基于调制阶数混淆的安全通信

Jingyi Wang 和 Fanggang Wang

arXiv:2601.05292v1 [cs.IT] 8 Jan 2026

摘要——**随着无线通信的发展，安全传输面临着日益严峻的挑战。调制分类对于解码截获信号至关重要，而这使窃听者得以威胁通信安全。本文提出一种基于调制阶数混淆（MOC）的安全通信方法，将原始信号伪装成高阶或低阶调制，以误导 Eve 的分类器并防止信息泄露。对于单天线系统，我们设计了两种方案，即符号随机映射方案和符号时间分集方案。前者通过以概率方式将每个原始符号映射到多个备选符号，将低阶调制伪装成高阶调制，并通过凸优化调整映射概率，以平衡误差性能与安全性。后者通过将部分信息编码在变化的符号持续时间中，将高阶调制伪装成低阶调制，从而在不丢失信息的情况下降低表观调制阶数。这两种方案均要求 Bob 采用定制的接收机设计，以实现正确解调。对于多天线系统，我们提出无需修改接收机的调制阶数混淆方案。我们引入了两种信号设计策略：一种是基于级数展开的方案，由基于泰勒级数的混淆发射机将原始信号分解为结构化分量；另一种是星座路径设计混淆方案，将信号表示为沿预定义轨迹排列的一般分量之和。我们进一步将多天线 MOC 方法扩展至可重构智能表面（RIS）系统，并提出 RIS反射与波束成形器的联合设计。即使 Eve 执行完美的盲源分离，也无法推断出真实的调制格式。数值结果表明，所提出的调制阶数混淆方案能够有效抵御现有调制分类器，包括基于深度学习和基于专家知识的方法，同时不损害通信质量。**

索引词—**调制分类、可重构智能表面、安全通信**。

一、引言

随着智能设备数量的增长和网络覆盖范围的扩大，无线通信得到了迅速发展 [1]。然而，由于无线通信媒介具有广播特性，无线通信的安全性面临严峻挑战 [2]–[4]。增强无线通信安全性的常见方法包括基于加密的方案和物理层安全（PLS） [5], [6]。前一类方案通常计算开销较大，因此难以部署在低成本设备上。近年来，物理层安全方案因其复杂度低、可靠性高而受到关注。

对于无线通信系统而言，调制分类是非合作接收机在信号解调和译码前的一项关键工作。考虑一个由 Alice、Bob 和 Eve 组成的通信系统，[1]其中 Bob 将事先约定的调制格式作为先验知识进行解调，而 Eve 则必须先识别 Alice 所用的调制格式，才能恢复数据。因此，无线信号调制分类与抗分类的研究已受到研究人员的广泛关注。

学者对调制分类的研究早在上世纪就已开始。早期工作大致可分为两类，即基于似然的方法和基于特征的方法，分别源自统计决策理论和模式识别理论。基于似然的方法性能最优，但难以求得闭式解。此外，在受衰落、频偏和相位偏移等问题影响的动态环境中，基于似然的方法鲁棒性有限 [7]–[10]。相比之下，基于特征的方法实现起来更简单，且性能接近最优，因此受到学者们的广泛研究。调制分类中，许多特征是利用专家知识提取的，例如累积量 [11]、循环平稳谱[13],、小波变换 [14], [15], 等。近年来，神经网络架构的发展、优化算法的改进以及硬件设备的更新，推动深度学习成为调制分类领域的主流。这些进展使深度学习取得出色表现，并逐步取代该领域的传统方法 [17], [18]。目前已有许多专为调制分类任务设计的神经网络，例如 VGG [18],、SCGNet[19],、WSMF [20], 、ChainNet [21], 和 CGDNet [22]。基于深度学习的调制分类方法为应对复杂的无线信号环境提供了一种鲁棒且灵活的方案。目前的调制分类策略主要面向单天线系统。由于每根天线接收的都是来自不同发射天线的混合信号，因此在多天线系统中识别调制方式更具挑战性。经典的多天线调制分类方法包括基于独立成分分析 [23] 和期望最大化 [24], 的方法，两者均旨在先分离多径信号，再分别识别其调制方式。相比之下，采用矩统计量的方法则被提出用于捕捉多天线信号的全面特征，

[1]在无线安全领域先前研究的基础上，我们分别用“Alice”、“Bob”和“Eve”表示发射机、预期接收机和窃听者。

以实现调制识别 [25], [26]。调制分类方案已日趋成熟，使 Eve 能够轻易解密 Alice 的发射信号，从而带来显著的安全风险。因此，抗调制分类技术日益受到关注。

如今，专注于调制方法的通信安全研究仍处于早期阶段。在 [27],中，作者提出了一种基于相位的自适应调制方案，以增强通信安全性。该方法根据信道相位动态调整调制类型，但要求 Alice 和 Bob 准确估计信道；否则，误码率（BER）将会升高。 [28] 中的研究人员提出了一种基于星座映射混淆的安全调制技术，该技术会为每个数据包随机改变星座映射规则，而不是为每个数据包使用预定义的映射方案。该方案要求 Alice 和 Bob 共享映射规则，并且只有在采用高阶调制时才能提供更好的安全性能。近年来，对抗机器学习因其能够引入细微扰动、误导深度学习模型的潜力而受到广泛关注。这种方法已被应用于无线通信中的安全调制分类系统，以阻止窃听者正确分类信号。研究将这些对抗策略分为两种主要类型：独立攻击和附加攻击。独立攻击通过外部干扰器引入扰动，而不改变原始信号；附加攻击则由发射机将扰动直接融入信号中。 [29] 中的作者介绍了针对基于深度学习的调制分类器的白盒攻击和黑盒攻击，并表明与传统干扰技术相比，这些方法只需较低的发射功率即可成功实现错误分类。 [30] 中的研究评估了针对该分类器的各种攻击策略，结果表明，对抗扰动会显著降低分类准确率，而且迭代方法的效果优于单步方法。此外， [31] 指出，在扰动设计未考虑衰落信道的场景中，对抗扰动并不起作用。 [32],中的作者提出了一个优化加性攻击的通用框架，有效地纳入了影响通信性能和安全性的因素。这些基于对抗攻击的反调制分类策略能够有效抑制基于深度学习的调制分类器的性能。然而，由于存在人为引入的扰动，Bob 的误码率不可避免地会受到影响。此外，尽管这些细微干扰能够削弱基于深度学习的调制分类算法的效能，但它们抑制基于专家特征的分类器的能力有限。

本文的主要贡献如下：

- 提出了一种基于调制阶数混淆（MOC）的安全通信方法，通过防止 Eve 准确识别合法链路所用的调制格式，确保传输机密性。我们针对单天线系统和多天线系统分别设计了调制阶数混淆方案。前者需要定制接收机设计，而后者不需要。与现有的安全通信和抗调制分类方案相比，所提出的方案不依赖于对 Eve 的任何了解。用户可以灵活地将原始信号伪装成更高阶或更低阶的调制，以平衡安全性和误差性能。
- 在单天线系统中，我们提出了两种调制阶数混淆方案，用于将原始信号伪装成高阶或低阶调制信号。第一种方案基于符号随机映射，以概率方式将每个原始符号映射为高阶调制符号。通过优化映射概率，在误码率与安全性之间取得平衡。第二种方案基于符号时间分集，使用数量较少的低阶符号表示每个原始符号，并将部分信息编码在变化的符号持续时间中。在接收机端，我们设计了相应的解调器，即第一种方案所用的符号逆映射解码器，以及第二种方案所用的基于动态规划的解码器。
- 在多天线系统中，我们还提出了两种调制阶数混淆方案：一种基于级数展开，另一种基于星座路径设计。对于前者，我们提出了基于泰勒级数的混淆方案，将原始信号分解为多个具有特殊结构的分量。对于后者，信号表示为沿预定义星座轨迹排列的广义分量之和。随后，我们将多天线调制阶数混淆方法扩展到可重构智能表面（RIS）系统，并提出RIS反射与波束成形器的联合设计。所有这些混淆方案均不需要接收机设计。

本文其余部分安排如下。第二节介绍单天线系统中的调制混淆方案。第三节提出多天线系统中的调制混淆方案。第四节介绍所提方案在RIS辅助系统中的扩展。第五节给出仿真结果。第六节总结全文。

符号说明：变量、向量和矩阵分别用斜体字母 x、粗斜体字母 $\boldsymbol{x}$ 和粗大写斜体字母 $\boldsymbol{X}$ 表示。对于任意向量 $\boldsymbol{x}$，$\mathrm{diag}\{\boldsymbol{x}\}$ 表示对角线由 $\boldsymbol{x}$的元素构成的对角方阵。对于任意方阵 $\boldsymbol{X}$，$[\boldsymbol{X}]_{\mathrm{diag}}$ 表示由$\boldsymbol{X}$的对角元素构成的对角方阵。$\mathbb{C}^M$ 表示所有 M 复值向量构成的集合，$\mathbb{C}^{M\times N}$ 表示所有 $M\times N$ 复值矩阵构成的集合。$\Re\{\cdot\}$ 表示该元素的实部。运算符 $(\cdot)^{\mathsf{T}}$ 表示转置。定义 $\mathcal{I}_N=\{1,2,\ldots,N\}$ 作为指标集的简写。复数的虚数单位记为 $\jmath=\sqrt{-1}$。对数默认以2为底。

II. 单天线通信中的调制阶数混淆

本节首先介绍一种单天线通信系统。随后提出两种调制阶数混淆方案，用于

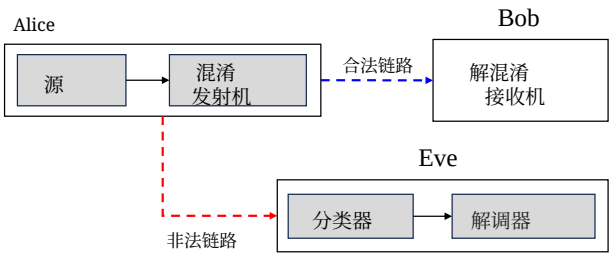

图 1. 单天线系统示意图。

混淆调制阶数，使其看起来像是更高阶或更低阶。最后，我们分析并比较这两种方案。

A. 单天线系统模型

我们考虑一个无线通信系统，其中 Alice 与 Bob 通信，而 Eve 试图识别 Alice 的调制格式，如图1所示。Alice、Bob 和 Eve 均配备一根天线。为防止 Eve 轻易识别调制格式，Alice 使用混淆发射机，将信号伪装成另一种调制格式。具体而言，Alice 的原始安全信号为 $\boldsymbol{s} = [s_1, s_2, \ldots, s_L]^{\mathsf{T}}$，混淆后的发射信号记为 $\boldsymbol{x} = [x_1, x_2, \ldots, x_L]^{\mathsf{T}}$，其中 $s_l \in \mathcal{A}$、$x_l \in \mathcal{B}$、$l \in \mathcal{I}_L$、$\mathcal{A} = \{a_1, a_2, \ldots, a_M\}$ 和 $\mathcal{B} = \{b_1, b_2, \ldots, b_N\}$ 分别是混淆前后的调制格式的信号字母表；M 和 N 分别表示 $\mathcal{A}$ 和 $\mathcal{B}$ 的调制阶数，其中 $M \neq N$；L 是信号序列的长度。

Bob 的接收信号序列为 $[y_1, y_2, \ldots, y_L]^{\mathsf{T}}$ l $\boldsymbol{y}$，其第 - 个符号为 =

$$y_l = hx_l + \mu, \quad l \in \mathcal{I}_L \tag{1}$$

其中，h是 Alice 与 Bob 之间的信道状态信息（CSI），μ表示 Bob 处的加性高斯白噪声（AWGN），该噪声服从圆对称复高斯分布，即 $\mu \sim \mathcal{CN}(0, \sigma^2)$。Eve 接收到来自 Alice 的信号$\boldsymbol{z} = [z_1, z_2, \ldots, z_L]^{\mathsf{T}}$，其 l 个符号中的第 $\boldsymbol{z}$ 个为

$$z_l = gx_l + \nu, \quad l \in \mathcal{I}_L \tag{2}$$

其中，g 是 Alice-Eve链路的信道状态信息，ν 是 Eve 处的加性高斯白噪声（AWGN），即 $\nu \sim \mathcal{CN}(0, \gamma^2)$。

注*1*：在单天线系统中，Bob 了解混淆策略，并采用经过专门设计的接收机，有效地对接收信号进行解混淆。由于调制识别错误，Eve 无法解码，具体内容将在后续小节中详细阐述。在复杂度和成本方面的考量使得重新设计 Bob 的接收机以适配 Alice 的混淆发射机并不可取时，我们提出了一种多天线安全通信系统，并将在下一节介绍。

B. 低阶到高阶混淆

本节首先介绍一种基于符号随机映射（SRM）的低阶到高阶混淆发射机。然后，我们建立映射概率优化问题，以平衡安全性和误差性能。最后，介绍 Bob 接收机的设计。

1) 混淆发射机：符号率调制（SRM）的概念是：根据特定概率，将原始调制格式$\mathcal{A}$ 中的每个符号映射到混淆后调制格式 $\mathcal{B}$中的若干符号之一。这种方法旨在使 Eve 高估合法信号的调制阶数。在这种低阶到高阶混淆场景中，我们有 $M < N$。首先，将调制格式 $\mathcal{B}$（阶数为 N）的信号字母表划分为 M个有序子集，记为

$$\mathcal{B}_m = \{b_1^{(m)}, b_2^{(m)}, \ldots, b_{K_m}^{(m)}\}, \quad m \in \mathcal{I}_M \tag{3}$$

满足

$$\bigcap_{m \in \mathcal{I}_M} \mathcal{B}_m = \emptyset, \quad \bigcup_{m \in \mathcal{I}_M} \mathcal{B}_m = \mathcal{B} \tag{4}$$

其中 K_m，$m \in \mathcal{I}_M$ 表示$\mathcal{B}_m$，$m \in \mathcal{I}_M$中的元素数量。随后，将 $\mathcal{A}$ 中的每个符号 a_m 以概率向量 $\boldsymbol{p}_m$映射为 $\mathcal{B}_m$ 中的一个符号，具体如下：

$$\boldsymbol{p}_m = [p_1^{(m)}, p_2^{(m)}, \ldots, p_{K_m}^{(m)}], \quad m \in \mathcal{I}_M \tag{5}$$

其中 $p_i^{(m)}$，$i \in \mathcal{I}_{K_m}$ 表示符号a_m 被映射到 $b_i^{(m)}$，$i \in \mathcal{I}_{K_m}$的概率。实际应用中，由于M 和 N 均为 2 的幂次，不失一般性，我们将 $\mathcal{B}$ 均匀划分为 M 组，每组包含 $K = \frac{N}{M}$ 个元素。当 $\mathcal{B}$ 中的符号均匀划分为 M组且 $\boldsymbol{p}_m$，$m \in \mathcal{I}_M$ 中的概率相等时，混淆信号 $\boldsymbol{x}$中的 b_n，$n \in \mathcal{I}_N$ 具有相等且相互独立的概率，因此，$\boldsymbol{x}$ 的物理特性完全符合调制格式 $\mathcal{B}$。然而，由于信道条件较差且存在噪声，Alice 通常会选择低阶调制 $\mathcal{A}$。将其完全伪装成高阶调制 $\mathcal{B}$ 虽能增强安全性，却会显著损害误差性能。因此，在下一小节中，我们将设计一种优化方案，以平衡安全性和误差性能。

2）映射概率优化问题：我们采用 BER ϑ 作为误差性能的衡量指标，并以混淆前后符号概率分布之间的 Kullback–Leibler（KL）散度作为安全性能的衡量指标。Alice 的目标是在满足 BER 约束的前提下，通过优化概率向量 $\boldsymbol{p}_m$，$m \in \mathcal{I}_M$ 来最小化 KL 散度。具体优化问题见下述引理。

引理 *1*：在误码率约束下，最小化原始分布与混淆分布之间 KL 散度的问题

符号分布可表示为

$$\mathcal{P}1: \min_{\boldsymbol{p}_m, m\in\mathcal{I}_M} \quad \log K - \frac{1}{M}\sum_{m=1}^{M} H(\boldsymbol{p}_m) \tag{6a}$$

$$\text{s.t.} \quad \vartheta \leqslant \eta \tag{6b}$$

$$\sum_{i=1}^{K} p_i^{(m)} = 1, \quad m \in \mathcal{I}_M \tag{6c}$$

其中 $H(\boldsymbol{p}_m) = -\sum^{K} p_i^{(m)} \log p_i^{(m)}$，$\eta$ 是由$i=1$给出的误码率约束

$$\vartheta = \frac{1}{M\log M}\sum_{m=1}^{M}\sum_{i=1}^{K} p_i^{(m)} \sum_{j=1}^{N-K} \rho_{i,j}^{(m)} Q\left(\frac{\Delta_{i,j}^{(m)}}{\sqrt{2}\sigma}\right). \tag{7}$$

证明：证明见附录。 ■

该问题 $\mathcal{P}1$ 是一个凸熵最小化问题，可使用 CVX [33]直接求解。

3）解混淆接收机：Bob 的接收机可设计为由传统解调器和解映射器级联构成。首先，Bob 对 $\boldsymbol{y}$ 进行解调，以获得调制格式 $\mathcal{B}$的符号$\boldsymbol{x}$。然后，基于 Alice 对 $\mathcal{B}$中符号的分组，Bob 将 $\boldsymbol{x}$ 中的每个符号重新映射回 $\mathcal{A}$中的对应符号，从而恢复 s，即

$$s_l = \sum_{m\in\mathcal{I}_M} a_m \mathbb{I}_{\{x_l\in\mathcal{B}_m\}}, \quad l \in \mathcal{I}_L \tag{8}$$

其中，$\mathbb{I}_{\{x_l\in\mathcal{B}_m\}}$ 是一个指示函数：若$x_l \in \mathcal{B}_m$ 则取值为 1，否则取值为 0。Eve 难以实施这一过程，原因如下。首先，Eve 根据调制分类的结果对 $\boldsymbol{z}$进行解调，因此难以检测出信号已被映射。其次，即使 Eve 意识到发送符号已被映射，也没有任何信息来确定映射规则。第三，Alice 可以在与 Bob 通信期间动态调整分组规则和映射概率。

C. 高阶到低阶混淆

本节提出一种基于符号时间分集（STD）的方案，将高阶调制混淆为低阶调制。我们首先介绍 Alice 的混淆发射机，然后通过动态规划（DP）设计 Bob 的解混淆接收机。

1) 混淆发射机：STD 的原理是使用混淆调制 $\mathcal{B}$ 中时长变化的相同符号，来表示原始调制 $\mathcal{A}$ 中的多个符号。对于阶数为 M 、其中 $M > N$ 的原始调制格式 $\mathcal{A}$，首先将信号字母表划分为 $N-1$ 个有序子集，记为

$$\mathcal{A}_n = \left\{a_1^{(n)}, a_2^{(n)}, \ldots, a_{K_n}^{(n)}\right\}, \quad n \in \mathcal{I}_{N-1} \tag{9}$$

满足

$$\bigcap_{n\in\mathcal{I}_{N-1}} \mathcal{A}_n = \emptyset, \quad \bigcup_{n\in\mathcal{I}_{N-1}} \mathcal{A}_n = \mathcal{A} \tag{10}$$

其中，K_n，$n \in \mathcal{I}_{N-1}$ 表示$\mathcal{A}_n$，$n \in \mathcal{I}_{N-1}$中的元素数量。接下来，符号 $a_i^{(n)}$，$i \in \mathcal{I}_{K_n}$，$n \in \mathcal{I}_{N-1}$

算法1 高阶到低阶混淆发射机

输入： $\boldsymbol{s}$;

初始化： $\boldsymbol{x} = \mathbf{0}$;

1：使用 (11) 更新 x_1；

2: **对于** $l = 2:\ L$ **执行**

3: **若** x_{l-1} 未映射到 b_N 且 $\exists\mathcal{A}_n$，$n \in \mathcal{I}_{N-1}$

4: 使得 s_{l-1}，$s_l \in \mathcal{A}_n$ **则**

5: 使用 (12) 更新 x_l；

6: **else**

7: 使用（11）更新 x_l；

8: **结束 if**

9: **结束 for**

输出： $\boldsymbol{x}$。

被映射到 b_n，$n \in \mathcal{I}_{N-1}$，并持续 i 个符号周期。这意味着，不同的高阶调制符号被映射到相同的低阶调制符号，但各自的长度不同，即，

$$x_l = \underbrace{b_n \cdots b_n}_{i},\ s_l = a_i^{(n)},\ i \in \mathcal{I}_{K_n},\ n \in \mathcal{I}_{N-1},\ l \in \mathcal{I}_L \tag{11}$$

其中，每个 b_n 持续一个符号周期。如果 $\boldsymbol{s}$中两个相邻符号属于同一个 $\mathcal{A}_n$，则会形成一段更长的相同符号序列。Bob 很难准确判断每个符号的实际持续时间。例如，对于符号序列 $b_1b_1b_1$，Bob 无法分辨它表示的是$b_1\ b_1b_1$、$b_1b_1\ b_1$还是 $b_1\ b_1\ b_1$。因此，如果 s_l，$l \in \mathcal{I}_L \setminus \{1\}$ 属于与 s_{l-1} 相同的子集，且s_{l-1} 未映射到 b_N，那么 s_l 会在保持原持续时间的情况下映射到 b_N，即

$$x_l = \underbrace{b_N \cdots b_N}_{i},\ s_l = a_i^{(n)},\ i \in \mathcal{I}_{K_n},\ n \in \mathcal{I}_{N-1},\ l \in \mathcal{I}_L\backslash\{1\}. \tag{12}$$

如果它们不属于同一个子集，或者 s_{l-1} 已映射到 b_N，则按照（11）正常映射该符号。根据此规则，原始安全信号 $\left[s_1, s_2, \ldots, s_L\right]^{\mathsf{T}}$ $\boldsymbol{x} = [x_1, x_2, \ldots, x_L]^{\mathsf{T}}$

被映射为，其中 $\boldsymbol{x}$ 中的相邻符号始终不同，且每个符号的持续时间都是符号周期的整数倍。如果按照原始符号周期进行分析，实际观测到的信号序列记为 $\boldsymbol{x'} = [x'_1, x'_2, \ldots, x'_J]^{\mathsf{T}}$，其中$J$ 表示混淆后采样的符号数量。与低阶调制符号相比，高阶调制符号所包含的额外信息通过符号持续时间的差异传递，从而产生 $L < J$。高阶到低阶混淆发射机总结于算法1中。

考虑到通信效率和信号处理的便利性，原始调制格式的阶数 M $\mathcal{A}$通常为 2 的幂。对于混淆调制格式 $\mathcal{B}$，其阶数 N 也可以设为 2 的幂，例如采用常见的正交幅度调制或相移键控调制。然而，这种配置会导致 M无法均匀划分为 $N-1$个子集，使混淆序列 $\boldsymbol{x'}$中各符号出现的概率差异显著，从而可能引起 Eve 的警觉。因此，可以考虑采用阶数灵活的

调制格式，例如黄金角调制（GAM） [34]，将 $N-1$ 设为 2 的幂，使符号在 $\boldsymbol{x}'$中以相同概率出现。具体而言，GAM 的第 n个星座点的复振幅为

$$x_n = r_n e^{j2\pi\varphi n}, \quad n \in \mathcal{I}_N \tag{13}$$

其中 $\varphi = 1 - \frac{\sqrt{5}-1}{2}$ $r_n = c_{\text{disc}}\sqrt{n}$ $n \in \mathcal{I}_N$ $c_{\text{disc}} \triangleq \sqrt{\frac{2\bar{P}}{N+1}}$，且 $\bar{P}$。考虑到功率归一化约束，通常设为 1。

2）解混淆接收机：由于 Bob 事先无法知道 $\boldsymbol{x}$ 中每个符号的持续时间，因此采用单位符号周期进行采样，得到 $\boldsymbol{y}' = [y'_1, y'_2, \ldots, y'_J]^{\mathsf{T}}$，其中第 j 个符号表示为

$$y'_j = hx_j + \mu, \quad j \in \mathcal{I}_J. \tag{14}$$

算法1生成的 $\boldsymbol{x}$ 中，相邻符号始终不同。因此，在 $\boldsymbol{y}'$中，我们可以通过检测符号变化点，并根据每次变化的时间间隔进行综合判断，恢复原始符号序列。由于每个符号的持续时间是随机的，在衰落信道和噪声的影响下，序列前部的符号一旦被误判 $\boldsymbol{y}'$，就可能导致严重的错误传播。例如，将 $b_1\ b_2$ 误判为 $b_1\ b_1$ 可能会导致两个原始符号被误认为一个，从而造成符号丢失。因此，我们设计了一种基于动态规划方法的 Bob 解混淆接收机，以防止错误传播。

首先，Bob 构建一个动态规划表 $\boldsymbol{D}_{\text{T}}$ 和一个路径表 $\boldsymbol{P}_{\text{T}}$，其中 $d_{\text{T}}(j,\ l)$ 和 $p_{\text{T}}(j,\ l)$ $l \in \mathcal{I}_L,\ \ j \in \mathcal{I}_J$分别表示 $\boldsymbol{D}_{\text{T}}$ 和 $\boldsymbol{P}_{\text{T}}$中第 j 行、第 l 列的元素。对于 $d_{\text{T}}(j,\ l)$，它表示将前 j 个符号划分为 l 组的最小差异代价，而$d_{\text{T}}(0,\ 0)$设为零，因为将零个符号划分为零组不产生任何代价。 $\boldsymbol{D}_{\text{T}}$ 中的所有其他元素均初始化为一个非常大的值，表示无效或尚未计算的状态。 $\boldsymbol{P}_{\text{T}}$ 中的所有元素均设为零。此处，Bob 知道一个包含L 个原始符号的接收帧 $\boldsymbol{y}'$，也知道 $K_n,\ \ n \in \mathcal{I}_{N-1}$的最大值，即 $K_{\max}$，这是 Alice 和 Bob 先前约定的。随后，Bob 遍历接收符号序列 $\boldsymbol{y}'$。如果 y'_j 构成一个新组 l，则分组的总代价为

$$c_{j,1} = d_{\text{T}}(j-1, l-1) + c_1,\ j \in \mathcal{I}_J \tag{15}$$

其中， c_1 是表示单个符号组成本的常数成本。此外，如果将 y'_j 及其前面的 $k-1$个符号（共 k 个符号）归为一组，则总成本为

$$c_{j,k} = d_{\text{T}}(j-k, l-1) + c'_{j,k} \quad j \in \mathcal{I}_J \setminus \{1\},\quad k \in \mathcal{I}_{K_{\max}} \setminus \{1\} \tag{16}$$

其中

$$c'_{j,k} = \frac{1}{k}\sum_{i=0}^{k-1} \left| y'_{j-i} - \tilde{b}_{j,k} \right| \quad j \in \mathcal{I}_J \setminus \{1\},\quad k \in \mathcal{I}_{K_{\max}} \setminus \{1\} \tag{17}$$

$$\tilde{b}_{j,k} = \underset{b_n,\ n \in \mathcal{I}_N}{\arg\min} \left| \frac{1}{k}\sum_{i=0}^{k-1} y'_{j-i} - b_n \right| \quad j \in \mathcal{I}_J \setminus \{1\},\ k \in \mathcal{I}_{K_{\max}} \setminus \{1\}. \tag{18}$$

请注意，使用 (16) 时，必须满足 $j \geqslant k$。动态规划表更新如下：

$$d_{\text{T}}(j,l) = \min\left\{c'_{j,k}\right\},\ j \in \mathcal{I}_J,\ l \in \mathcal{I}_L,\ k \in \mathcal{I}_{K_{\max}}. \tag{19}$$

路径信息记录在 $\boldsymbol{P}_{\text{T}}$ 中，以便重构分组序列，即

$$p_{\text{T}}(j,l) = \underset{k \in \mathcal{I}_{K_{\max}}}{\arg\min}\left\{c'_{j,k}\right\}, \quad j \in \mathcal{I}_J, \quad l \in \mathcal{I}_L. \tag{20}$$

接下来，从 $p_{\text{T}}(J,\ L)$开始，Bob利用存储的路径信息回溯，以重构符号的最优分组。通过检查 $\boldsymbol{P}_{\text{T}}$中记录的转换来确定分组路径，这些转换标识了组成一个分组的符号数量。首先，Bob将 $\tilde{\boldsymbol{x}}_{\text{inv}} = [\tilde{x}_{\text{inv},1}, \tilde{x}_{\text{inv},2}, \ldots, \tilde{x}_{\text{inv},L}]^{\mathsf{T}}$ 设置为解混淆后的$[\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_L]^{\mathsf{T}}$ $j = J\ \ l = L$ 的逆序列，并设置，。随后，Bob从 $\boldsymbol{P}_{\text{T}}$中获取元素 k^*，即

$$k^* = p_{\text{T}}(j,l) \tag{21}$$

且 $\tilde{x}_{\text{inv},\ l}$ 由下式给出

$$\tilde{x}_{\text{inv},l} = \underbrace{\tilde{b}_{j,k^*} \cdots \tilde{b}_{j,k^*}}_{k^*}, \quad l \in \mathcal{I}_L \tag{22}$$

其中 $\tilde{b}_{j,\ k^*}$ 使用式（18）计算。然后，Bob 将 j 更新为$j - k^*$，并将 l 更新为 $l-1$，通过迭代计算得到完整序列 $\tilde{\boldsymbol{x}}_{\text{inv}}$，而 $\tilde{\boldsymbol{x}}$ 则通过反转 $\tilde{\boldsymbol{x}}_{\text{inv}}$得到，即

$$\tilde{x}_l = \tilde{x}_{\text{inv},L-l+1}, \quad l \in \mathcal{I}_L. \tag{23}$$

高阶到低阶去混淆接收器总结于算法2中。

备注*2*：所提出的高阶到低阶混淆在概念上与变长源编码（如霍夫曼编码）相似，在这类编码中，符号被映射为长度不等的表示形式。然而，将这类编码直接应用于调制混淆会造成显著的频谱效率损失，因为前缀无关约束会使长序列占据大部分传输时间。未来的工作可以探索在明确速率约束下受源编码启发的设计，以更好地平衡安全性与频谱效率。

备注 *3*：在高阶到低阶调制映射中，固定长度映射简化了接收机设计，但与变长映射相比，其频谱效率和安全性较低。这是因为每个高阶符号都与一个固定的低阶序列绑定，导致低阶符号的统计分布直接反映原始调制的统计分布。调制分类算法可以轻易利用这类相关性；即使源分布均匀，固定映射也会引入序列规律性，从而削弱对分类的抵抗能力。

D. 单天线方案分析

本节首先分析所提出方案的安全性。然后，我们详细分析并比较

算法2高阶到低阶去混淆接收器

输入： $\boldsymbol{y}'$，L;
初始化： $d_{\mathrm{T}}(0,\ 0)=0,\quad d_{\mathrm{T}}(j,\ l)=10^{6},\quad j\in\mathcal{I}_J,\quad l\in\mathcal{I}_L$;
初始化： $p_{\mathrm{T}}(j,\ l)=0,\quad j\in\mathcal{I}_J,\quad l\in\mathcal{I}_L$;
对于 $j=1:\ J$ **执行**
  对于 $l=1:$ 最小值$\{L,j\}$ **执行**
    使用 (15) 计算$c'_{j,\ 1}$；
    对于 $k=1:\ K_{\max}$ **do**
      如果 $j\geqslant k$ **则**
        使用 (16) 计算$c'_{j,\ k}$；
      结束如果
    结束循环
    使用（19）更新 $d_{\mathrm{T}}(j,l)$;
    使用（20）更新 $p_{\mathrm{T}}(j,l)$;
  结束循环
结束循环
$j=J$;
$l=L$;
当 $j>0$ 且 $l>0$ **执行**
  使用式 (21) 计算 k^*；
  使用式 (22) 计算 $\tilde{x}_{\mathrm{inv},\ l}$
  $j=j-k^*$;
  $l=l-1$;
结束循环
使用 (23) 计算 $\tilde{\boldsymbol{x}}$;
输出： $\boldsymbol{x}$。

两种混淆方案的优缺点。

对于低阶到高阶混淆方案，其一项显著优势是能够通过调整映射概率，平衡通信性能与安全性。与自适应调制技术中僵化的切换方式相比，该方案在适应信道条件方面更加灵活。然而，其缺点是调制阶数增加不可避免地会导致误码率性能下降。

对于高阶到低阶混淆方案，其优势在于误码率性能有所提升。原因之一是阶数降低会使星座图更加稀疏，从而增强抗噪性。另一个重要原因是所提接收机基于动态规划方法，具备错误检测能力。如第二节 II.B 所述，在 $\boldsymbol{y}'$ 中，同一符号最多会连续出现 $K_{\max}$ 次。如果出现次数更多，算法2将根据最优路径进一步对这些符号进行分组，并对同一组中的多个符号进行联合判决解调，如公式 (18) 所示。然而，高阶到低阶混淆方案的缺点是频谱效率降低。例如，将 8 阶调制伪装成 4 阶调制时，频谱效率会从 3bit/s/Hz 降至 2bit/s/Hz。

所提出的调制阶数混淆方案主要通过符号率调制（SRM）和符号持续时间调制（STD）误导 Eve 的调制分类器，从而实现安全性。通过优化符号映射概率或改变符号持续时间，发送信号分布会变得与另一种调制阶数的分布无法区分，而配备映射信息或持续时间信息的合法接收机则能够可靠地恢复原始符号。然而，如果 Eve 获得了有关映射或持续时间分布的部分先验知识，所提出方案的安全性可能会降低。此外，安全性与通信性能之间存在固有的权衡，因为过度混淆可能导致频谱效率降低或误比特率升高。这些局限表明，未来的工作可通过引入动态映射、时频混合混淆和多天线协作来增强该方案的鲁棒性。

在单天线系统中，所提出的两种调制阶数混淆方案要求 Bob 设计专用接收机，并预先与 Alice 商定一些参数设置；但在某些场景下，这可能无法实现，例如 Bob 的计算资源有限时。为解决这一问题，下一节将介绍多天线调制阶数混淆方案，即使 Bob 缺乏先验信息，也能实现安全通信。

III. 多天线通信中的调制阶数混淆

本节首先介绍一个多天线通信系统，然后介绍一种基于信号融合的调制阶数混淆方案。

A. 多天线系统模型

考虑一个点对点通信系统，其中包括一台具有 T_{A} 根天线的发射机（Alice）、一台单天线合法接收机（Bob）以及一台具有 T_{E} 根天线的被动窃听者（Eve）。原始安全符号为 $\left[x_1,x_2,\ldots,x_{T_{\mathrm{A}}}\right]^{\mathsf{T}}$ $x_{t_{\mathrm{A}}}\ \ t_{\mathrm{A}}\in\mathcal{I}_{T_{\mathrm{A}}}$，$s\in\mathcal{A}$，经混淆后的发射信号为，其中，表示 Alice 的第 t_{A} 根天线发送的符号，且 $x_{t_{\mathrm{A}}}\in\mathcal{B}_{t_{\mathrm{A}}}$。这里，$\mathcal{B}_{t_{\mathrm{A}}}$，$t_{\mathrm{A}}\in\mathcal{I}_{T_{\mathrm{A}}}$ 是第 t_{A} 根天线的信号字母表，而 $N_{t_{\mathrm{A}}}$，$t_{\mathrm{A}}\in\mathcal{I}_{T_{\mathrm{A}}}$ 表示 $\mathcal{B}_{t_{\mathrm{A}}}$ 的调制阶数。Bob 接收到的符号为

$$y=\boldsymbol{h}\boldsymbol{W}\boldsymbol{x}+\mu \tag{24}$$

其中，$\boldsymbol{W}=\mathrm{diag}\{\boldsymbol{w}\}\in\mathbb{C}^{T_{\mathrm{A}}\times T_{\mathrm{A}}}$ 表示波束成形矩阵；$\boldsymbol{w}=[w_1,w_2,\ldots,w_{T_{\mathrm{A}}}]\in\mathbb{C}^{T_{\mathrm{A}}}$为波束成形向量；$\boldsymbol{h}=[h_1,h_2,\ldots,h_{T_{\mathrm{A}}}]\in\mathbb{C}^{T_{\mathrm{A}}}$表示从 Alice 到 Bob 的信道；$\mu$ 为 Bob 处的噪声，服从 $\mathcal{CN}(0,\ \sigma^2)$。Bob 的接收信号为

$$\boldsymbol{z}=\boldsymbol{G}\boldsymbol{W}\boldsymbol{x}+\boldsymbol{\nu} \tag{25}$$

其中，$\boldsymbol{G}\in\mathbb{C}^{T_{\mathrm{E}}\times T_{\mathrm{A}}}$ 为从 Alice 到 Eve 的信道响应；$\boldsymbol{\nu}$表示 Eve 处的噪声，即 $\boldsymbol{\nu}\sim\mathcal{CN}(0,\ \gamma^2)$。由于 Eve 不提供任何信息，该信道 $\boldsymbol{G}$ 对合法节点而言始终完全不可知。

B. 波束成形器设计

本节提出波束成形设计策略。我们的目标是使 Alice 的每根天线发出的信号在没有信道干扰的情况下直接汇聚到 Bob 处，从而

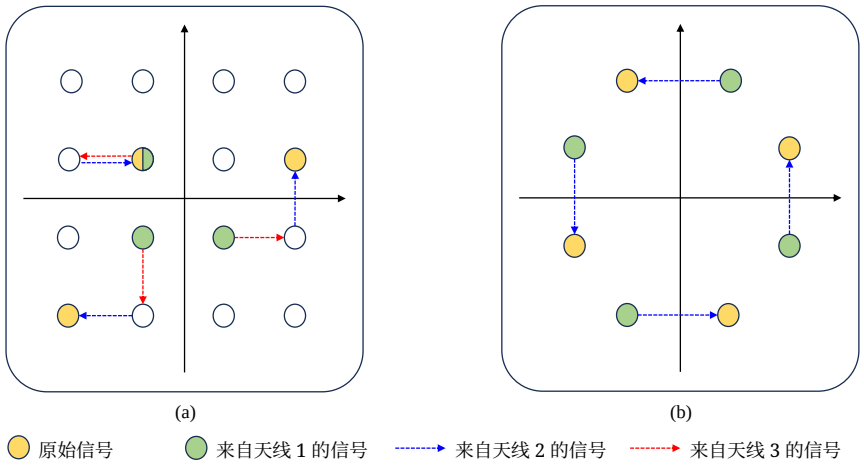

图 2 $\mathcal{B}_2 = \mathcal{B}_3 = \{2, -2, 2\jmath, -2\jmath\}$ 1 $\mathcal{B}_1 = \{1+1\jmath, 1-1\jmath, -1+$. 基于 CPD 的符号设计策略示意图。在子图 (a) 中，天线从集合中发射信号，$1\jmath, -1-1\jmath\}$ 2 3 而天线和从相同的集合中发射信号。在子图 (b) 中，天线从集合 $\mathcal{B}_1 = \{e^{\frac{3}{8}\pi}, e^{\frac{7}{8}\pi}, e^{-\frac{1}{8}\pi}, e^{-\frac{5}{8}\pi}\}$ 1 中发射符号，而天线 2 使用集合 $\mathcal{B}_2 = \{\sqrt{2}-\sqrt{2}, -\sqrt{2}-\sqrt{2}, \sqrt{2}-\sqrt{2}\jmath, -\sqrt{2}-\sqrt{2}\jmath\}$。

便于设计混淆发射机。因此，我们设定约束条件

$$\boldsymbol{h}\boldsymbol{W} = \boldsymbol{I}_{T_\mathrm{A}} \tag{26}$$

其中 $\boldsymbol{I}_{T_\mathrm{A}} = \underbrace{[1, 1, \ldots, 1]}_{T_\mathrm{A}}$，我们有

$$y = \boldsymbol{h}\boldsymbol{W}\boldsymbol{x} + \mu \tag{27}$$

$$= \sum_{t_\mathrm{A}=1}^{T_\mathrm{A}} x_{t_\mathrm{A}} + \mu. \tag{28}$$

这里，我们假设 Alice 已知 $\boldsymbol{h}$ ，这在物理层安全文献中是一个常见假设。因此，可以利用以下方法轻松设计波束成形向量 $\boldsymbol{w}$

$$w_{t_\mathrm{A}} = \frac{1}{h_{t_\mathrm{A}}}, \quad t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}}. \tag{29}$$

C. 低阶到高阶混淆

本节提出一种基于泰勒展开的混淆发射机。在 Alice 处，原始安全信号s 经过非线性变换，生成 $f(s)$。一个天线发射 $f(s)$，其余天线则发射 $f(s)$ 的泰勒级数展开中的非线性项的相反数。所有天线的信号在 Bob 处叠加后，得到原始安全信号 s 的线性项。具体而言，对于在 s_0 处可微的非线性函数 $f(s)$，第一个天线直接发射非线性信号 $f(s)$，即

$$x_1 = f(s). \tag{30}$$

天线 t_A, $t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}} \setminus \{1\}$ 发射

$$x_{t_\mathrm{A}} = -\sum_{n \in \mathcal{M}_{t_\mathrm{A}}} \frac{\lambda_n}{n!}(s-s_0)^n, \quad t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}} \setminus \{1\}$$

$$\bigcap_{t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}} \setminus \{1\}} \mathcal{M}_{t_\mathrm{A}} = \emptyset, \quad \bigcup_{t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}} \setminus \{1\}} \mathcal{M}_{t_\mathrm{A}} = \mathcal{I}_\infty \setminus \{1\} \tag{31}$$

其中

$$\lambda_n = \lim_{s \to s_0} \frac{\mathrm{d}^n f(s)}{\mathrm{d}s^n}, \quad n \in \mathcal{I}_\infty. \tag{32}$$

因此，Bob 的接收信号为

$$y = \sum_{t_\mathrm{A}=1}^{T_\mathrm{A}} x_{t_\mathrm{A}} + \mu \tag{33}$$

$$= f(s) - \sum_{t_\mathrm{A}=1}^{T_\mathrm{A}} \sum_{n \in \mathcal{M}_{t_\mathrm{A}}} \frac{\lambda_n}{n!}(s-s_0)^n + \mu \tag{34}$$

$$= f(s_0) + \sum_{n \in \mathcal{I}_\infty} \frac{\lambda_n}{n!}(s-s_0)^n - \sum_{n \in \mathcal{I}_\infty \setminus \{1\}} \frac{\lambda_n}{n!}(s-s_0)^n + \mu \tag{35}$$

$$= \lambda_1 s + f(s_0) - \lambda_1 s_0 + \mu \tag{36}$$

其中，(33)由(28)得出；(34)由(30)和(31)得出；(35)由泰勒定理得出。然后，Bob可以通过滤除直流电并对功率进行归一化，恢复原始安全信号 s。请注意，每根天线上的发射信号通常都包含直流分量，这对Bob恢复 s至关重要。尽管天线在发射前需要移除直流分量，Bob仍可通过直流偏置等简单方法恢复 s。为简要说明，我们在公式推导中省略了这一因素。通常， s 的均值为零，因此我们可以令 $s_0 = 0$，这意味着 $f(s)$在 $s = 0$ 附近展开，且Bob可以降低计算开销。事实上， s_0 的不同取值可以带来额外的保密自由度。

实际上，Alice 无法通过有限数量的天线传输无限多个泰勒级数项。通常，只传输其中最大的若干项，就足以让 Bob 几乎完美地接收到原始安全信号 s 。这一点将在后文的仿真部分讨论。天线可以随机分配信号项，使原始的 M 阶调制在每根天线上伪装成 N 阶调制。当集合 $\mathcal{M}_{t_\mathrm{A}}$, $t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}} \setminus \{1\}$ 固定时，$N = MT_\mathrm{A}$。

此外，函数 $f(s)$ 需要分析其收敛半径，该半径定义为以级数收敛中心为圆心、级数在其中收敛的最大圆盘的半径。以 $f(s) = \text{反正切}\ s$为例，其半径确定为 1。因此，对于相移键控调制，功率归一化后，所有星座点都位于单位圆上，从而确保泰勒级数展开收敛。相比之下，对于QAM调制，即使经过功率归一化，仍有若干符号位于单位圆之外。因此，需要进行幅度归一化，以确保所有星座点都位于单位圆内或圆上。有关基于级数展开的安全通信方案的详细讨论，请参阅我们先前的工作 [35]。

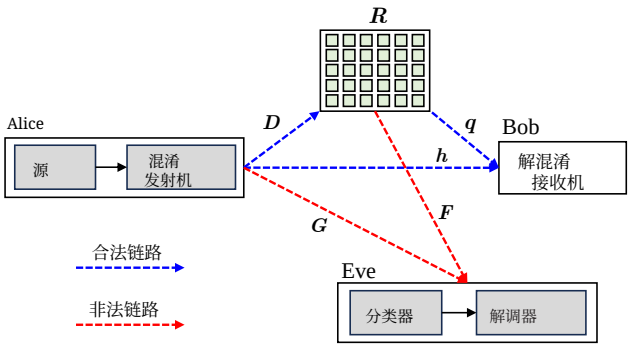

图 3. RIS辅助多天线系统示意图。

D. 高阶到低阶混淆

在本节中，我们提出一种基于星座路径设计（CPD）的混淆发射机，将从 Alice 的每根天线发射的信号伪装成低阶调制信号。具体而言，当从阶数为 M 的调制集合 $\mathcal{A}$ 发送原始安全信号 s 时，Alice 的第一根天线发送带有 $N_1 < M$ 的信号 $x_1 \in \mathcal{B}_1$。其余天线发射的信号会调整星座图中 x_1 的位置，最终将其移至 s 的位置。天线 t_{A}, $t_{\mathrm{A}} \in \mathcal{I}_{T_{\mathrm{A}}} \setminus \{1\}$ 发射的信号，记为 $x_{t_{\mathrm{A}}}$, $t_{\mathrm{A}} \in \mathcal{I}_{T_{\mathrm{A}}} \setminus \{1\}$，使 x_1 能够经历精心设计的移位。注意，$N_{t_{\mathrm{A}}} < M$, $t_{\mathrm{A}} \in \mathcal{I}_{T_{\mathrm{A}}} \setminus \{1\}$。这些移位形成集合 $\mathcal{B}_{t_{\mathrm{A}}}$, $t_{\mathrm{A}} \in \mathcal{I}_{T_{\mathrm{A}}} \setminus \{1\}$，作为用于混淆 Eve 的调制集合。

作为一个说明性示例，图2展示了如何通过 CPD 将 16QAM 和 8PSK 调制伪装成低阶调制。在图2(a)中，16QAM 调制中的每个星座点都可以从 $\mathcal{B}_1$ 中的一个符号出发，通过叠加来自 $\mathcal{B}_2$ 和 $\mathcal{B}_3$ 的符号偏移得到。即使 Eve 使用盲源分离来获取从三根天线发射的信号，也只能判断每根天线采用了某种 4 阶数字调制，因此无法解码原始安全信号。类似地，在图2(b)中，天线 1 发送集合 $\mathcal{B}_1$ 中的符号，而天线 2 使用集合 $\mathcal{B}_2$。两根天线协同工作，基于各自的 4 阶符号集发送 8PSK 调制符号。

注*4*：在多天线系统中，我们为 Alice 的每根天线设计发射符号，使得阶数
每个传输符号集的阶数都高于或低于原始安全符号集，但 Bob 可以将这些符号聚合起来，以恢复原始安全符号。因此，即使 Eve 使用先进的盲源分离技术捕获 Alice 的部分天线发出的信号，也仍然无法准确识别调制格式。此外，由于盲源分离固有的幅度和相位模糊，Eve 无法简单地将来自不同天线的信号相加来恢复原始安全信号。

IV. MOC方法在RIS辅助多天线通信中的应用

近年来，多天线系统发展出了各种新的通信范式，其中可重构智能表面（RIS）受到了广泛关注。本节首先介绍一种由 RIS 辅助的多天线通信系统，然后给出 RIS 和波束成形器的设计。

A. RIS辅助多天线系统模型

考虑一个RIS辅助通信系统，该系统由一个配备 T_{A} 根天线的发射机（Alice）、一个单天线合法接收机（Bob）、一个配备T_{E} 根天线的被动窃听者（Eve）以及一个含有 V个反射单元的RIS组成，如图3所示。当Alice与Bob之间存在和不存在直达链路时，Bob处接收到的符号分别为 y_1 和 y_2，即

$$y_1 = \boldsymbol{h}\boldsymbol{W}\boldsymbol{x} + \boldsymbol{q}\boldsymbol{R}\boldsymbol{D}\boldsymbol{W}\boldsymbol{x} + \mu_1 \tag{37}$$

$$y_2 = \boldsymbol{q}\boldsymbol{R}\boldsymbol{D}\boldsymbol{W}\boldsymbol{x} + \mu_2 \tag{38}$$

其中，矩阵 $\boldsymbol{D} \in \mathbb{C}^{V \times T_{\mathrm{A}}}$ 表示从Alice到RIS的信道状态信息；$\boldsymbol{R} = \text{diag}\{\boldsymbol{r}\} \in \mathbb{C}^{V \times V}$是RIS的相移矩阵，且有 $\boldsymbol{r} = [r_1, r_2, \ldots, r_V] \in \mathbb{C}^V$，其中$r_v = \rho_v e^{\jmath\theta_v}$，$v \in \mathcal{I}_V$、$\rho_v$和 θ_v 分别表示RIS第 v个反射单元的幅度和相移。[2] 向量 $\boldsymbol{q} = [q_1, q_2, \ldots, q_V] \in \mathbb{C}^N$表示从RIS到Bob的信道。 μ_1 和 μ_2 是Bob处的噪声，服从$\mathcal{CN}(0, \sigma^2)$。Eve接收到的信号为

$$\boldsymbol{z} = \boldsymbol{G}\boldsymbol{W}\boldsymbol{x} + \boldsymbol{F}\boldsymbol{R}\boldsymbol{D}\boldsymbol{W}\boldsymbol{x} + \boldsymbol{\nu} \tag{39}$$

其中，$\boldsymbol{F} \in \mathbb{C}^{T_{\mathrm{E}} \times V}$ 是可重构智能表面到 Eve 的信道响应；$\boldsymbol{\nu}$ 表示 Eve 处的噪声，即 $\boldsymbol{\nu} \sim \mathcal{CN}(0, \gamma^2)$。我们假设 Alice 完全已知 $\boldsymbol{D}$、$\boldsymbol{q}$ 和 $\boldsymbol{h}$，而 Bob 对它们一无所知。[3] 此外，假设 Eve 完全了解 $\boldsymbol{G}$，并使用 $\boldsymbol{G}$进行最大似然检测。我们还假设 Eve 不知道 $\boldsymbol{F}$，原因有几方面。首先，可重构智能表面不会发射任何 Eve 能够检测到的公共信号。此外，

[2]为研究广义模型，我们考虑理想的可重构智能表面情形，即每个可重构智能表面单元的幅度和相位均可独立、连续地控制 [36]。此外，我们考虑无源可重构智能表面，即 $\rho_v \leqslant 1$, $v \in \mathcal{I}_V$。

[3]信道 $\boldsymbol{D}$ 和 $\boldsymbol{q}$ 可由 Alice 通过两阶段信道估计方法 [37]分别进行估计。即使 $\boldsymbol{D}$ 和 $\boldsymbol{q}$ 可能被不精确地估计为 $\boldsymbol{D}'$ 和 $\boldsymbol{q}'$，其中 $\boldsymbol{D}' = \boldsymbol{D}\boldsymbol{\Phi}$ 和 $\boldsymbol{q}' = \boldsymbol{\Phi}^{-1}\boldsymbol{q}$，且 $\boldsymbol{\Phi}$ 为满秩对角矩阵，建议的反射设计仍然有效，因为 $\boldsymbol{q}\boldsymbol{R}\boldsymbol{D} = \boldsymbol{q}'\boldsymbol{R}\boldsymbol{D}'$。更多信息请参阅 [37]。

可重构智能表面的反射系数会持续变化，这使 Eve 难以监测 $\boldsymbol{F}$。最后，可以采用保密信道估计技术 [38] 来保护与合法信道相关的信息。请注意，在可重构智能表面辅助的多天线系统中，Alice 每根天线上的发射信号与第III.C节和第III.D节中所述的相同。区别在于还需要对波束成形器和可重构智能表面进行额外的专门设计。

B. 波束成形器与*RIS*设计

本节提出一种波束成形器与RIS设计策略。当 Alice 与 Bob 之间存在直达链路时，(37) 可写为

$$y_1 = (\boldsymbol{h} + \boldsymbol{qRD})\,\boldsymbol{W}\boldsymbol{x} + \mu_1. \tag{40}$$

然后，在约束条件中

$$(\boldsymbol{h} + \boldsymbol{qRD})\,\boldsymbol{W} = \boldsymbol{I}_{T_\mathrm{A}} \tag{41}$$

其中 $\boldsymbol{I}_{T_\mathrm{A}} = \underbrace{[1, 1, \ldots, 1]}_{T_\mathrm{A}}$，我们有

$$y_1 = \sum_{t_\mathrm{A}=1}^{T_\mathrm{A}} x_{t_\mathrm{A}} + \mu_1. \tag{42}$$

考虑第 t_A 根天线的功率预算 Γ_{t_A}，RIS设计问题可表述为

$$\begin{aligned} \mathcal{P}2: \quad & \text{Find } \boldsymbol{R} && (43a)\\ & \text{s.t. } |w_{t_\mathrm{A}}|^2 \leqslant \Gamma_{t_\mathrm{A}}, \quad t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}} && (43b)\\ & \qquad \rho_v \leqslant 1, \quad v \in \mathcal{I}_V && (43c) \end{aligned}$$

其中

$$w_{t_\mathrm{A}} = \frac{1}{h_{t_\mathrm{A}} + \boldsymbol{qRD}_{:,t_\mathrm{A}}}, \quad t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}} \tag{44}$$

且$\boldsymbol{D}_{:,\ t_\mathrm{A}}$ 是矩阵 $\boldsymbol{D}$的第 t_A列。公式（44）由（41）推导得出。由于约束中包含相互耦合的项， $\mathcal{P}2$ 中的问题是非凸的。为求解 $\mathcal{P}2$中的问题，我们利用绝对值不等式变换（43b），得到

$$|\boldsymbol{qRD}_{:,t_\mathrm{A}}| \geqslant \frac{1}{\sqrt{\Gamma_{t_\mathrm{A}}}} - |h_{t_\mathrm{A}}|, \quad t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}}. \tag{45}$$

然后，我们将（45）放宽为关于实部的约束，并将$\mathcal{P}2$ 改写为

$$\begin{aligned} \mathcal{P}3\text{: 求 } & \boldsymbol{R} && (46a)\\ \text{s.t. } & \Re\{\boldsymbol{qRD}_{:,t_\mathrm{A}}\} \geqslant \frac{1}{\sqrt{\Gamma_{t_\mathrm{A}}}} - |h_{t_\mathrm{A}}|,\ t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}} && (46b)\\ & \rho_v \leqslant 1,\ v \in \mathcal{I}_V. && (46c) \end{aligned}$$

$\mathcal{P}3$ 中的问题是一个凸问题，可以使用 CVX 求解。请注意，尽管 CVX 可以求解未指定目标函数、仅定义约束的可行性问题，但求解过程并不涉及随机采样。相反，求解器会返回由优化器选定的确定性可行点，该点通常位于内部区域或边界区域，而非随机选取。

在非直连链路的情况下，约束需要改写为

$$\boldsymbol{qRDW} = \boldsymbol{I}_{T_\mathrm{A}} \tag{47}$$

可行性问题可表述为

$$\begin{aligned} \mathcal{P}4: \quad & \text{Find } \boldsymbol{R} && (48a)\\ & \text{s.t. } \Re\{\boldsymbol{qRD}_{:,t_\mathrm{A}}\} \geqslant \frac{1}{\sqrt{\Gamma_{t_\mathrm{A}}}}, \quad t_\mathrm{A} \in \mathcal{I}_{T_\mathrm{A}} && (48b)\\ & \qquad \rho_v \leqslant 1, \quad v \in \mathcal{I}_V && (48c) \end{aligned}$$

该问题也可以用 CVX 求解。因此，我们还有

$$y_2 = \sum_{t_\mathrm{A}=1}^{T_\mathrm{A}} x_{t_\mathrm{A}} + \mu_2. \tag{49}$$

注释*5*：与第三节讨论的传统多天线系统相比，可重构智能表面引入了乘性随机性 [39], ，这进一步使 Eve 无法获取任何有用信息。

五、数值结果

本节从误差性能和安全有效性两方面评估所提出的安全方案。主要发现如下。

观察***1***：在单天线系统中，所提出的低阶到高阶和高阶到低阶调制混淆方案均能有效防止 *Eve* 识别调制格式。此外，随着信噪比的提高，所提出的方案对调制分类的抵抗能力也有所增强（参见图4 和5）。

我们在单天线系统中评估所提出的调制阶数混淆方案的安全性。正确分类概率 P_c用作安全性能指标。由于所提出的方案需要定制发射机设计，我们没有使用公开可用的调制数据集，而是自行生成数据集。该数据集包含10种调制方案，即二进制频移键控、四进制频移键控、最小频移键控、高斯最小频移键控、二进制相移键控、四相相移键控、8PSK、16相移键控、16QAM和三十二进制正交幅度调制，滚降因子为0.35，过采样率为8。为模拟信道效应，我们对功率归一化后的样本施加随机相位旋转。在图4中，通过符号率调制将四相相移键控伪装成16QAM。所得符号集被划分为四个旋转对称子集。具体而言，原始四相相移键控中的每个符号都会映射到16QAM星座图指定象限内的一个随机符号。例如，符号 $1 + 0\jmath$ 被映射到映射子集 $\{1 + 1\jmath,\ 3 + 1\jmath,\ 1 + 3\jmath,\ 3 + 3\jmath\}$中的一个符号。在子图（a）中，映射概率为 $\boldsymbol{p} = [0, 0, 0, 1]$，这意味着伪装信号保留了4阶调制的特征，实际上并未发生调制混淆。因此，所有四种基于深度学习的分类器——VGG[18], SCGNet [19],WSMF [20], 和 ChainNet [21], ——都能准确识别调制格式，且分类性能随信噪比提高而改善。在子图（b）中，映射概率为 $\boldsymbol{p} = [0.1, 0.2, 0.3, 0.4]$，表明四相相移键控被部分映射为16阶调制，但星座点分布并不均匀。与子图（a）相比，分类性能

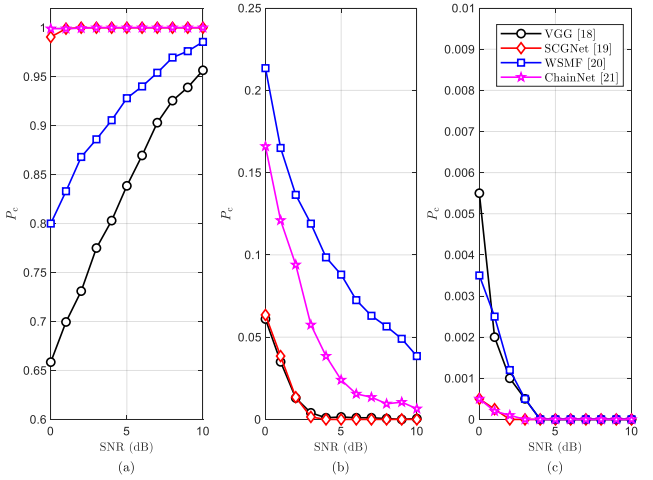

Fig. 4. 分类准确率是在 .r.信噪比下针对低-to-high-阶数混淆在单天线系统中的情况进行评估。在仿真中，QPSK 被伪装成 16 QAM。三个子图对应不同的符号映射概率，即 (a) $\boldsymbol{p} = [0, 0, 0, 1]$、(b) $\boldsymbol{p} = [0.1, 0.2, 0.3, 0.4]$ 和 (c) $\boldsymbol{p} = [0.25, 0.25, 0.25, 0.25]$。此外，我们假设 Eve 使用四种基于深度学习的调制分类器，即 VGG [18], SCGNet [19], WSMF [20], 和 ChainNet [21]。

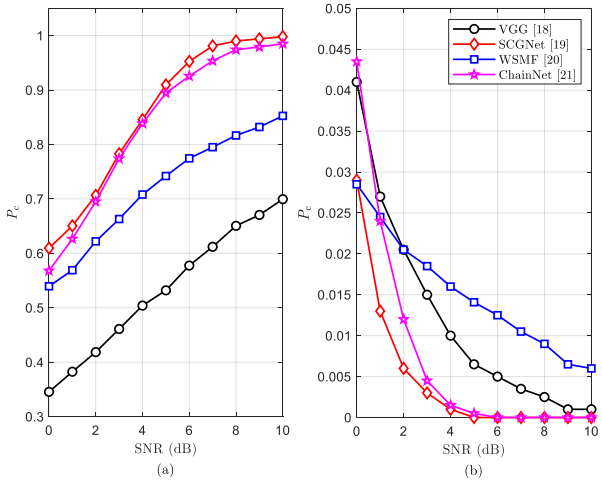

Fig. 5. 分类准确率随信噪比的变化 .r.高阶 -to-low-单天线系统中的阶数混淆。在仿真中，16相移键控被伪装为9GAM。两个子图分别对应调制混淆前后的情况，即(a)未进行混淆，(b)混淆后。这里还假设Eve分别采用VGG[18], SCGNet [19], WSMF [20], 和 ChainNet [21] 。

四种分类器的性能均明显下降，并且随着信噪比提高而进一步恶化。这是因为噪声功率降低时，伪装信号与典型四相相移键控模式之间的偏差会变得更加明显。在子图（c）中，映射概率为 $\boldsymbol{p} = [0.25, 0.25, 0.25, 0.25]$，这意味着伪装信号完全呈现出传统16QAM调制的特征。因此，分类器性能进一步恶化，分类准确率随着信噪比提高而降至零。这表明在这种情况下，Eve无法正确识别原始调制格式。在图5中，使用STD将16相移键控伪装成9GAM。在子图（a）中未应用阶数混淆，因此所有四种分类器均表现出正常的调制分类性能。在子图（b）中，分类器对伪装信号的分类准确率显著下降，且安全性能随信噪比提高而改善。

观察***2***：在单天线系统中，采用所提出的低阶到高阶调制阶数混淆方案时，*Bob* 处的误码率介于原始低阶调制和目标高阶调制的误码率之间。此外，误码率性能还受符号映射概率的影响（参见图 6）。

在图6中，我们模拟了单天线系统中 Bob 将四相相移键控伪装为 16QAM 时的误码率性能。符号映射遵循观察***1***中定义的相同规则。正如预期，由于调制阶数提高，伪装信号的误码率性能比原始低阶调制更差。然而，伪装信号的性能始终优于目标高阶调制。这是因为即使噪声导致符号错误，被误判的符号仍可能落在与正确符号相同的映射子集中，因此不会影响最终的解映射结果。此外，我们观察到 Eve 在不同符号映射概率下的误码率性能略有差异。这是由于噪声对映射后的 16QAM 星座图中各星座点的抗噪能力不同，而这种差异受其在星座空间中的相对位置影响。

观察***3***：在单天线系统中，所提出的高阶到低阶调制阶数混淆方案在高信噪比下可显著提升误码率性能（参见图7）。

在图7中，我们采用STD将16相移键控和8PSK分别伪装为9GAM和5进制广义幅度调制，每帧包含10个原始调制符号。与原始高阶调制相比，系统在高信噪比下的误码率性能显著提升。这一改善归因于两个因素。首先，较低的调制阶数增强了抗噪能力。其次，所提出的动态规划解调器通过联合解码一帧中的全部10个符号，提供了纠错能力，从而提升性能。然而，在低信噪比下，由于严重的噪声引发错误传播，削弱了动态规划解调器的有效性，伪装信号的误码率性能相比原始高阶调制有所下降。

观察***4***：在多天线系统中，基于泰勒级数的混淆方案只需消除 $f(s)$ 展开中的前6 个非线性项，*Bob* 就能成功恢复原始信号（参见图8）。

在图8中，我们选择非线性函数 $f(s)$ =反正切(s)，并为每根天线分配一个泰勒级数中的非线性项以将其消除。首先，不同调制方案下的结果表明，随着 T_{A} 增加，Bob 的误码率性能会提升。这是因为更大的 T_{A} 可以消除泰勒级数中更多的非线性干扰项，从而提高信号恢复的准确性。此外，通过比较不同调制方案下的误码率性能，我们发现，对于四相相移键控， T_{A} 对误码率的影响相对较小，低于高阶调制。这是因为诸如

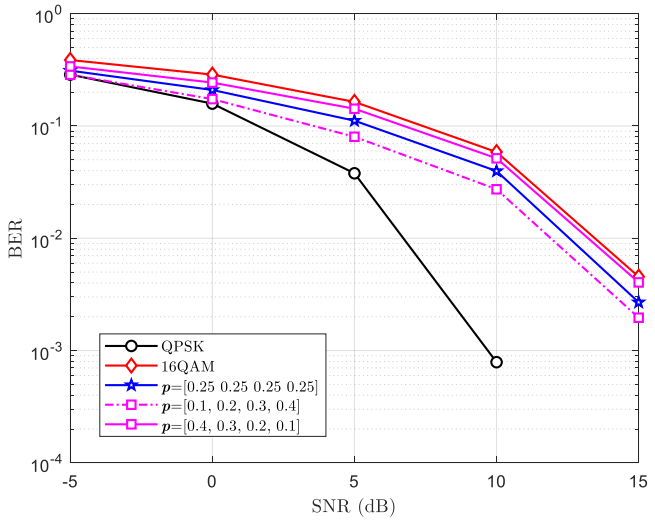

图6. 在单天线系统中，评估低阶到高阶混淆时 Bob 的误码率随信噪比的变化情况。仿真中，四相相移键控被伪装为16QAM。我们在两种不同的符号映射概率 $\boldsymbol{p} = [0.1, 0.2, 0.3, 0.4]$ 和 $\boldsymbol{p} = [0.25, 0.25, 0.25, 0.25]$下仿真误码率。我们还仿真了四相相移键控和16QAM的误码率，作为比较基准。

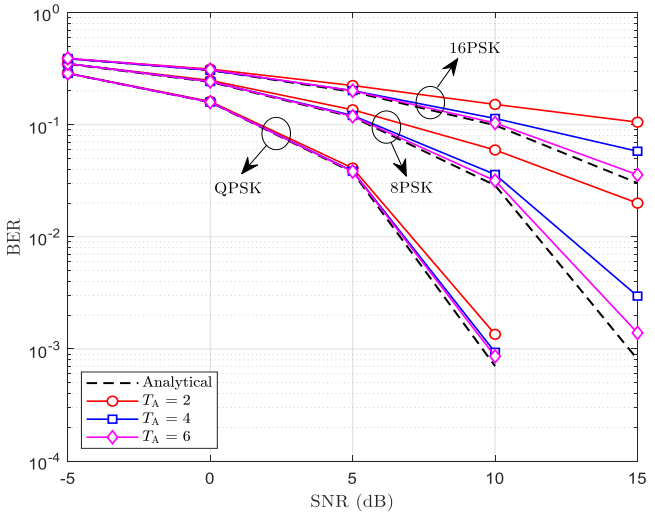

图 8. 在多天线系统中，针对低阶到高阶混淆，评估 Bob 的误码率随信噪比的变化。在仿真中，我们采用基于泰勒展开的混淆方案，且非线性函数为 $f(s) =$ 反正切 s。 $f(s)$ 的泰勒展开中的非线性项数量设为 $T_A - 1$。

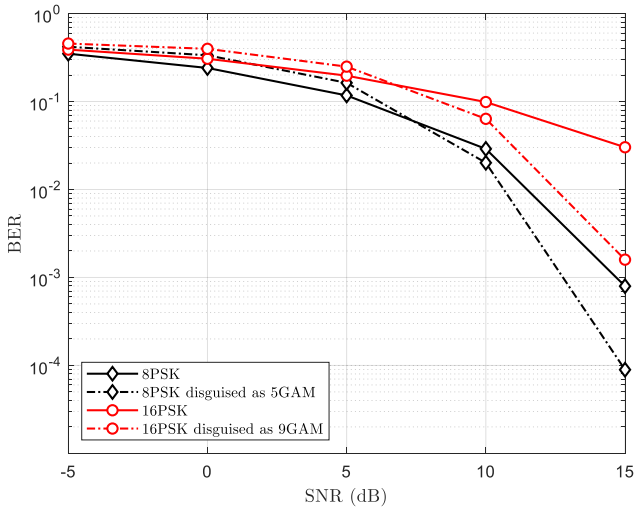

图7. 在单天线系统中，评估高阶到低阶混淆时 Bob 的误码率随信噪比的变化情况。仿真中，16相移键控被伪装为9GAM，8PSK被伪装为5进制广义幅度调制。每帧包含10个原始调制符号。我们还仿真了传统16PSK和8PSK的误码率，作为比较基准。

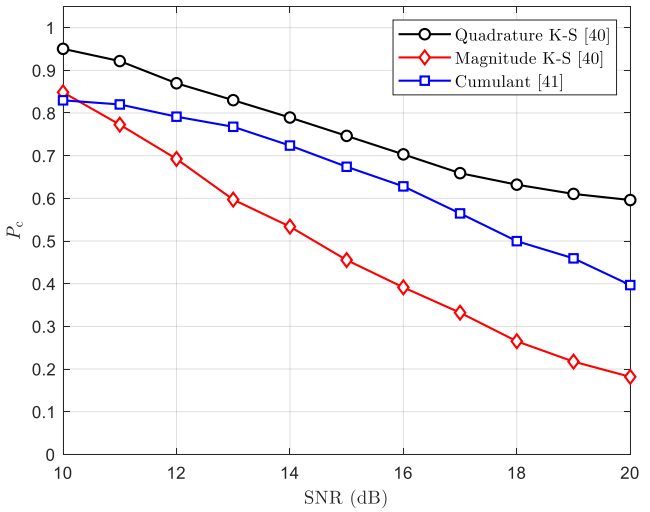

图 9. 在多天线系统中，针对高阶到低阶混淆，评估分类准确率随信噪比的变化。在仿真中，16QAM 被伪装成 4QAM。我们假设 Eve 部署了三种基于专家知识的分类器，即正交 K-S 分类器 [40], 幅度 K-S 分类器 [40], 和基于累积量的分类器 [41]。

$f(s)$ = 反正切(s)之类的非线性变换对低阶调制的稀疏星座影响有限。然而，对于高阶调制，星座包含许多均匀分布的符号，一些非线性变换可能会严重破坏原始布局，因此需要消除大量干扰项才能恢复原始分布。此外，当 $T_A = 6$时（对应于消除 6 个非线性项），Bob 的误码率接近理想情况。尽管将 T_A 增加到 6 以上可以进一步提升误码率性能并增强混淆效果，但也会导致计算复杂度升高。

观察***5***：在多天线系统中，即使 *Eve* 通过盲源分离成功提取出 *Alice* 每根天线上的信号，所提出的安全方案仍能有效阻止其识别出正确的调制格式（参见图 9）。

在图9中，我们模拟了所提出的多天线系统中高阶到低阶调制混淆方案的抗调制分类性能。候选调制集合包括4QAM和16QAM。Alice使用3根天线，按照图2所示的CPD方案，将16QAM伪装成4QAM。Eve同样配备了3

根天线，并应用快速独立成分分析 [42]进行盲源分离，以恢复来自Alice各根天线的信号，并尝试分别识别其调制类型。为了更全面地评估我们方案的鲁棒性，并区别于观察***1***，我们假设Eve采用三种基于专家知识的分类器，即正交 K-S 分类器 [40], 幅度 K-S 分类器[40],和基于累积量的分类器 [41]。候选调制集合定义为16QAM和4QAM。Eve对每个分离出的信号分别进行调制分类，并记录正确分类率。结果表明，所提出的方案能够有效阻止三种分类器进行调制分类。与基于深度学习的分类器类似，随着信噪比的增加，混淆性能得到提升。

VI. 结论

本文提出了一种基于调制阶数混淆的安全通信方法，通过阻止 Eve 正确识别合法调制格式来确保安全性。针对单天线情形，我们提出了两种调制阶数混淆方案：符号随机映射方案将低阶调制伪装成高阶调制，而符号时间分集方案则将高阶调制伪装成低阶调制。针对多天线系统，我们采用基于级数展开的方案或星座路径设计方案来设计发射信号。仿真结果表明，所提出的方案能够有效抵御 Eve 在单天线和多天线系统中的调制分类，包括基于深度学习和专家知识的分类器。此外，随着信噪比的提高，抗分类性能也会提升。在单天线系统中，符号随机映射方案的误码率受映射概率影响，而符号时间分集方案在高信噪比下能够带来误码率增益。在多天线系统中，对于基于级数展开的方案，建议在展开中使用前 6 项，以平衡计算复杂度和误差性能。此外，即使 Eve 成功进行盲源分离，并提取出 Alice 的每根天线发出的信号，也无法识别真实的调制格式。与现有的安全通信和抗调制分类技术相比，所提出的方法无需了解 Eve 的任何信息。该方法还赋予用户灵活性，可将原始信号伪装成高阶或低阶调制，从而实现通信可靠性与安全性之间的可调平衡。

附录 引理 1 的证明

调制混淆后，映射概率为 $\boldsymbol{p}_m,\quad m\in\mathcal{I}_M$ 时的符号分布 $P_{\text{ob}}(b_n)$ 为

$$P_{\text{ob}}(b_n)=\sum_{m=1}^{M}P(a_m)P(b_n|a_m) \tag{50}$$

其中

$$P(a_m)=\frac{1}{M} \tag{51}$$

$$P(b_n|a_m)=\begin{cases}p_i^{(m)},\text{if } b_n \text{ is the } i\text{th symbol of } \mathcal{B}_m\\ 0,\text{otherwise.}\end{cases} \tag{52}$$

待混淆的目标调制格式的理想符号分布 $P_{\text{id}}(b_n)$ 为

$$P_{\text{id}}(b_n)=\frac{1}{N}. \tag{53}$$

分布 P_{ob} 和 P_{id} 之间的 KL 散度为

$$D_{\text{KL}}(P_{\text{ob}}||P_{\text{id}})=\sum_{n=1}^{N}P_{\text{ob}}(b_n)\log\frac{P_{\text{ob}}(b_n)}{P_{\text{id}}(b_n)} \tag{54}$$

$$=\sum_{m=1}^{M}\sum_{i=1}^{K}\frac{1}{M}p_i^{(m)}\log N\frac{1}{M}p_i^{(m)} \tag{55}$$

$$=\sum_{m=1}^{M}\sum_{i=1}^{K}\frac{1}{M}p_i^{(m)}\left(\log K+\log p_i^{(m)}\right) \tag{56}$$

$$=\log K+\frac{1}{M}\sum_{m=1}^{M}\sum_{i=1}^{K}p_i^{(m)}\log p_i^{(m)} \tag{57}$$

$$=\log K-\frac{1}{M}\sum_{m=1}^{M}H(\boldsymbol{p}_m). \tag{58}$$

然后，令 $\mathcal{B}_m=\mathcal{B}\setminus\mathcal{B}_m,\quad m\in\mathcal{I}_M$ 表示 $\mathcal{B}_m$ 的补集，记为

$$\bar{\mathcal{B}}_m=\left\{\bar{b}_1^{(m)},\bar{b}_2^{(m)},\ldots,\bar{b}_{N-K}^{(m)}\right\},\ m\in\mathcal{I}_M. \tag{59}$$

根据联合界技术，ϑ 可以近似表示为

$$\vartheta=\frac{1}{M\log M}\sum_{m=1}^{M}\sum_{i=1}^{K}p_i^{(m)}\sum_{j=1}^{N-K}\rho_{i,j}^{(m)}p\left(b_i^{(m)}\to\bar{b}_j^{(m)}\right) \tag{60}$$

$$=\frac{1}{M\log M}\sum_{m=1}^{M}\sum_{i=1}^{K}p_i^{(m)}\sum_{j=1}^{N-K}\rho_{i,j}^{(m)}Q\left(\frac{\Delta_{i,j}^{(m)}}{\sqrt{2}\sigma}\right) \tag{61}$$

其中，$\rho_{i,j}^{(m)}$ 表示 $b_i^{(m)}$ 与 $\bar{b}_j^{(m)}$ 之间码字的汉明距离，$\Delta_{i,j}^{(m)}=\left|b_i^{(m)}-\bar{b}_j^{(m)}\right|$，$Q(\cdot)$是高斯 Q函数。

参考文献

[1] V.-L. Nguyen、P.-C. Lin、B.-C. Cheng、R.-H. Hwang 和 Y.-D. Lin，“6G 的安全与隐私：前瞻性技术与挑战综述”，IEEE 通信调查与教程，第 23 卷，第 4 期，第 2384–2428 页，2021 年第四季度。[2] Y. Zou、J. Zhu、X. Wang 和 L. Hanzo，“无线安全综述：技术挑战、最新进展与未来趋势”，《IEEE 论文集》，第 104 卷，第 9 期，第 1727–1765 页，2016 年 9 月。[3] P. Angueira、I. Val、J. Montalban、 ´O. Seijo、E. Iradier、P. S. Fontaneda、L. Fanari 和 A. Arriola，“工业安全无线通信物理层技术综述”，IEEE 通信调查与教程，第 24 卷，第 2 期，第 810–838 页，2022 年第二季度。[4] F. Jameel、S. Wyne、G. Kaddoum 和 T. Q. Duong，“物理层安全的协作中继与干扰策略综合综述”，IEEE 通信调查与教程，第 21 卷，第 3 期，第 2734–2771 页，2018 年第三季度。[5] M. Bloch、J. Barros、M. R. Rodrigues 和 S. W. McLaughlin，“无线信息论安全”，IEEE 信息论汇刊，第 54 卷，第 6 期，第 2515–2534 页，2008 年 6 月。[6] S. Goel 和 R. Negi，“利用人工噪声保障保密性”，IEEE 无线通信汇刊，第 7 卷，第 6 期，第 2180–2189 页，2008 年 6 月。[7] C.-Y. Huan 和 A. Polydoros，“MPSK 调制分类的似然方法”，IEEE 通信汇刊，第 43 卷，第 2/3/4 期，第 1493–1504 页，1995 年 2 月。[8] T. Yucek 和 H. Arslan，“一种用于自适应 OFDM 系统的新型次优最大似然调制分类算法”，载于《2004 年 IEEE 无线通信与网络会议（WCNC）论文集》，第 2 卷，2004 年 7 月，第 739–744 页。[9] D. Zhu 、 V. J. Mathews 和 D. H. Detienne，“一种基于似然的 QAM 和 PSK 信号盲识别算法”，IEEE 无线通信汇刊，第 17 卷，第 5 期，第 3417–3430 页，2018 年 5 月。[10] W. Wei 和 J. M. Mendel，“数字幅相调制的最大似然分类”，IEEE 通信汇刊，第 48 卷，第 2 期，第 189–193 页，2000 年 2 月。[11] A. Swami 和 B. M. Sadler，“利用累积量进行分层数字调制分类”，IEEE 通信汇刊，第 48 卷，第 3 期，第 416–429 页，2000 年 3 月。[12] H.-C. Wu、M. Saquib 和 Z. Yun，“一种针对多径信道通信、利用累积量特征的新型自动调制分类方法”，IEEE 无线通信汇刊，第 7 卷，第 8 期，第 3098–3105 页，2008 年 8 月。[13] D.-C. Chang 和 P.-K. Shih，“基于累积量的多径衰落信道调制分类技术”，IET 通信，第 9 卷，第 6 期，第 828–835 页，2015 年 4 月。[14] O. A. Dobre、Y. Bar-Ness 和 W. Su，“一种基于循环累积量的稳健 QAM 调制分类算法”，载于《2004 年 IEEE 无线通信与网络会议（WCNC）论文集》，第 2 卷，2004 年 3 月，第 745–748 页。[15] O. A. Dobre、A. Abdi、Y. Bar-Ness 和 W. Su，“平坦衰落信道中线性数字调制的基于循环平稳性的调制分类”，《无线个人通信》，第 54 卷，第 4 期，第 699–717 页，2010 年。[16] C.-S. Park、J.-H. Choi、S.-P. Nah、W. Jang 和 D. Y. Kim，“利用小波特征和支持向量机对数字信号进行自动调制识别”，载于《国际先进通信技术会议论文集》，第 1 卷，2008 年，第 387–390 页。[17] T. J. O’Shea 和 J. Hoydis，“物理层深度学习导论”，IEEE 认知通信与网络汇刊，第 3 卷，第 4 期，第 563–575 页，2017 年 12 月。[18] T. J. O’Shea、T. Roy 和 T. C. Clancy，“基于空中传输深度学习的无线电信号分类”，IEEE 信号处理精选主题期刊，第 12 卷，第 1 期，第 168–179 页，2018 年 1 月。[19] G. B. Tunze、T. Huynh-The、J.-M. Lee 和 D.-S. Kim，“用于高效自动调制识别的稀疏连接卷积神经网络”，IEEE车辆技术汇刊，第 69 卷，第 12 期，第 15 557–15 568 页，2020 年 12 月。[20] P. Qi、X. Zhou、S. Zheng 和 Z. Li，“基于融合多模态信息的深度残差网络的自动调制分类”，IEEE 认知通信与网络汇刊，第 7 卷，第 1 期，第 21–33 页，2021 年 3 月。

[21] T. Huynh-The、V.-S. Doan、C.-H. Hua、Q.-V. Pham 和 D.-S. Kim，《Chain-net：针对合成信道损伤下调制分类的深度模型学习》，载于 IEEE全球通信会议（GLOBECOM）论文集，2020年12月，第1–6页。[22] J. N. Njoku、M. E. Morocho-Cayamcela 和 W. Lim，《CGDNet：用于鲁棒自动调制识别的高效混合深度学习模型》，《IEEE网络快报》，第3卷，第2期，第47–51页，2021年6月。[23] V. Choqueuse、S. Azou、K. Yao、L. Collin 和 G. Burel，《MIMO系统的盲调制识别》，《MTA Review》，第19卷，第2期，第183–196页，2009年6月。[24] Z. Zhu 和 A. K. Nandi，《使用期望最大化的MIMO系统盲调制分类》，载于 IEEE MILCOM 论文集，美国马里兰州巴尔的摩，2014年，第754–759页。[25] X. Liu、C. Zhao、P. Wang、Y. Zhang 和 T. Yang，《基于机器学习的空间相关MIMO系统盲调制分类算法》，《IET Commun.》，第11卷，第7期，第1000–1007页，2017年5月。[26] K. Hassan、I. Dayoub、W. Hamouda、C. N. Nzeza 和 M. Berbineau，《空间相关MIMO系统的盲数字调制识别》，《IEEE Trans. Wireless Commun.》，第11卷，第2期，第683–693页，2011年2月。[27] S. Althunibat、V. Sucasas 和 J. Rodriguez，《一种基于相位的自适应调制物理层安全方案》，《IEEE Trans. Veh. Technol.》，第66卷，第11期，第9931–9942页，2017年11月。[28] I. Bang 和 T. Kim，《基于OFDM的TDD系统中利用星座映射混淆实现的安全调制》，《IEEE Access》，第8卷，第197 644–197 653页，2020年11月。[29] M. Sadeghi 和 E. G. Larsson，《针对基于深度学习的无线电信号分类的对抗攻击》，《IEEE无线通信快报》，第8卷，第1期，第213–216页，2018年2月。[30] Y. Lin、H. Zhao、X. Ma、Y. Tu 和 M. Wang，《利用卷积神经网络进行调制识别时的对抗攻击》，《IEEE Trans. Rel.》，第70卷，第1期，第389–401页，2021年3月。[31] B. Kim、Y. E. Sagduyu、K. Davaslioglu、T. Erpek 和 S. Ulukus，《针对深度学习无线信号分类器的信道感知对抗攻击》，《IEEE Trans. Wireless Commun.》，第21卷，第6期，第3868–3880页，2022年6月。[32] B. He 和 F. Wang，《针对深度学习方法的抗调制分类发射机设计》，《IEEE Trans. Wireless Commun.》，第23卷，第7期，第6808–6823页，2024年7月。[33] M. Grant、S. Boyd 和 Y. Ye，《CVX：用于规范凸编程的Matlab软件》，2009年。[34] P. Larsson，《黄金角调制》，《IEEE无线通信快报》，第7卷，第1期，第98–101页，2017年9月。[35] J. Wang、F. Wang、B. He 和 J. Luo，《通过非线性发射与协作中继实现安全通信》，《IEEE Trans. Commun.》，2025年。[36] Zheng 等，《利用幅度可调超表面实现超宽带旁瓣电平抑制》，《J. Phys. D: Appl. Phys.》，第52卷，第6期，第065102页，2018年12月。[37] Z.-Q. He 和 X. Yuan，《大型智能超表面辅助大规模MIMO的级联信道估计》，《IEEE无线通信快报》，第9卷，第2期，第210–214页，2020年2月。[38] S. Yan、X. Zhou、N. Yang、T. D. Abhayapala 和 A. L. Swindlehurst，《利用全双工接收机进行秘密信道训练以增强物理层安全》，《IEEE信息取证与安全汇刊》，第13卷，第11期，第2788–2800页，2018年11月。[39] J. Luo、F. Wang、S. Wang、H. Wang 和 D. Wang，《可重构智能表面：针对被动窃听的反射设计》，《IEEE Trans. Wireless Commun.》，第20卷，第5期，第3350–3364页，2021年5月。[40] F. Wang 和 X. Wang，《通过Kolmogorov-Smirnov检验实现快速、鲁棒的调制分类》，《IEEE Trans. Commun.》，第58卷，第8期，第2324–2332页，2010年8月。[41] A. Swami 和 B. M. Sadler，《利用累积量进行分层数字调制分类》，《IEEE Trans. Commun.》，第48卷，第3期，第416–429页，2000年3月。[42] A. Hyv¨arinen 和 E. Oja，《独立成分分析：算法与应用》，《Neural Netw.》，第13卷，第4–5期，第411–430页，2000年6月。