIN E, SHAFIQUE T, et al. Intelligent reflecting surface enabled covert communications in wireless networks[J]. IEEE Network, 2020, 34(5): 148-155.

[65] WU C Y, YAN S H, ZHOU X B, et al. Intelligent reflecting surface (IRS)-aided covert communication with warden's statistical CSI[J]. IEEE Wireless Communications Letters, 2021, 10(7): 1449-1453.

[66] KONG J, DAGEFUS F T, CHOI J, et al. Intelligent reflecting surface assisted covert communication with transmission probability optimization[J]. IEEE Wireless Communications Letters, 2021, 10(8): 1825-1829.

[67] ZHOU X B, YAN S H, WU Q Q, et al. Intelligent reflecting surface (IRS)-aided covert wireless communications with delay constraint[J]. IEEE Transactions on Wireless Communications, 2022, 21(1): 532-547.

[68] SI J B, LI Z, ZHAO Y, et al. Covert transmission assisted by intelligent reflecting surface[J]. IEEE Transactions on Communications, 2021, 69(8): 5394-5408.

[69] WANG C, LI Z, SHI J, et al. Intelligent reflecting surface-assisted multi-antenna covert communications: joint active and passive beamforming optimization[J]. IEEE Transactions on Communications, 2021, 69(6): 3984-4000.

[70] CHEN X, ZHENG T X, DONG L M, et al. Enhancing MIMO covert communications via intelligent reflecting surface[J]. IEEE Wireless Communications Letters, 2022, 11(1): 33-37.

[71] ZHENG M F, HAMILTON A, LING C. Covert communications with a full-duplex receiver in non-coherent Rayleigh fading[J]. IEEE Transactions on Communications, 2021, 69(3): 1882-1895.

[72] AGHDAM S R, DUMAN T M. Joint precoder and artificial noise design for MIMO wiretap channels with finite-alphabet inputs based on the cut-off rate[J]. IEEE Transactions on Wireless Communications, 2017, 16(6): 3913-3923.

[73] KANG X, LIANG Y C, YANG J. Riding on the primary: a new spectrum sharing paradigm for wireless-powered IoT devices[C]// Proceedings of 2017 IEEE International Conference on Communications. Piscataway: IEEE Press, 2017: 1-6.

[74] GUO S S, LV S H, ZHANG H X, et al. Reflecting modulation[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(11): 2548-2561.

[75] HU J S, YAN S H, ZHOU X Y, et al. Covert wireless communications with channel inversion power control in Rayleigh fading[J]. IEEE Transactions on Vehicular Technology, 2019, 68(12): 12135-12149.

[76] HU J S, YAN S H, ZHOU X B, et al. Covert communications without

channel state information at receiver in IoT systems[J]. IEEE Internet of Things Journal, 2020, 7(11): 11103-11114.

[77] SUN L L, XU T Z, YAN S H, et al. On resource allocation in covert wireless communication with channel estimation[J]. IEEE Transactions on Communications, 2020, 68(10): 6456-6469.

[78] 李啸天, 雷菁, 刘伟, 等. 平坦慢衰落信道下基于 HOS 的 PSK 调制盲信道估计[J]. 通信学报, 2015, 36(5): 144-151.
LI X T, LEI J, LIU W, et al. High-order statistics based blind channel estimation for PSK modulation in flat and slow fading channels[J]. Journal on Communications, 2015, 36(5): 144-151.

[79] HUANG K W, WANG H M, TOWSLEY D, et al. LPD communication: a sequential change-point detection perspective[J]. IEEE Transactions on Communications, 2020, 68(4): 2474-2490.

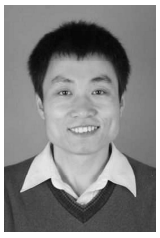
[80] HUANG K W, WANG H M, POOR H V. On covert communication against sequential change-point detection[J]. IEEE Transactions on Information Theory, 2021, 67(11): 7285-7303.

[作者简介]

陈炜宇（1996− ），男，福建龙岩人，国防科技大学博士生，主要研究方向为无线隐蔽通信、无源寄生通信。

骆俊杉（1992− ），男，重庆人，博士，国防科技大学讲师，主要研究方向为空间调制、信息安全。

王方刚（1982− ），男，黑龙江哈尔滨人，博士，北京交通大学教授，主要研究方向为无线通信、信号处理和信息论。



丁海洋（1980− ），男，北京人，博士，国防科技大学教授，主要研究方向为无线通信系统设计与性能分析、智能超材料、无线携能通信。

王世练（1976− ），男，江苏徐州人，博士，国防科技大学教授，主要研究方向为抗干扰安全通信与通信对抗、武器协同数据链。

夏国江（1981− ），男，江苏无锡人，博士，北京宇航系统工程研究所高级工程师，主要研究方向为无线测控与通信技术。