面向知情窃听者的安全通感一体化波形随机化

Zexin Fang*、Bin Han*、Shuangyang Li†和Hans D. Schotten*‡
*凯泽斯劳滕-兰道莱茵兰-普法尔茨工业大学， †柏林工业大学，
‡德国人工智能研究中心（DFKI），德国

arXiv:2611.32506v1 [eess.SP] 24 Nov 2026

摘要—**我们研究了通感一体化（ISAC）的波形级保护问题，目标是防御一名了解波形构造和相位密钥生成规则的无人机搭载的窃听者（Eve）。本文的创新在于开展了系统且明确计算预算的攻击分析：我们不依赖未公开的设计细节，而是量化知情窃听者 Eve能够学习和重构的内容，以及所需的计算量。我们采用傅里叶曲线调制、相位密钥和切向人工噪声（AN）保护感知参考信号，并通过安全回传链路共享突发特定信息。针对完整或部分名义序列知识，我们比较了三种相位密钥生成规则，以应对基于离线卷积神经网络（CNN）的序列识别，以及在线Adam和相位感知期望最大化（EM）密钥恢复。功率域模型将残余密钥误差与不完全人工噪声消除联系起来，并预测相干时延锁定。结果表明：可复用的密钥结构即使在解调失败时仍允许进行序列识别；位置相关的密钥生成提高了恢复难度；而种子扩展密钥生成规则能在给定学习预算内抵抗所评估的分类器。在多径、杂波和回波累积条件下进行的波形仿真进一步证实了其对感知性能的影响。**

索引词—人工噪声、通感一体化、5G-Advanced、6G、安全性。

I. 引言

一体化感知与通信（通感一体化）通过共享资源和硬件集成数据传输与环境感知，为下一代网络带来更高的频谱效率和更低的部署成本 [1]。然而，支持合法感知的同一组发射信号也可能将环境信息暴露给非预期接收机 [2], [3]。许多通感一体化系统会复用导频或其他已知参考信号进行感知。这些信号可被授权通信用户访问，也可能被系统外部的窃听者截获。这可能进一步使任一接收机执行未授权检测、定位或跟踪 [4]。

另一项威胁是被动直达波-回波旁路感知：Eve 在不了解信号结构的情况下，将截获的直达路径信号与目标反射信号进行相关处理。利用非合作照射源进行此类感知已在无源雷达中得到充分研究，包括性能分析以及实验检测和跟踪 [5], [6]。然而，其性能对参考信道质量以及监视信道中的干扰高度敏感 [7]。在城市环境中，并发传输产生的杂波和背景无线电干扰还会进一步降低回波检测性能。对于移动接收机而言，信道不平衡也会使直达路径与杂波抑制变得更加复杂 [8]，，而采样时钟失配则会降低参考信号对齐性能 [9]。被动直达波-回波旁路感知已得到充分研究，但其性能取决于参考信号质量和监视信道干扰。相较之下，我们关注研究较少的知情相干感知攻击，在此类攻击中，Eve 利用名义参考信号知识重构相干参考信号。

感知安全研究借鉴了成熟的物理层安全（PLS）工具，包括波束成形和人工噪声（AN） [10], [11]。这些设计旨在限制未授权接收机可获取的目标及环境信息，同时保持合法感知性能。Zou 等人 [4] 考虑一名充当感知窃听者的通信用户，并设计结合人工噪声的波束成形，在保持合法感知和通信质量的同时限制其感知互信息。Ren 等人 [12] 将联合保护扩展至无蜂窝一体化感知与通信，针对感知窃听者优化协作信息和感知波束成形。联合信号扰动与波束成形同样旨在实现感知信号不可区分性 [13]。Papanikolaou 等人 [14] 设计鲁棒发射协方差，以在窃听者角度不确定性下误导未授权角度感知。然而，空间保护通常需要窃听者的信道或位置信息，或预先指定的不确定性区域。对于被动移动窃听者而言，获取并维护这些信息颇具挑战。一旦空间分离条件不利，这些空间域和协方差域设计便促使研究转向波形级保护。搭载于无人机（UAV）上的窃听者可以重新调整位置，以寻求强视距（LOS）链路，并截获原本用于合法节点的能量；因此，应当对保护性能进行评估

在有利的截获几何关系下。

波形域方法会改变未授权感知接收机可获得的信号，从而在无需了解 Eve 的几何位置、也不依赖空间分离的情况下提供保护。Han 等人 [15] 设计模糊函数以引入人工目标，并增大 Eve 的距离模糊。Du 等人 [16] 提出一种面向检测的 Kullback–Leibler 散度度量，该度量计入主瓣、旁瓣和噪声的贡献，并优化时频幅度与相位扰动。他们的分析将波形整形与感知安全与通信权衡联系起来。Erdem 等人 [17]引入人工相位和多普勒频移，用于被动正交频分复用（OFDM）感知保护，并通过测量验证了协作补偿。Temiz 等人 [18] 将

索引调制与相位编码应用于调频连续波啁啾信号，以削弱未授权检测和测距。Zhang 等人 [19] 则利用环境中的物联网（IoT）设备作为协作干扰器和虚假目标，联合设计发射波束成形与设备反射调制。Keskin 等人 [20] 研究振荡器相位噪声，表明单基地与双基地接收中不同的相位噪声相关性会在合法测距、未授权测距和通信性能之间形成权衡。与生成的相位密钥不同，该机制利用的是振荡器引起的不对称性。这些方法表明，未授权检测与估计可以通过波形操控而非仅靠空间抑制来削弱。

然而，面对知情窃听者 Eve，波形域保护面临两种威胁。首先，Eve 可能估计并补偿波形修改。在通感一体化中，一种应对策略是将感知参考信号伪装在通信信号中。[21] 中的相位密钥和人工噪声可以阻止 Eve 正确解调，从而妨碍她识别受保护信号中相似的底层比特序列结构，以进行相干感知。其次，如果 Eve 了解安全设计和参考信号的生成方式，她可能利用经过专门训练的机器学习模型绕过保护。这种风险尚未得到充分研究，而且正变得日益重要。现有的波形域保护 [15]–[20]是在 Eve 不掌握保护参数的情况下进行评估的；而在 [17], 中，则是在单一测量场景下，针对单个启发式相位跟踪型窃听者 Eve 进行评估。因此，安全性不应仅依赖于未公开的设计细节或估计复杂度。我们分析了在波形构造和密钥生成规则已知时 Eve 能够学习和重建什么；保密性仅依赖于通过安全回传链路共享的突发专用密钥。

我们考虑一个 OFDM 通感一体化系统，该系统面临一名具有有利截获几何关系的搭载于无人机上的窃听者 Eve。系统可以切换调制阶数：在信令等低速率关键通信和感知中使用正交相移键控（QPSK），在高速率通信中使用高阶调制，这与新空口（NR）的调制灵活性一致 [22], [23]。协同基站（BS）通过安全回传链路共享感知调度、标称序列种子和密钥，从而实现参考信号重构和相干感知。通信域密钥与感知域密钥相互分离，以防止获取通信权限导致感知参考信号泄露。本文扩展了我们关于相位加密傅里叶曲线波形保护的会议论文工作 [24]。本文的贡献如下：

- **保护框架**。 我们采用双层设计，将傅里叶曲线调制、切向人工噪声和相位加密相结合，在保留合法通信与感知功能的同时，隐藏序列身份并保护相干参考信号重构。该设计能够阻碍序列识别，并在标称序列暴露时阻止直接提取密钥。

- **面向攻击的密钥分析**。我们评估了三种密钥生成规则（共享、平滑的位置相关和种子扩展），并针对一系列逐步升级的知情 Eve 攻击进行测试：盲跨突发相关、基于卷积神经网络 (CNN) 的离线根标识，以及在线 Adam 和阶段感知期望最大化 (EM) 密钥恢复。我们报告在掌握完整和部分名义序列知识时的恢复准确率和计算成本。

- **泄漏到感知的分析**。 我们揭示了 QPSK 特定谐波泄漏，推导了用于序列定位的符号一致概率，并建立了一个功率域模型，将残余密钥误差与不完美的人工噪声消除联系起来，预测正确时延锁定；同时通过多径、杂波和回波累积条件下的波形仿真对其进行了验证。

与会议版本相比 [24],该版本引入了相位加密的傅里叶曲线波形保护，本文进行了以下补充：

1）将单一密钥模型替换为共享密钥、平滑的位置依赖密钥和种子扩展密钥在基于 CNN 的序列识别下的对比。2）增加了在线密钥恢复攻击（Adam 和具有相位感知能力的 EM），涵盖完整或部分标称序列知识，以及有无谐波结构初始化的情况，并比较了不同计算预算下的检测准确率和密钥恢复准确率。3）从符号错误率（SER）推导符号一致概率，以刻画序列定位；同时增加了一个功率域模型，将相位密钥失配与残余切向人工噪声和相干时延锁定联系起来，并通过使用不完美密钥及人工噪声估计的协同合法接收机与 Eve 进行比较，在波形级别对其进行了评估。

本文其余部分安排如下。第二节介绍安全通信与感知模型。第三节介绍威胁模型、密钥生成规则、推理攻击和检测度量指标。第四节报告数值结果，第五节总结全文。

II. 安全通信与感知模型

A. 傅里叶曲线调制器

设 $M = 2^q$。每组 q 个编码比特选择一个索引 $i \in \{0, \dots, M-1\}$，并将其映射为一个阶段

$$\theta_i = \frac{2\pi i}{M}. \tag{1}$$

不同于传统 M- PSK 中对单一阶段进行调制的方法，我们使用 θ_i 生成一个 k维码字，其分量是同一角度的谐波，

$$\boldsymbol{x}_i = \frac{1}{\sqrt{k}} \left[e^{j\theta_i} \quad e^{j2\theta_i} \quad \cdots \quad e^{jk\theta_i} \right]^{\mathsf{T}}, \qquad \|\boldsymbol{x}_i\| = 1. \tag{2}$$

对于 $k > M$，谐波相位 $m\theta_i$ 以 2π 为模回绕，并在各分量之间循环重复。这些 k 分量由 i确定，并可根据物理实现映射到并行子载波、正交信令维度或连续资源元素。

对 $\boldsymbol{x}_i$ 关于 θ_i 求导，可以追踪随着 i变化时代码字曲线的局部方向，

$$\boldsymbol{x}'(\theta_i) = \frac{j}{\sqrt{k}} \left[e^{j\theta_i} \quad 2e^{j2\theta_i} \quad \cdots \quad k e^{jk\theta_i} \right]^{\mathsf{T}}. \tag{3}$$

将其按范数归一化，

$$v_k = \sqrt{\frac{1}{k} \sum_{\ell=1}^{k} \ell^2}, \tag{4}$$

即可得到 $\boldsymbol{x}_i$ 处的单位切向量，

$$\hat{\boldsymbol{t}}_i = \frac{\boldsymbol{x}'(\theta_i)}{v_k}, \qquad \|\hat{\boldsymbol{t}}_i\| = 1. \tag{5}$$

该切向量与码字本身正交，即在实嵌入 $\mathbb{R}^{2k}$中满足 $\Re\{\boldsymbol{x}_i^{\mathsf{H}} \hat{\boldsymbol{t}}_i\} = 0$。

B. 切向人工噪声与信道

在注入人工噪声之前，发射机在各个 k 谐波分量之间应用共享的阶段密钥向量 $\boldsymbol{\varphi} = [\varphi_1, \ldots, \varphi_k]^{\mathsf{T}}$，从而得到加密傅里叶曲线码字

$$\boldsymbol{x}_i(\boldsymbol{\varphi}) = \frac{1}{\sqrt{k}} \left[e^{j(\theta_i + \varphi_1)} \quad e^{j(2\theta_i + \varphi_2)} \quad \cdots \quad e^{j(k\theta_i + \varphi_k)} \right]^{\mathsf{T}}. \tag{6}$$

通过对 $\boldsymbol{x}_i(\boldsymbol{\varphi})$关于 θ_i 求导，可得到加密切向量 $\hat{\boldsymbol{t}}_i(\boldsymbol{\varphi})$。合法接收机知道 $\boldsymbol{\varphi}$，并直接构建加密码本；而不具备该密钥的非预期接收机即使在未考虑人工噪声之前，也会面临几何失配。

对于码字 r，发射机抽取一个实数 $\xi_r \sim \mathcal{N}(0, 1)$，并在 k 个谐波分量之间共享，然后构造

$$\boldsymbol{x}_{i,r}^{\mathrm{tx}} = \sqrt{1-\beta}\, \boldsymbol{x}_i(\boldsymbol{\varphi}) + \sqrt{\beta}\, \xi_r \hat{\boldsymbol{t}}_i(\boldsymbol{\varphi}), \qquad 0 \le \beta < 1. \tag{7}$$

对于固定的 i，切向量是确定的，而幅度ξ_r 按码字独立抽取，而非按分量抽取。由于 $\boldsymbol{x}_i(\boldsymbol{\varphi})$和$\hat{\boldsymbol{t}}_i(\boldsymbol{\varphi})$是单位范数且相互正交，

$$\mathbb{E}\big[\|\boldsymbol{x}_{i,r}^{\mathrm{tx}}\|^2\big] = 1. \tag{8}$$

经过同步和信道均衡后，实值接收码字为

$$\boldsymbol{Y}_r = \sqrt{1-\beta}\, \boldsymbol{x}_i(\boldsymbol{\varphi}) + \sqrt{\beta}\, \xi_r \hat{\boldsymbol{t}}_i(\boldsymbol{\varphi}) + \boldsymbol{N}_r, \tag{9}$$

其中 $\boldsymbol{Y}_r, \boldsymbol{x}_i, \hat{\boldsymbol{t}}_i, \boldsymbol{N}_r \in \mathbb{R}^{2k}$和 $\boldsymbol{N}_r \sim \mathcal{N}(\boldsymbol{0}, \sigma_c^2 \boldsymbol{I}_{2k})$，其中 σ_c^2 是每个实分量的噪声方差。

*C. QPSK*感知波形设计

我们考虑QPSK相位序列

$$s[n] = e^{j\theta_n}, \ \theta_n \in \left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}, \ n = 0, \ldots, N-1. \tag{10}$$

在 k次谐波傅里叶构造中，每个感知符号$s[n]$ 映射为 k分量子载波权重码字

$$\boldsymbol{u}_k[n] = \frac{1}{\sqrt{k}} \left[e^{j\theta_n}, e^{j2\theta_n}, \ldots, e^{jk\theta_n} \right]^{\mathsf{T}}. \tag{11}$$

算法1 固定条件下的 QPSK 谐波波形设计 k

1: 选择 N、k、重启次数 R、扫描次数 S；定义 $\mathcal{Q} = \{0, \pi/2, \pi, 3\pi/2\}$ 和目标函数 $J_k(\boldsymbol{\theta})$，见式（13）。
2: **对于** $r = 1, \ldots, R$ **执行**
3: 初始化 $\boldsymbol{\theta}^{(r)}$（结构化或随机种子）。
4: **对于** $s = 1, \ldots, S$ **执行**
5: 改进 $\leftarrow$ 假。
6: **对于**每个码片 n（随机顺序）**执行**
7: 设置 $\theta_n \leftarrow \arg\min_{\theta \in \mathcal{Q}} J_k$，其余保持不变；如果 J_k 减少，则改进 $\leftarrow$ 真。
8: **结束循环**
9: **如果**改进 = 假 **则**
10: **中断**（停止重启 r）。
11: **结束 if**
12: **结束 for**
13: 存储重启 r 得到的最佳序列。
14: **结束 for**
15: 返回总体最佳序列（或所有与其误差在容差范围内的序列）。

逆快速傅里叶变换（IFFT）将激活的 OFDM 子载波系数转换为时域感知突发。感知采用组合谐波自相关：

$$R_k[\tau] = \sum_n \boldsymbol{u}_k[n]^{\mathsf{H}} \boldsymbol{u}_k[n-\tau]. \tag{12}$$

设计目标为

$$J_k(\boldsymbol{\theta}) = \sum_{\tau \neq 0} |R_k[\tau]|^2 + \lambda \max_{\tau \neq 0} |R_k[\tau]|^2, \tag{13}$$

其中，$\boldsymbol{\theta} = [\theta_0, \ldots, \theta_{N-1}]^{\mathsf{T}}$ 收集感知序列的 QPSK 相位。第一项惩罚总旁瓣能量，第二项惩罚峰值旁瓣，λ 控制二者之间的权衡；为突出峰值旁瓣比（PSR），我们始终设置 $\lambda = 10$。由于相位字母表是离散的，所得优化问题具有组合性质；我们通过带随机重启的离散坐标下降法求解，按谐波阶数 k 重复执行，并在算法1中进行了总结。

名义感知序列采用相位加密，并由切向人工噪声提供保护，其中相位密钥 $\boldsymbol{\varphi}_{\mathrm{s}}$ 通过安全回传链路共享。协作基站还共享感知调度、OFDM 帧定时、活动资源以及名义序列种子。标准同步可提供粗略对齐，而目标相关传播时延仍需通过匹配感知进行估计。在补偿已知的前端失真和信道失真后，重构感知波形，并通过回波累积进一步降低剩余的定时不确定性。对于通信，基站与通信用户则共享通信域密钥 $\boldsymbol{\varphi}_{\mathrm{c}}$ [21]，以构建加密码本和切向方向，从而无需人工噪声实现即可进行协方差感知解调，并保护感知参考信号免受非预期接收机的获取。

D. 协方差感知解调

1) 未知人工噪声最大似然接收机：不同于感知场景，在该场景中波形 $\boldsymbol{x}$ 已知，通信并不具备这样的先验信息：候选项 i 本身就是未知量，因此其$\hat{}$切向方向 $\boldsymbol{t}_i$ 在确定 i之前也是未知的。因此，接收机对 ξ_r 进行边缘化处理，而不是对其进行估计，得到

$$\boldsymbol{Y}_r \mid i \sim \mathcal{N}\Big(\sqrt{1-\beta}\boldsymbol{x}_i, \boldsymbol{\Sigma}_i\Big), \tag{14}$$

其中

$$\boldsymbol{\Sigma}_i = \sigma_c^2 \boldsymbol{I}_{2k} + \beta \hat{\boldsymbol{t}}_i \hat{\boldsymbol{t}}_i^{\mathsf{T}}. \tag{15}$$

人工噪声仅沿候选项 i 的切向方向增加方差。由于所有切向量均为单位范数，

$$\det(\boldsymbol{\Sigma}_i) = (\sigma_c^2)^{2k-1}(\sigma_c^2 + \beta) \tag{16}$$

与 i 无关。定义 $\boldsymbol{r}_i = \boldsymbol{Y}_r - \sqrt{1-\beta}\boldsymbol{x}_{i^\circ}$ 应用谢尔曼–莫里森恒等式可得候选项度量

$$\Lambda_i(\boldsymbol{Y}_r) = \frac{\|\boldsymbol{r}_i\|^2}{\sigma_c^2} - \frac{\beta(\boldsymbol{r}_i^{\mathsf{T}}\hat{\boldsymbol{t}}_i)^2}{\sigma_c^2(\beta+\sigma_c^2)}. \tag{17}$$

$\hat{}$ 硬判决为 $i = \text{argmin}_i \Lambda_{i^\circ}$ 第一项为欧几里得项；第二项降低了候选项 i人工噪声方向上残差的惩罚。

2) 软解映射与*LDPC*译码：令 $b_a(i)$表示候选项i二进制标签中的比特位置 $a \in \{0,\dots,q-1\}$。协方差感知软解映射器计算

$$L_{r,a} = \log \frac{\sum_{i:b_a(i)=0} \exp[-\Lambda_i(\boldsymbol{Y}_r)/2]}{\sum_{i:b_a(i)=1} \exp[-\Lambda_i(\boldsymbol{Y}_r)/2]}. \tag{18}$$

低密度奇偶校验（LDPC）码仅应用于控制与载荷信道，这些信道必须满足明确的误码率（BER）要求；感知波形不进行编码，因为这样会扰动优化相位序列。相反，其调度信息和标称序列通过协同基站之间的安全回传链路共享。对于控制与载荷信道，采用具有迭代置信传播译码的标准码率为1/2 的LDPC码，作为具有代表性的编码层。

III. 威胁模型

A. 窃听检测模型

窃听者并非通信用户，但在观测直达链路时，仍可能推断出占用带宽、突发时序和处于活动状态的感知子载波等粗粒度特征。突发时序的随机化可能会妨碍其循环平稳检测。我们假设 Eve：（i）利用长期观测，尝试进行跨突发相干参考重构；（ii）可能了解波形结构和密钥生成规则，以便从接收波形中识别标称序列；（iii）可能利用标称序列知识恢复用于相干感知的相位密钥。

B. 已知参考的正确锁定分析

对于相干感知攻击，我们首先假设 Eve 拥有精确的复数波形参考信号 $x[n]$。我们采用仅考虑延迟的检测模型，假设 Eve 补偿后的残余多普勒引起的载波间干扰和相干处理间隔内的阶段漂移可以忽略不计。我们假设 Eve 在目标上空悬停或盘旋，且能够无遮挡地观测目标，并将反射路径建模为单抽头、以视距路径为主的信道。这些假设有利于 Eve，并简化了分析；下面的正确锁定上界来自忽略区间竞争。接收回波为

$$\begin{aligned} \mathcal{H}_0 &: \quad r[n] = w[n], \\ \mathcal{H}_1 &: \quad r[n] = g_r\, x[n-\ell_0] + w[n], \end{aligned} \tag{19}$$

其中， $\mathcal{H}_0$ 表示 Eve 处不存在目标生成的回波，$\mathcal{H}_1$ 表示目标存在假设， g_r 表示复路径增益， ℓ_0 表示相对于发射参考的未知回波延迟，而 $w[n] \sim \mathcal{CN}(0,\sigma_w^2)$ 表示在时间上相互独立的加性高斯白噪声（AWGN）。

Eve 对接收回波与已知参考信号相关信号：

$$z[\ell] = \sum_n r[n]\, x^*[n-\ell], \qquad \ell = 0,\dots,L-1, \tag{20}$$

然后应用峰值搜索规则

$$\max_\ell |z[\ell]| \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta, \qquad \hat{\ell} = \arg\max_\ell |z[\ell]|. \tag{21}$$

阈值 η 在 $\mathcal{H}_0$ 下进行校准，以满足搜索范围内的虚警概率 $P_{\text{FA}} = \Pr(\max_\ell |z[\ell]| > \eta \mid \mathcal{H}_0)$。我们假设真实延迟 ℓ_0 位于搜索网格上，但 Eve 不知道其位置。正确锁定要求阈值被超过且选中真实频点。定义感知突发信号的归一化自相关，

$$\chi[\ell] \triangleq \frac{1}{E_s}\sum_n x[n]\, x^*[n-\ell], \qquad E_s = \sum_n |x[n]|^2. \tag{22}$$

1) 噪声模型：对于完全观测到的无噪声参考信号，复高斯相关噪声的方差为

$$\sigma_z^2 = \sigma_w^2 E_s, \tag{23}$$

在两种假设下均相等，从而得到

$$\begin{aligned} z[\ell_0] \mid \mathcal{H}_0 &\sim \mathcal{CN}(0,\sigma_z^2), \\ z[\ell_0] \mid \mathcal{H}_1 &\sim \mathcal{CN}(g_r E_s,\, \sigma_z^2). \end{aligned} \tag{24}$$

2）正确频点与错误锁定概率：与之前一样，

$$\begin{aligned} P_{\text{corr}} &= \Pr\big(\hat{\ell} = \ell_0,\ |z[\hat{\ell}]| > \eta\big), \\ P_{\text{false}} &= \Pr\big(\hat{\ell} \neq \ell_0,\ |z[\hat{\ell}]| > \eta\big), \end{aligned} \tag{25}$$

其中 $P_D = P_{\text{corr}} + P_{\text{false}}$和 $P_{\text{miss}} = 1 - P_{D^\circ}$

3）主瓣的作用：由于 $\chi[0]=1$，真实频点的均值为 $\mu_0 = g_r E_{s^\circ}$ 对于相同的校准阈值 η， $P_{\text{corr}} \le \Pr(|z[\ell_0]| > \eta)$，因为正确锁定还要求真实频点在搜索中胜出。在此高斯分布模型下，

$$P_{\text{corr}} \;\le\; Q_1\!\left(\frac{\sqrt{2}|\mu_0|}{\sigma_z}, \frac{\sqrt{2}\eta}{\sigma_z}\right), \tag{26}$$

其中 $|\mu_0|^2/\sigma_z^2$ 是主瓣信噪比（SNR）。该界限忽略了其他延迟频点的竞争。

4) 旁瓣的作用： P_{false} 取决于非峰值取值 $\chi[\ell], \ell \neq 0$: 偏移量为 $\ell' \neq 0$ 处较大的旁瓣会使 $\ell_0+\ell'$ 位置的平均响应达到 $g_r E_s \chi[\ell']$，可能超过 η 并增大P_{false}，进而增大 P_D，但不会提升测距精度。与高旁瓣波形相比，低旁瓣波形的更低，同时可达到相同或更高的 P_{corr° 峰值旁瓣比（PSR） $= 1/\max_{\ell\neq 0}|\chi[\ell]|^2$与主瓣信噪比（SNR）$|\mu_0|^2/\sigma_z^2$相结合，比单独使用 P_D 更全面地表征测距可靠性。

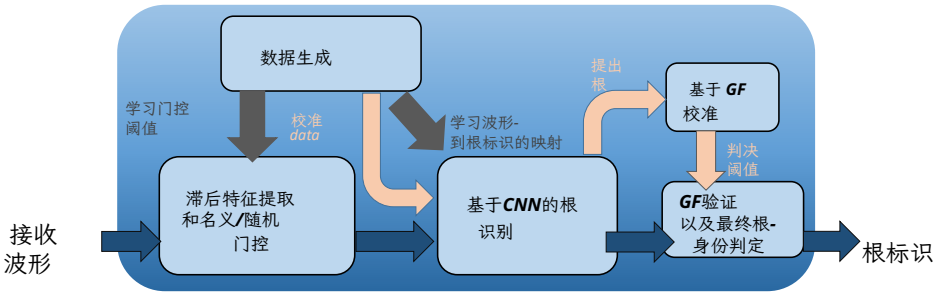


图1。卷积神经网络辅助的序列检测与根识别流程。生成的训练数据决定标称/随机门控器以及从波形到根的映射。卷积神经网络提出候选根，而经过独立校准的GF阈值则验证最终的根ID判定。

C. 相位密钥生成模型

我们区分三种按突发密钥生成模型。

*1)***共享查找表密钥**：第一个模型是文献 [21] 中相位加密傅里叶曲线查找表的突发级扩展。对于突发 b，发射机抽取

$$\boldsymbol{\varphi}^{(b)} = \left[\varphi_1^{(b)}, \ldots, \varphi_k^{(b)}\right]^{\mathsf{T}}, \qquad \varphi_m^{(b)} \overset{\text{i.i.d.}}{\sim} \mathcal{U}[-\pi, \pi), \tag{27}$$

并将同一个 k 系数向量应用于该突发中的所有 N 个符号。因此，它为每个突发实例化一个特定于该突发的查找表 $\{\boldsymbol{x}_i(\boldsymbol{\varphi}^{(b)}),\ \hat{\boldsymbol{t}}_i(\boldsymbol{\varphi}^{(b)})\}_{i=0}^{M-1}$，并在每次突发时刷新。

2) **平滑位置相关密钥**：第二个模型在此作为一种结构化基准引入，其设计受到用于安全 OFDM 波形的受控相位扰动方法 [17] 的启发。对于每个突发，合法节点使用共享密钥，从预定义空间中为每个谐波 m 选择 a_m、b_m 和 c_m，从而得到

$$\begin{aligned}\varphi_m^{(b)}[n] = d_\varphi[&\sin(2\pi a_m n + c_m) \\ &+0.55\sin(2\pi b_m n + 0.7c_m)],\end{aligned} \tag{28}$$

其中，d_φ 控制相位密钥深度；在仿真中，我们设定 $d_\varphi = 2.0$。该公式为每个突发生成一个位置相关的加密码本。

3) **种子扩展伪随机密钥**：第三个模型遵循标准的确定性随机比特生成方法 [25]。运行前，协同的合法节点通过安全回传链路接收共享主种子 $K_{\text{seed}} \in \{0,1\}^\lambda$，并维护一个同步突发计数器 b。密码学安全伪随机数生成器（CSPRNG）针对每个位置 n 和谐波 m，根据这对输入生成一个伪随机值：

$$\begin{aligned}\boldsymbol{U}^{(b)} &= \mathcal{G}(K_{\text{seed}}, b) \in [0,1)^{N\times k}, \\ \boldsymbol{\Phi}^{(b)} &= 2\pi\boldsymbol{U}^{(b)} - \pi\mathbf{1}_{N\times k},\end{aligned} \tag{29}$$

其中 $\Phi_{n,\ m}^{(b)} = \varphi_m^{(b)}[n] \in [-\pi, \pi)$；$b$ 用于分隔突发域。

采用 q 位参数时，共享和平滑规则要求每个突发分别使用 kq 位和 $3kq$ 位。种子扩展规则共享一个 λ 位种子，用于本地掩码生成；其安全性取决于种子空间的大小，但代价是需要进行伪随机扩展。

D. *Eve* 密钥与符号恢复模型

我们假设知情窃听者 Eve 知道算法1中的波形构造方式以及相位密钥生成规则。该标称序列类别集合为 $\mathcal{R} = \{1, \ldots, R\}$，种子空间为 $\mathcal{S}$。种子 $s \in \mathcal{S}$ 通过 $r = g(s)$选择一个类别。种子通过安全回传链路共享，并定期更新。Eve 知道这两个空间及其映射关系，但不知道实际使用的种子或类别。Eve 可以使用离线训练模型将受保护波形映射到其标称根 $r \in \mathcal{R}$，从而绕过符号和相位密钥估计。

*1)*离线攻击：基于***CNN***的序列检测与根识别：数据驱动的Eve首先将标称感知突发信号与随机突发区分开，然后识别每个被接受的标称突发所对应的生成根，如图 1 所示。数据生成模块已知类别集合 $\mathcal{R}$、种子空间及选择规则、相位密钥生成规则以及人工噪声占比 β。该模块利用这些结构知识生成带标签的受保护突发。每个训练样本均通过从已知候选空间中独立抽取一个标称根和一个相位密钥实现来生成，同时从预定义范围内随机选择信噪比。

在检测模型中，标称/随机门控器从标称和随机数据集中学习时延特征，并决定拒绝输入，或将其传递给基于卷积神经网络的根标识模块。卷积神经网络随后提出候选根，而格拉姆特征（GF）模块则给出最终的根ID判定。在此之前，带标签的校准数据包括已见标称样本（用于训练卷积神经网络的标称样本）、随机序列（长度相同的随机序列）和未见标称样本（未用于训练卷积神经网络的标称样本）。这些采样点被输入卷积神经网络，以获得候选根标识，并据此计算相应的GF分数。随后，GF校准模块根据这三个数据集的分数分布设定判决阈值。

步骤 1：时延特征提取与标称/随机门控。输入为接收的活动子载波矩阵$\boldsymbol{Y} = [\boldsymbol{y}[0], \ldots, \boldsymbol{y}[N-1]]^{\mathsf{T}} \in \mathbb{C}^{N\times k}$。对于每个非零符号时延，Eve计算归一化相关功率

$$\rho_\ell = \left|\frac{\sum_{n=\ell}^{N-1} \boldsymbol{y}[n]^{\mathsf{H}}\boldsymbol{y}[n-\ell]}{\sum_{n=0}^{N-1}\|\boldsymbol{y}[n]\|^2}\right|^2, \quad \ell = 1, \ldots, N-1. \tag{30}$$

并构成二维特征向量

$$\boldsymbol{f} = \left[-10\log_{10}\left(\max_\ell \rho_\ell\right),\ 2\sum_{\ell=1}^{N-1}\rho_\ell\right]^{\mathsf{T}} \tag{31}$$

其各个分量分别为接收信号的峰值旁瓣比和归一化双侧旁瓣能量。特征向量 $\boldsymbol{f}$ 使用训练单元均值 $\boldsymbol{\mu}_f$ 和标准差 $\boldsymbol{\sigma}_f$ 逐元素进行标准化。线性逻辑门产生

$$g(\boldsymbol{f}) = \boldsymbol{w}_g^{\mathsf{T}}\left((\boldsymbol{f}-\boldsymbol{\mu}_f)\oslash\boldsymbol{\sigma}_f\right)+c_g, \tag{32}$$

其中，$\oslash$表示逐元素除法，$\boldsymbol{w}_g \in \mathbb{R}^2$ 是学习得到的门控权重向量，$c_g \in \mathbb{R}$ 是学习得到的偏置。对于训练样本 i，令 $z_i = 1$ 表示标称突发，$z_i = 0$ 表示随机突发，并令 $p_i = \left(1+e^{-g(\boldsymbol{f}_i)}\right)^{-1}$。使用小批量 Adam 学习参数，以最小化

$$(\hat{\boldsymbol{w}}_g, \hat{c}_g) = \arg\min_{\boldsymbol{w}_g, c_g} -\frac{1}{B}\sum_{i=1}^{B}\left[z_i \log p_i + (1-z_i)\log(1-p_i)\right].$$

当 $g(\boldsymbol{f}) < 0$时，Eve 将观测判定为随机；否则，便进行根识别。

步骤 2：使用相位不变 CNN 进行根识别。令

$$E_y = \frac{1}{N}\sum_{n=0}^{N-1}\|\boldsymbol{y}[n]\|^2. \tag{33}$$

对于 $n \geq 1$，Eve 构造相邻符号乘积 $\boldsymbol{d}[n] = \boldsymbol{y}[n]\odot\boldsymbol{y}[n-1]^*/E_y$，令 $\boldsymbol{d}[0] = \boldsymbol{0}$，并定义

$$\boldsymbol{q}[n] = \left[\Re\{\boldsymbol{d}[n]\}^{\mathsf{T}}, \Im\{\boldsymbol{d}[n]\}^{\mathsf{T}}, \frac{\left(|\boldsymbol{y}[n]|^2\right)^{\mathsf{T}}}{E_y}\right]^{\mathsf{T}} \in \mathbb{R}^{3k}. \tag{34}$$

在每个位置，$\boldsymbol{q}[n]$ 由两个连续的 k分量接收向量之间逐分量乘积的实部和虚部，以及当前向量的归一化分量功率构成。这三个 k 维项构成 $3k \times N$ CNN 输入。相邻符号乘积会抑制连续符号共有的相位分量，而功率项则保留幅度信息。表 I 总结了该 CNN；它采用高斯误差线性单元 (GELU) 激活函数，并输出根逻辑值。

表 I 用于 Eve 侧标称根识别的 CNN 架构。

层	大小/通道数	操作
输入	$3k \times N$	相位不变特征 $\boldsymbol{q}[n]$
卷积块 1	$3k \to 32$	一维卷积，卷积核 7，GELU
卷积块2	$32 \to 32$	一维卷积，卷积核 7，GELU
隐藏层	$32N \to 64$	展平层、线性层、GELU
输出	$64 \to R$	名义根对数几率

根分类头在带有标签 $r_i \in \mathcal{R}$ 的 B名义突发上最小化多类交叉熵：

$$\mathcal{L}_{\mathrm{CNN}}(\boldsymbol{\psi}) = -\frac{1}{B}\sum_{i=1}^{B}\log\frac{\exp(h_{i,r_i})}{\sum_{r=1}^{R}\exp(h_{i,r})}, \tag{35}$$

其中，$\boldsymbol{\psi}$ 表示卷积神经网络参数，$r \in \mathcal{R}$ 索引一个候选根类别，$h_{i,r}$ 是突发 i对应的逻辑值；因此，h_{i,r_i} 是真实类别对数几率。对于一个被接受的突发，卷积神经网络会返回训练单元期间已知的 R 个根的根逻辑值 $\boldsymbol{h} = [h_1, \ldots, h_R]^{\mathsf{T}}$。Eve会对这些逻辑值进行排序并保留包含排名最高的 L个根的集合 $\mathcal{C}_L$ 。我们使用 $L = 20$ 构成候选根短名单。

步骤 3：GF验证。接收突发在符号位置上进行中心化，如下所示

$$\tilde{\boldsymbol{y}}[n] = \boldsymbol{y}[n] - \frac{1}{N}\sum_{n'=0}^{N-1}\boldsymbol{y}[n'], \tag{36}$$

其中，n' 是遍历所有 N 接收符号位置的虚拟索引。中心化 Gram 矩阵$[\boldsymbol{G}_y]_{n,n'} = \tilde{\boldsymbol{y}}[n]^{\mathsf{H}}\tilde{\boldsymbol{y}}[n']$ 的严格上三角元素构成 $\boldsymbol{g}_y$。利用预先计算的名义根向量 $\boldsymbol{g}_r$，Eve 对候选项 r 进行评分：

$$s_r = \frac{\Re\{\boldsymbol{g}_r^{\mathsf{H}}\boldsymbol{g}_y\}}{\|\boldsymbol{g}_r\|\,\|\boldsymbol{g}_y\|}. \tag{37}$$

GF 模块为每个入围候选项评分。

步骤 4：独立阈值校准。验证阈值在独立数据集上校准，具体如下：

$$\eta^* = \arg\max_{\eta}\frac{1}{2}\left[\Pr(s^+ \geq \eta) + \Pr(s^- < \eta)\right]. \tag{38}$$

这里，$s_i^+ = s_{i,r_i}$ 是分配给名义校准突发 i中真实根的 GF 分数。如果该根不在 $\mathcal{C}_L$中，则将该突发计为漏识别。对于随机校准突发 j，$s_j^- = \max_{r\in\mathcal{C}_L} s_{j,r}$ 是其入围候选项中的最高分。因此，这两个概率分别衡量正确根接受和随机突发拒绝。式（38）对这两种结果进行权衡；由此得到的η^* 随后固定下来，用于最终决策。

步骤 5：最终决策。Eve 选择 GF 分数最高的入围候选项，$r^* = \arg\max_{r\in\mathcal{C}_L} s_r$，并且仅当 $s_{r^*} \geq \eta^*$时才将r^* 作为检测到的名义根 ID 返回。否则，将通过逻辑门的突发报告为未知名义序列。该攻击会返回根 ID、未知名义序列判定或随机突发拒绝。

*2)*在线攻击：基于拟合的检测：该攻击不依赖离线训练的CNN。如果感知系统在较长时间内重复使用与固定根 $r \in \mathcal{R}$关联的标称序列，Eve可能会根据每个位置的经验符号分布推断出该序列的全部或部分内容。在获得这一估计后，Eve拟合相位密钥，并利用拟合分数门控判断受保护突发是否包含标称序列。拟合成功后，可重建用于相干匹配滤波和时延估计的复参考信号；符号级定位只能提供粗略定时。

令 $A_n \in \{0,1,2,3\}$ 表示符号位置 n处的标称 QPSK标签，其中 $\theta_{A_n} = 2\pi A_n/4$。QPSK谐波构造存在结构性暴露。由于 $\theta_{A_n} \in\{0, \pi/2, \pi, 3\pi/2\}$，

$$e^{j4\theta_{A_n}} = 1, \qquad e^{j5\theta_{A_n}} = e^{j\theta_{A_n}}.$$

因此，四次谐波以及第五谐波相对于第一谐波的相位可以消除未知符号依赖，并揭示密钥相关结构。这些观测仍与人工噪声耦合，无法揭示完整密钥，但可用于初始化或约束拟合算法。

由此得到的攻击是一个模型感知约束最大似然问题。令 $\boldsymbol{\zeta}$ 表示未知密钥参数：对于式 (27) 中的共享密钥，为 $\boldsymbol{\varphi}$；对于式 (28) 中的平滑密钥，为 $\{a_m, b_m, c_m\}_{m=1}^{k}$。将切向人工噪声系数 $\boldsymbol{\xi}$ 视为干扰参数后，Eve寻求

$$(\hat{\boldsymbol{\zeta}}, \hat{\boldsymbol{A}}_{\mathcal{U}}) = \arg\max_{\boldsymbol{\zeta}, \boldsymbol{A}_{\mathcal{U}}} p(\boldsymbol{Y} \mid \boldsymbol{A}_{\mathcal{K}}, \boldsymbol{A}_{\mathcal{U}}, \boldsymbol{\zeta}), \tag{39}$$

这里，$\boldsymbol{Y}$ 是接收突发。此外，$\mathcal{K}$ 和 $\mathcal{U}$ 分别是已知和未知符号位置集合。切向人工噪声系数会被投影消去，未知符号则与密钥联合拟合。非凸似然可能存在等价分解。

基于 Adam 的连续拟合： Adam 被用作该拟合问题的一阶数值求解器 [26], [27]。对于候选密钥参数 $\boldsymbol{\zeta}$ 和已知符号 A_n，定义

$$\boldsymbol{a}_n(\boldsymbol{\zeta}) = \boldsymbol{y}[n] - \sqrt{1-\beta}\, \boldsymbol{x}_{A_n}(\boldsymbol{\varphi}_{\boldsymbol{\zeta}}[n]),$$

其中，$\boldsymbol{\varphi}_{\boldsymbol{\zeta}}[n]$ 由共享密钥参数或平滑密钥参数生成。对于固定的候选密钥，每个符号对应的切向人工噪声系数的最小二乘估计为

$$\hat{\xi}_n(\boldsymbol{\zeta}) = \frac{\Re\{\hat{\boldsymbol{t}}_{A_n}^{\mathsf{H}}(\boldsymbol{\varphi}_{\boldsymbol{\zeta}}[n])\, \boldsymbol{a}_n(\boldsymbol{\zeta})\}}{\sqrt{\beta}\, \left\|\hat{\boldsymbol{t}}_{A_n}(\boldsymbol{\varphi}_{\boldsymbol{\zeta}}[n])\right\|^2}.$$

Eve 将该估计代入残差能量目标函数

$$\mathcal{L}_{\mathrm{Adam}}(\boldsymbol{\zeta}) = \sum_{n\in\mathcal{K}} \left\| \boldsymbol{a}_n(\boldsymbol{\zeta}) - \sqrt{\beta}\, \hat{\xi}_n(\boldsymbol{\zeta}) \hat{\boldsymbol{t}}_{A_n}(\boldsymbol{\varphi}_{\boldsymbol{\zeta}}[n]) \right\|_2^2, \tag{40}$$

其中，$\mathcal{K}$ 包含已知符号位置。该投影会在每个此类位置移除拟合效果最佳的切向人工噪声分量。随后，密钥参数根据式（40）的梯度，通过 Adam [26]进行更新：

$$\boldsymbol{\zeta}^{(q+1)} = \Pi_{\mathcal{Z}}\left(\boldsymbol{\zeta}^{(q)} - \alpha_q \frac{\widehat{\boldsymbol{m}}_q}{\sqrt{\widehat{\boldsymbol{v}}_q} + \epsilon} \right),$$

其中，$\widehat{\boldsymbol{m}}_q$ 和 $\widehat{\boldsymbol{v}}_q$ 是 Adam 的偏置校正一阶和二阶矩估计，α_q 是步长，ϵ 用于避免除以零。$\Pi_{\mathcal{Z}}$ 会对相位参数进行回绕，并将其余参数投影到指定域。若 Eve 知晓并利用这种结构性暴露，则第一次重启会根据四次谐波以及第五次谐波相对于第一次谐波的相位观测进行初始化。若不具备这些知识，则所有重启均采用随机初始化。达到固定的迭代预算，或相对损失下降量低于指定容差时，过程即停止。

相位感知期望最大化： 如果泄露的标称符号存在不确定性，Eve 可以采用相位感知期望最大化过程 [28]↓[29], ，参照 OFDM 系统中基于期望最大化的联合检测与估计 [30]。不同于 Adam 的固定标签拟合，相位感知期望最大化会评估不确定位置处的所有 M 候选项。对于 $i \in \{0, \ldots, M-1\}$，定义

$$\boldsymbol{a}_{n,i}(\boldsymbol{\zeta}) = \boldsymbol{y}[n] - \sqrt{1-\beta}\, \boldsymbol{x}_i(\boldsymbol{\varphi}_{\boldsymbol{\zeta}}[n]),$$

并将每个符号的切向人工噪声系数剖析消去，得到

$$\hat{\xi}_{n,i}(\boldsymbol{\zeta}) = \frac{\Re\{\hat{\boldsymbol{t}}_i^{\mathsf{H}}(\boldsymbol{\varphi}_{\boldsymbol{\zeta}}[n])\, \boldsymbol{a}_{n,i}(\boldsymbol{\zeta})\}}{\sqrt{\beta}\, \left\|\hat{\boldsymbol{t}}_i(\boldsymbol{\varphi}_{\boldsymbol{\zeta}}[n])\right\|^2}.$$

算法 2 Eve 基于 Adam 的相位密钥拟合

1: 输入接收突发 $\boldsymbol{y}$、候选标称序列、 k、 β、迭代次数 Q 和重启次数 R.
2: **对于** $r = 1, \ldots, R$ **do**
3: 如果具备结构知识，则对其使用谐波信息初始化第一次重启；否则随机初始化。将 Adam矩 $\boldsymbol{m}^{(0)}$, $\boldsymbol{v}^{(0)}$ 设置为零。
4: **对于** $q = 0, \ldots, Q-1$ **执行**
5: 生成 $\boldsymbol{\varphi}_{\boldsymbol{\zeta}^{(q)}}[n]$ 并形成 $\boldsymbol{x}_{A_n}$ 和 $\hat{\boldsymbol{t}}_{A_n}$，对于每个 $n \in \mathcal{K}$。
6: 通过切向投影计算每个 $\hat{\xi}_n(\boldsymbol{\zeta}^{(q)})$。
7: 评估 $\mathcal{L}_{\mathrm{Adam}}$ 及其梯度。
8: 更新 Adam矩并将 $\boldsymbol{\zeta}^{(q+1)}$ 投影到 $\mathcal{Z}$上。
9: **结束循环**
10: 存储最终残差最小的密钥。
11: **结束循环**
12: 返回最佳密钥及其逐符号切向AN估计。

算法 3 Eve的相位感知EM密钥估计

1: 输入接收突发 $\boldsymbol{Y}$、符号先验 π_n、i、 M、 k、 β、 σ_c^2、EM循环次数 Q 以及重启次数 R。2: 对于 $a = 1$、.....、R，执行 3: 如果结构知识可用，则在第一次重启时使用谐波信息初始化；否则在 $\mathcal{Z}$ 中随机初始化 $\boldsymbol{\zeta}$。4: 对于 $q = 0$、.....、$Q-1$，执行 5: 针对每个 (n, i)，构造 $\boldsymbol{x}_i(\boldsymbol{\varphi}_{\boldsymbol{\zeta}^{(q)}}[n])$ 和 $\hat{\boldsymbol{t}}_i(\boldsymbol{\varphi}_{\boldsymbol{\zeta}^{(q)}}[n])$。6: 剖析消去 $\hat{\xi}_n$、i，计算 Λ_n、i，并将其归一化以获得 $q_{n\,i}^{(q)}$。7: 固定 $q_{n\,i}^{(q)}$，并执行 Adam步以最小化 $\mathcal{L}_{\mathrm{EM}}$。8: 将更新后的 $\boldsymbol{\zeta}^{(q+1)}$ 投影到 $\mathcal{Z}$ 上。9: 如果相对似然变化低于容差，则停止。10: 结束循环。11: 计算边际似然并存储最佳重启结果。12: 结束循环。13: 返回最佳密钥和符号估计。

相应的剖面似然得分为

$$\Lambda_{n,i}(\boldsymbol{\zeta}) = -\frac{1}{2\sigma_c^2} \left\| \boldsymbol{a}_{n,i}(\boldsymbol{\zeta}) - \sqrt{\beta}\, \hat{\xi}_{n,i}(\boldsymbol{\zeta}) \hat{\boldsymbol{t}}_i(\boldsymbol{\varphi}_{\boldsymbol{\zeta}}[n]) \right\|_2^2.$$

令 $\pi_{n,i}$ 表示 Eve 先验认为位置 n包含符号 i的概率。对于已知标签，该概率为独热分布；对于擦除标签，该概率为均匀分布。在 EM迭代 q中，E步计算

$$q_{n,i}^{(q)} = \frac{\pi_{n,i} \exp[\Lambda_{n,i}(\boldsymbol{\zeta}^{(q)})]}{\sum_{j=0}^{M-1} \pi_{n,j} \exp[\Lambda_{n,j}(\boldsymbol{\zeta}^{(q)})]}.$$

因此，E步使用当前密钥估计执行软符号检测：$q_{n\,i}^{(q)}$，</style}表示在剖除候选项特定的人工噪声系数后，位置 n 处候选项i 的后验概率。M步固定 $q_{n\,i}^{(q)}$,</style}，并使用 Adam 通过最小化下式来更新 $\boldsymbol{\zeta}$

$$\mathcal{L}_{\mathrm{EM}}(\boldsymbol{\zeta}) = -\frac{1}{N} \sum_{n=0}^{N-1} \sum_{i=0}^{M-1} q_{n,i}^{(q)} \Lambda_{n,i}(\boldsymbol{\zeta}), \tag{41}$$

每次更新后，将 $\boldsymbol{\zeta}$ 投影到密钥参数集 $\mathcal{Z}$上。因此，声明为已知的标签保持不变，而擦除标签或不确定标签则与密钥共同细化。更新后的密钥会改变下一次 E步所使用的候选项得分，两个步骤交替进行，直至似然收敛或迭代预算耗尽。由于似然是非凸的，因此保留多个初始化结果。

拟合分数判决： 这两种算法都可用于检测标称波形。对于 $a \in$ {Adam，期望最大化}，Eve 计算 $d_a = \min_{\boldsymbol{\zeta}} \mathcal{L}_a(\boldsymbol{\zeta}) / c_a$，其中 $c_{\mathrm{Adam}} = \|\boldsymbol{Y}\|_F^2$和$c_{\mathrm{EM}} = 1$。这里，$\mathcal{L}_{\mathrm{Adam}}$ 是重构残差，而 $\mathcal{L}_{\mathrm{EM}}$已经是取平均后的负对数似然。候选项

当 $d_a \le \eta_a$ 时，该候选项会被接受，否则将被拒绝。每个 η_a 都经过校准，以便在接受完全正确或部分正确的标称候选项与拒绝随机候选项之间取得平衡。

基于拟合的攻击利用了可用的结构泄漏，但仍有两项局限。首先，Adam 和期望最大化仍需求解非凸的联合密钥–人工噪声问题，并且可能收敛到等价的波形分解。其次，共享密钥仅有 k 个未知相位，而平滑密钥有 $3k$ 个生成器参数，种子扩展密钥则不存在可微分相位关系。这些拟合算法无法直接恢复种子扩展相位密钥。确定标称根后，Eve 必须搜索 λ 位密钥种子；结构泄漏或许能提前排除候选项，但无法对伪随机空间排序。在最坏情况下，这种无结构搜索需要 $\Omega(2^{\lambda})$ 次经典测试（平均约为 $2^{\lambda-1}$ 次），或 Θ 次 Grover 查询（$2^{\lambda/2}$）。

E. 符号匹配与序列定位

恢复同一感知序列的多个不完美副本后，Eve 可以通过最大化它们的符号一致性得分来定位该序列。设 $A \in \{0,\dots,M-1\}$ 为一个传输符号，A_1 和 A_2 为根据两个独立恢复的副本得到的估计值。我们假设采用对称的 M 元错误模型，符号错误率为 p_s，

$$\Pr(\hat{A}_j = b \mid A = a) = \begin{cases} 1 - p_s, & b = a, \\ p_s/(M-1), & b \neq a, \end{cases} \qquad j \in \{1,2\}.$$

对齐时，如果两者都正确或选择了相同的错误符号，则估计结果一致。由条件独立性可得

$$\begin{aligned} p_{\mathrm{a}}(p_s) &= \Pr(\hat{A}_1 = \hat{A}_2 \mid A = a) \\ &= \sum_{b=0}^{M-1} \Pr(\hat{A}_1 = b \mid A = a) \Pr(\hat{A}_2 = b \mid A = a) \\ &= (1-p_s)^2 + (M-1)\left(\frac{p_s}{M-1}\right)^2 \\ &= (1-p_s)^2 + \frac{p_s^2}{M-1}. \end{aligned} \tag{42}$$

在一个估计正确而另一个错误的混合情形下，由于错误估计排除了真实符号，因此无法产生一致结果。在无关对齐处，底层符号彼此独立；对于均匀字母表和对称错误模型，恢复的符号在边缘上同样服从均匀分布，因此以 $1/M$ 的概率一致。对于长度为 N 的序列，正确对齐得分近似服从 $S_{K_0} \sim$ 二项分布$(N,\ p_{\mathrm{a}})$，而无关符号偏移服从 $S_K \sim$二项分布$(N,\ 1/M)$。ˆ当采用 $K = \operatorname{argmax}_K S_K$ 且真实符号偏移为 K_0 时，定位平均绝对误差（MAE）为

$$D_{\mathrm{MAE}}(p_s) = \mathbb{E}\{|\hat{K} - K_0|\} = \sum_{K} |K - K_0| \Pr(\hat{K} = K). \tag{43}$$

这种映射并非仅由符号错误率决定，因为它还取决于 N、M 和搜索区间。

存在相位密钥失配和残余人工噪声的相干感知攻击： 我们通过功率域近似，将密钥恢复准确率与正确时延锁定联系起来。对于回波 b，令残余密钥误差为 $\delta_{\phi,\,b} \sim \mathcal{N}(0,\ \sigma_\phi^2)$。其相干幅度和功率因子为

$$\rho_\phi = \mathbb{E}\big[e^{j\delta_{\phi,b}}\big] = e^{-\sigma_\phi^2/2}, \quad G_\phi = |\rho_\phi|^2 = e^{-\sigma_\phi^2}. \tag{44}$$

对于 B 独立累积的回波，每个回波的线性信噪比为 γ，归一化热噪声、密钥失配和残余人工噪声功率近似为

$$P_{\mathrm{th}} = \frac{1}{(1-\beta)B\gamma},\ P_{\mathrm{key}} = \frac{1-G_\phi}{B},\ P_{\mathrm{AN}} = \frac{\beta(1-G_\phi)}{(1-\beta)B}.$$

$$\gamma_{\mathrm{eff}}^{(\mathrm{key+AN})} = \frac{G_\phi}{P_{\mathrm{th}} + P_{\mathrm{key}} + P_{\mathrm{AN}}}. \tag{45}$$

该表达式考虑了相位密钥失配及其导致的不完美切向人工噪声抵消。在相同信道、前端、延迟搜索和阈值条件下，相对于理想参考检测器评估正确锁定概率：

$$P_{\mathrm{corr}}(\sigma_\phi) \approx \mathcal{P}_{\mathrm{corr}}^{(0)}(\gamma_{\mathrm{eff}}), \tag{46}$$

其中 $\mathcal{P}_{\mathrm{corr}}^{(0)}(\cdot)$表示信道感知的基线正确锁定曲线。该近似假设密钥误差与回波实现相互独立且均值为零。

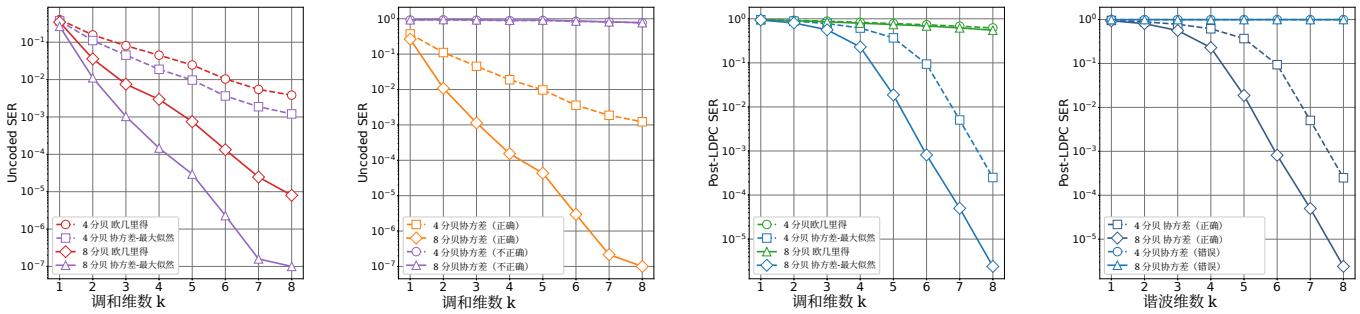
IV. 数值结果

我们评估 Eve 的知识与能力逐步增强时的安全性。在验证通信与波形设计后，我们测试盲跨突发相关。在已知波形和密钥生成规则的情况下，Eve 使用离线卷积神经网络识别标称根；若进一步掌握标称符号知识，她便使用 Adam 或相位感知的期望最大化在线拟合相位密钥。最后，我们通过检测和时延锁定（密钥不完美）来评估相干感知攻击。

A. 安全通信与波形设计的验证

我们使用 QPSK 评估用于感知和控制的通信安全性，并使用高阶调制传输有效载荷。天真的 Eve 使用欧几里得解映射，而知情窃听者 Eve 使用协方差感知解映射，但不知道相位密钥。切向人工噪声和相位密钥分别独立重新生成，其中 $\beta = 0.5$ 如 [21]所示。

图2(a)–(b)给出了未编码四相移键控的结果。增大 k会通过增加谐波特征和冗余来降低符号错误率，而协方差感知解映射优于欧几里得度量。在采用密钥时，合法接收机保留正确码本，而Eve的失配码本使其符号错误率保持较高。在 $k = 5$ 和8分贝时，对于共享、平滑和种子扩展密钥生成规则，Eve的符号错误率分别为0.7498、0.7497和0.7484。因此，它们的通信性能相近；为简便起见，图2采用共享密钥。图2(c)–(d)给出了相应码率$1/2$ 的LDPC编码64-PSK结果。相同趋势仍然保持，尽管更密集的星座图提高了对噪声和切向人工噪声的敏感性。更大的 k 因此提高了可靠性，其代价在于



(a) (b) (c) (d)

图 2. 4 和 8 分贝下 SER 随谐波维度的变化。(a)–(b) 未编码四相移键控：未加密的欧几里得解调和协方差感知解调，以及使用和不使用相位密钥的加密协方差感知解调。 $M = 4$ 阶段在 k 谐波分量间循环重复。(c)–(d) 在相应的未加密和加密设置下，码率为$1/2$ 的 LDPC编码64-PSK。

表 II 优化和随机四相移键控波形的峰值旁瓣比（分贝）：$N = 64$，信噪比 $= 5$ 分贝，$\beta = 0.5$，2000 次蒙特卡洛运行。

k	1	2	3	4	5	6	7	8
优化峰值旁瓣比	20.95							
随机基线 峰值								

额外的信号维度，这对于较短的感知与控制信号是一种合适的折中。总体而言，即使Eve知道接收机架构并采用协方差感知解映射，密钥失配仍使她保持较高的错误率。

1) 波形设计与合法感知： 我们验证了协作基站的感知波形设计。表 II 显示，优化可使峰值旁瓣比高于随机基线，在大多数 k 的情况下达到约 20 分贝。 $k = 4$ 和 $k = 8$处的下降是 QPSK 字母表所导致的结构性效应：对于 $\phi_n = i\pi/2$，谐波和 $\sum_{m=1}^{k} e^{jm\phi_n}$ 的周期为 $4/\gcd(i,\ 4)$ 在 m中；当 k 可被此周期整除时，该谐波和会消失，仅留下$\phi_n = 0$ 非退化项，从而降低分集。

2) 重复突发波形保护： 此处，Eve 观测重复接收波形，但不了解其生成结构，也无法可靠地解码其中的符号，如上文所示。因此，她的检测器对观测结果进行互相关。使用独立刷新的相位密钥和人工噪声实现传输相同的标称序列。表III根据式(21)中的峰值阈值规则，比较了优化序列和随机序列的检测概率 P_D 。未受保护的优化序列（**Opt. No**）为$P_D = 1.0$，而.05对应于**Rand. No**（不同的随机序列实现）。在 $\beta = 0.5$ 处使用相同密钥和独立人工噪声（**Opt. A+SK**）时，检测概率为 $P_D = 0.925$。仅刷新密钥即可将 P_D 降至 0.386；加入人工噪声后，其低于未受保护的随机基线 $\beta = 0.3$，对于 $\beta \geq 0.6$未观察到任何检测结果，这与受保护的随机基线（**Rand. A+K**，$\beta = 0.5$）一致，凸显了密钥刷新的重要性。尽管受保护的优化序列保留了更高的峰值旁瓣比，但该比值描述的是相关形状：检测还要求足够大的峰值幅度。独立密钥抑制了跨突发对齐及由此产生的峰值，因此即使峰值旁瓣比更高，也能降低检测概率。

表III 重复突发密钥化QPSK互相关： $N = 64, k = 5$，信噪比 $= 5$ 分贝， $P_{\mathrm{FA}} = 0.05$。

β	Peak	PSR	P_D	β	Peak	PSR	P_D
0.0	0.262	5.620	0.386	0.5	0.143	2.350	0.002
0.1	0.235	5.280	0.172	0.6	0.124	1.480	0.000
0.2	0.211	4.890	0.074	0.7	0.116	1.000	0.000
0.3	0.187	4.160	0.016	0.8	0.112	0.810	0.000
0.4	0.160	3.070	0.002	0.9	0.112	0.690	0.000
随机数	0.202			**随机数A+K**			
最优数	0.725			**方案 A+SK**			

B. 针对 *Eve* 推断攻击的验证

1) 相位密钥失配与搜索复杂度： 我们首先评估知情窃听者 Eve：她以残余平均误差 σ_ϕ重构相位密钥，并使用协方差感知接收机， $\beta = 0.5$ 且信噪比为 $= 1$ 分贝。表 IV 显示，所得符号错误率从使用精确密钥时的 0.055 增加到 $\sigma_\phi = 0.5\pi$时的 0.581。如果 Eve 仅知道相位密钥空间，则将 kN 个相位中的每一个量化为 $Q = \lceil 2/\sigma_\phi \rceil$ 个值。通过解调全部 N 个 QPSK 符号，并为每个符号计算四个度量指标，对每个候选项数组进行评分，得到

$$C_{\mathrm{Eve}} = 4NQ^{kN} = 4N\left\lceil \frac{2}{\sigma_\phi} \right\rceil^{kN} \tag{47}$$

每次突发的度量评估次数。此计数不需要知道密钥生成规则。表 IV 还报告了此盲搜索成本，以及根据式 (43) 得出的定位平均绝对误差，结果基于 200，000 次蒙特卡洛 (MC) 运行。64 符号的感知序列嵌入在两侧各 64 个随机符号之间。Eve 将 64 符号的参考信号沿 192 符号的数据流滑动，并选择匹配度最高的起始位置。

2) 序列检测与根识别验证：接下来，我们考虑一个更强的 Eve：她了解波形和相位密钥生成规则。我们评估离线序列识别和在线密钥拟合。卷积神经网络代表离线攻击，在无需显式密钥恢复的情况下检测标称感知序列并识别其根。门控器和卷积神经网络使用 $R = 2^{10} = 1024$ 优化后的标称根进行训练，采用 $N = 64$、 $k = 5$、 $\beta = 0.5$ 用于受保护

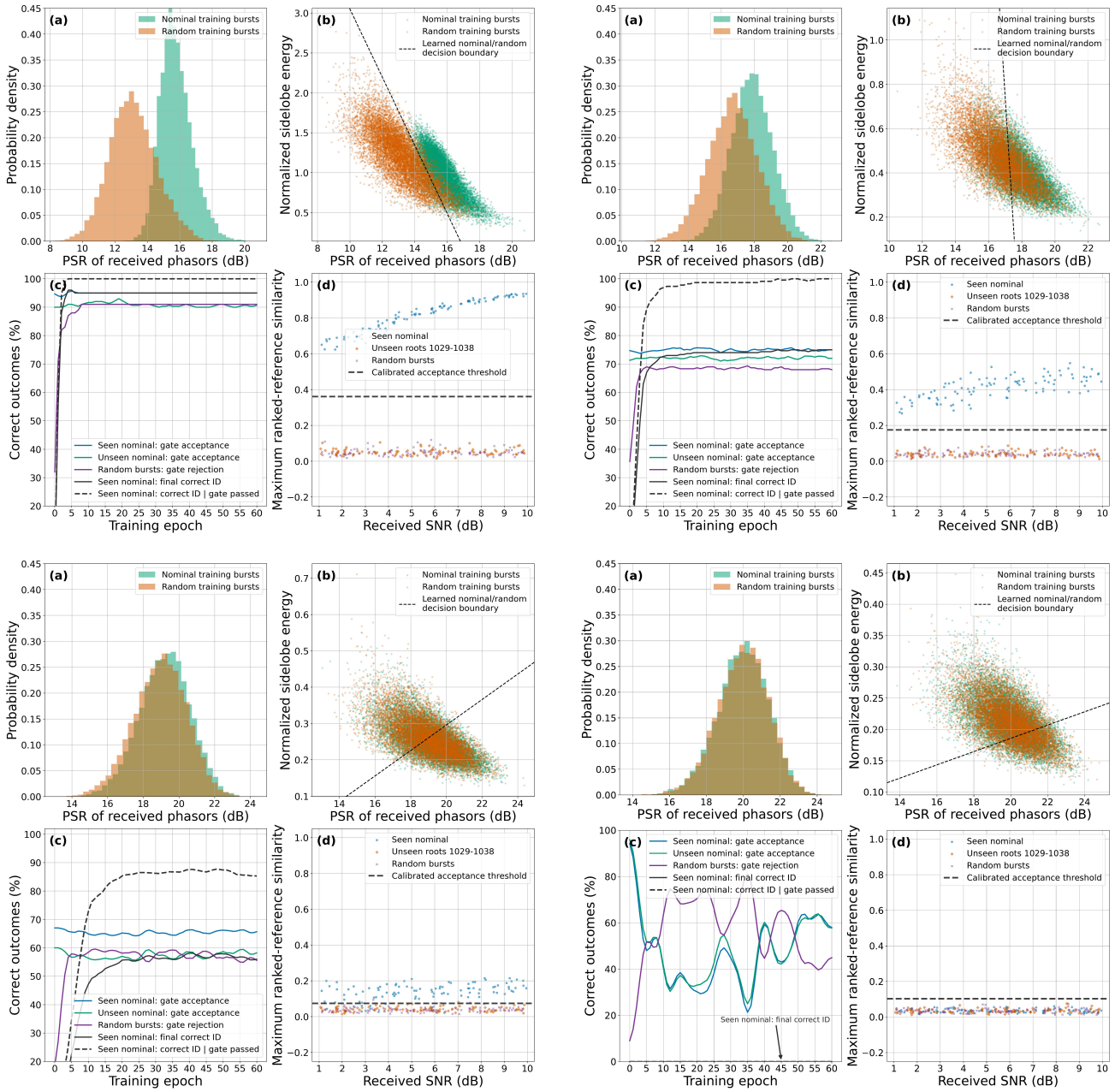
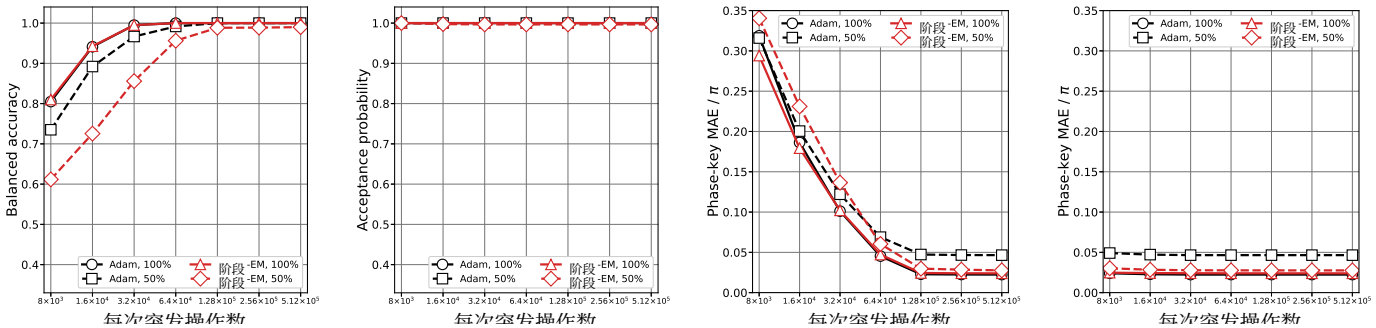


图3. 离线序列检测与根识别。左上：未受保护基线（$\beta = 0$）。右上：突发共享查找表密钥。左下：平滑位置相关密钥。右下：种子扩展伪随机密钥，种子空间为1024。在每个区块中，(a) 显示经验 PSR 分布，(b) 显示学习得到的门限边界，(c) 显示门限结果和根识别准确率，(d) 显示排序参考相似度及校准接受阈值。

表 IV 相位密钥失配下的符号错误率、盲搜索成本和定位平均绝对误差： $N = 64, k = 5$，信噪比 $= 1$ 分贝， $\beta = 0.5$。

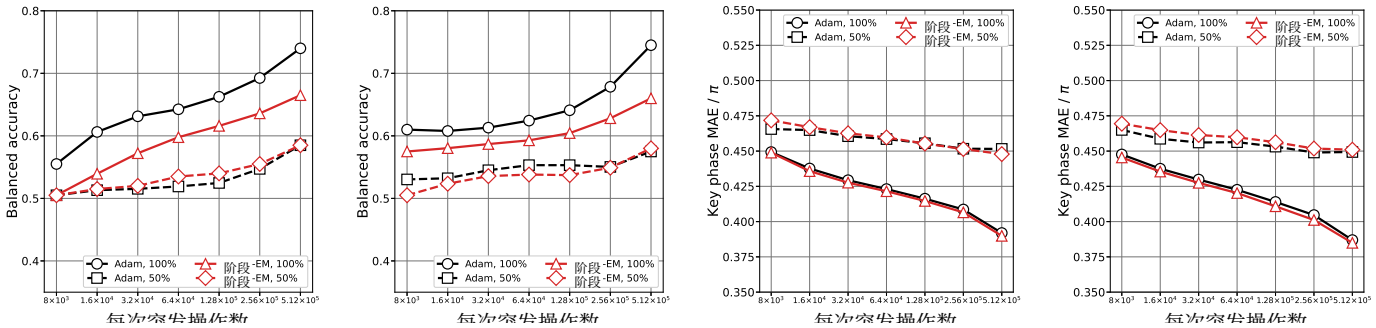
σ_ϕ (π)	**0**	**0.05**	**0.10**	**0.15**	**0.20**	**0.25**
SER	0.055	0.060	0.074	0.112	0.152	0.238
D_{MAE}	0.00	0.00	0.00	0.00	0.00	0.05
$\log_{10} C_{\mathrm{Eve}}$	–	515.1	418.7	369.2	322.4	291.4
σ_ϕ (π)	**0.30**	**0.35**	**0.40**	**0.45**	**0.50**	**–**
SER	0.289	0.377	0.529	0.527	0.581	–
D_{MAE}	0.74	9.27	29.37	29.22	31.22	–
$\log_{10} C_{\mathrm{Eve}}$	272.8	251.4	226.1	226.1	195.1	–

情况（无保护基线采用 $\beta = 0$），并在 1–10 分贝范围内独立采样信噪比。门控器使用来自每个标称根的 10 个突发，以及数量相同的随机序列；卷积神经网络则使用每个根对应的 30 个带根标签的标称突发。噪声、切向人工噪声和相位密钥均按突发独立重新生成。所有情况均采用相同的最大训练预算，即 60 个训练轮次；门控器和卷积神经网络的批量大小分别为 64 和 128。校准与测试彼此独立，其中包含 100 个已见标称样本、100 个未见标称样本和 100 个随机测试突发。每个参数采用 8 位量化后，共享密钥和平滑密钥每个突发分别使用 40 位和 120 位；扩展种子规则使用 10 位种子。因此，信令开销



(a) (b) (c) (d)

图4. 共享密钥下的基于在线拟合的检测与每个突发的操作预算之间的关系：不采用谐波结构初始化时的平衡检测准确率（a），以及采用谐波结构初始化时的标称序列接受率（b）；不采用谐波结构初始化时的相位密钥平均绝对误差（c），以及采用谐波结构初始化时的相位密钥平均绝对误差（d）。



(a) (b) (c) (d)

图5. 平滑位置相关密钥下的基于在线拟合的检测：不采用谐波结构初始化时（a）以及采用谐波结构初始化时（b）的平衡检测准确率；不采用谐波结构初始化时（c）以及采用谐波结构初始化时（d）的相位密钥平均绝对误差。

从种子扩展密钥增加到共享密钥再增加到平滑位置相关密钥。

在全部四种场景中，图3的（a）和（b）面板分别展示了标称/随机PSR分布，以及带有学习所得决策边界的联合PSR–归一化旁瓣能量空间。这些面板说明了Eve区分标称突发与随机突发的能力。对于无密钥基线，两类分布分离良好，从而能够实现可靠检测。在共享密钥、平滑密钥和种子扩展密钥下，两类分布逐渐合并，最后一种情况下几乎完全重叠。（c）面板报告了由此得到的门控器和根标识结果。在不使用密钥或人工噪声的情况下，Eve获得了95%的已见标称接受率、91%的未见标称接受率和随机突发拒绝率，以及95%的总体已见根识别率。共享密钥情况下，这些指标分别为75%、72%、68%和75%；平滑密钥情况下，分别为67%、60%、53%和57%。在通过门控器的突发中，已见根识别率分别为100%、100%和85.1%。在任一情况下的100个已见根采样点中，均没有错误根被接受。对于种子扩展密钥，强烈振荡的曲线表明，在固定学习预算下，门控器和卷积神经网络都未能学习到稳定的判别特征。

（d）面板显示入围候选项中的 maximumGF 得分；虚线表示校准阈值。对于无密钥和共享密钥 两种情况，得分分别列出；对于平滑密钥，得分部分重合；而对于种子扩展密钥，得分几乎无法区分。在最后一种情况下，上游门控器和卷积神经网络的失效也会阻碍有效校准。

相较于无保护基线，所有密钥规则都能降低根识别率。共享 k-阶段向量会从相邻符号乘积和中心化 Gram 特征中抵消，从而为 Eve 留下一种稳定特征。平滑密钥 会使该特征在不同符号间发生变化，而由共享种子和突发计数器扩展得到的伪随机掩码则消除了其重复使用，即使在固定预算下也仍然难以学习。有限的种子空间支持可处理的评估；更大的种子空间还可以在仅增加少量信令开销的情况下进一步增强密钥安全性。前两种规则的密钥生成成本可忽略不计，而种子扩展规则 要求两个合法节点执行相同的伪随机扩展，以额外计算量换取更低的信令开销和对波形学习攻击的抵抗能力。

3）基于在线拟合的检测：我们在两种情形下评估 Adam 和相位感知EM检测器。上界情形向 Eve 提供完整的标称序列，但不提供突发密钥或切向人工噪声实现。在部分知识情形下，50% 的位置具有标签：所有标签中有 40% 正确，10% 错误。Adam 在损失计算中排除未知位置，而相位感知EM检测器则为这些位置分配均匀的 QPSK先验。两种方法均采用 0.03 的学习率。在每个操作预算下，Eve 首先拟合候选波形并计算其拟合分数。随后，使用 50 个标称突发和 50 个随机突发对特定于方法的阈值进行校准，以最大化平衡准确率，并在评估过程中固定该阈值：低于阈值的分数判定为标称

表V 图6的感知仿真设置。

参数	值
标称序列 / 调和维数	$N = 64$ QPSK 符号 / $k = 5$
有效子载波 / 人工噪声占比	320 / $\beta = 0.5$
相位密钥规则 / 深度	平滑位置相关密钥/ 2弧度
发射 / 距离IFFT尺寸	512 / 4096
子载波间隔 / 采样率	120 千赫兹 / 61.44 兆采样/秒
循环前缀 / 完整符号持续时间	64 个采样点 / $9.375\ \mu$s
延迟 / 双基地超额路径分箱间隔	2.03 纳秒 / 0.61 米
每个回波的有用信号信噪比	-20 分贝/有效子载波
载波频率/回波间隔	3.5 GHz/1 ms
目标路径延迟（接收采样点）	$12 + \delta_0$、$21 + \delta_0$、$35 + \delta_0$；$\delta_0 \sim \mathcal{U}[-0.5, 0.5]$
相对目标路径功率	0, -8, -14 分贝
杂波延迟 / 相对功率	从10–50个样本中随机抽取 / -5, -10 分贝
路径相位 / 双基地路径长度变化率	每次蒙特卡洛运行独立 $\mathcal{U}[-\pi, \pi)$ / 1 米/秒接近
目标多普勒补偿	两台接收机；保留距离走动
Eve定时抖动	独立高斯分布，每个回波2纳秒均方根
搜索窗口宽度	40 m
单元平均恒虚警率保护单元 / 训练单元 / 步长	每侧 26 / 32 个单元 / 13 个分箱
虚警目标 / 锁定容差	全搜索范围 0.05 / ± 2 最近时延分箱

波形；否则，该突发将被拒绝。平衡准确率对名义接受率和随机拒绝率赋予相同权重。

图 4(a) 表明，两种方法的平衡准确率通常都会随着操作预算和名义序列知识水平的提高而提升。在掌握 50 % 信息的情况下，Adam 收敛更快，因为它只需根据已知位置优化密钥参数，而 EM 则必须联合更新未知符号后验概率和密钥。在图 4(b) 所示的结构化初始化下，有限样本接受率在测试预算中最小的情况下便达到 1。在图 4(c) 中，相位密钥的平均绝对误差会随着操作预算和名义序列知识的增加而降低。在图 4(c) 和 (d) 中，相位感知期望最大化在部分知识条件下均达到更低的平均绝对误差平台。错误标签会污染 Adam 的拟合集，而 EM 会在未知位置为四个 QPSK 候选分配后验概率，并在密钥更新中使用这些概率，从而减小错误标签的影响。

图5重复了对(28)中平滑密钥的评估。与包含 k 个相位的共享密钥不同，Eve必须估计 $3k$个参数，并在每个拟合步骤中重新生成一个 $N \times k$ 相位掩码，因此计算量显著增加。图5(a)和(b)分别报告了不含和含有
结构初始化。结构初始化并未显著提升性能，恢复完整的位置相关相位掩码仍然很困难。在最大操作预算下，精确掌握名义参数时，密钥的平均绝对误差约为 0.39π ；掌握50%信息时，约为 0.45π 。更大的操作预算可能会降低这些误差，但会增加搭载于无人机上的窃听者的计算负担。

C. 安全感知验证

此处，我们评估具有不完善阶段密钥知识的 Eve 所实施的相干感知攻击，并假设其拥有完备的标称序列知识和粗粒度突发定位能力。赋予 Eve 与合法接收机相同的波束成形增益，代表有利的截获几何关系。同时，假设 Eve 还拥有具有代表性的背景杂波与噪声观测

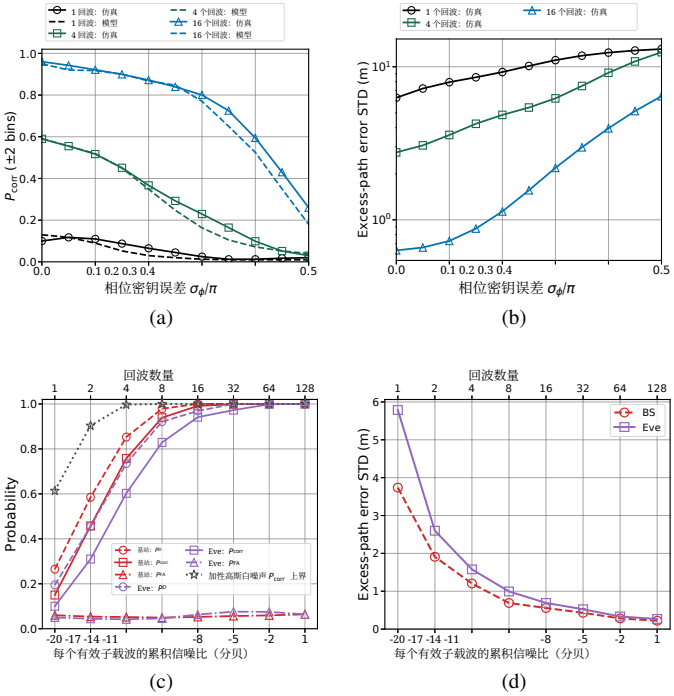


图6. 检测与时延锁定，$\beta = 0.5$：（a） P_{corr} 随密钥误差的变化，分别对应1、4和16个回波；（b）相应的模拟超额路径误差标准差；（c）检测概率和加性高斯白噪声（AWGN）上界随累积量的变化；（d）相应的超额路径误差标准差。在（c）–（d）中，Eve：$\sigma_\phi = 0.1\pi$。

用于恒虚警率（CFAR）校准。表V总结了图6的设置。

图6(a)比较了使用1、4或16个回波时的模型预测与波形仿真结果。式(45)和式(46)中的解析模型将波形失真转换为有效信噪比退化，以近似 P_{corr}。密钥误差增大通过两种相互耦合的效应降低正确锁定率：残余相位失配削弱相干相关，而错误切向方向会留下未抵消人工噪声。累积更多回波可提高正确锁定率，但较大的密钥误差仍会导致性能下降。图6(b)显示了相应的仿真超额路径误差标准差（STD），其中包括错误时延锁定。当密钥误差较小时，16个回波可保持亚米级标准差。随着失配增大，相干峰减弱，错误时延单元被选中的频率更高，从而增大误差离散程度。因此，更多回波既能提高锁定概率，也能提升定位精度，但无法消除对残余密钥误差和人工噪声误差的敏感性。

图6(c)–(d)比较了理想基站与 Eve 在相干回波累积下的检测性能和超额路径误差。基站能够完美解密钥波形并去除人工噪声；Eve 则使用错误的密钥估计人工噪声。两个接收机都知道标称参考信号。上方坐标轴给出回波计数 B；下方坐标轴采用共同的标称累积尺度 $-20 + 10\log_{10} B$ 分贝。尽管独立的密钥和人工噪声误差可以部分相互抵消，Eve 的时延锁定性能随累积增加而改善得较慢。然而，要达到所假设的密钥精度，仍需要先验信息和处理。在相干感知

攻击中，恢复共享查找表密钥 依赖于部分标称序列知识，而平滑的位置相关密钥 还需要付出高得多的拟合成本。对于种子扩展伪随机密钥，已知标称根时仍有 2^{λ} 个密钥种子候选项；若未进行根识别，联合穷举搜索则需考虑 $R2^{\lambda}$ 个根 – 种子对，其中 R 为候选根的数量。根识别可以缩小搜索范围，而不会泄露种子。

V. 讨论与结论

本文研究了针对搭载于无人机上的窃听者的通感一体化波形级安全性。我们结合傅里叶曲线调制、相位密钥和切向人工噪声，在保护感知参考信号的同时，维持合法通信与感知。为评估不同对手知识水平下的防护能力，我们考察了无密钥接收、离线序列识别、在线密钥拟合以及相干感知攻击。我们评估了三种密钥生成规则，并将相关的残余相位密钥误差和不完全人工噪声消除与正确时延锁定联系起来。数值结果表明，合法接收可靠，且 Eve 的推断性能有所降低。共享密钥仍保留可被利用的结构，平滑位置相关密钥增加了拟合难度，而在固定预算下，经评估的检测器仍难以学习由种子扩展的伪随机密钥。

所提出的框架在空间波束成形之外实现了波形级防护，同时也明确了其局限性。这些发现促使我们进一步研究波形与空间联合防护、长时观测攻击评估，以及针对受限对手的密钥恢复时延和能量测量。

参考文献

[1] F. Liu、C. Masouros、A. P. Petropulu、H. Griffiths 和 L. Hanzo，“联合雷达与通信设计：应用、最新进展与未来方向”，*IEEETrans.Commun.*，第 68 卷，第 6 期，第 3834–3862 页，2020 年。[2] K. Qu、J. Ye、X. Li 和 S. Guo，“泛在通感一体化中的隐私与安全：威胁、挑战与未来方向”，*IEEE Internet Things Mag.*，第 7 卷，第 4 期，第 52–58 页，2024 年。[3] J. Wang、H. Du、Y. Liu、G. Sun、D. Niyato、S. Mao、D. I. Kim 和 X. Shen，“基于生成式人工智能的ISAC网络安全无线感知”，*IEEE Trans. Inf. ForensicsSecurity*，第 20 卷，5210，2025 5195页。– 。[4] J. Zou、C. Masouros、F. Liu 和 S. Sun，“保障ISAC网络中的感知功能：一种人工噪声设计”，*IEEE Trans. Veh. Technol.*，第 73 卷，第 11 期，第 17 800–17805 页，2024 年。[5] H. D. Griffiths 和 C. J. Baker，“无源相干定位雷达系统。第 1 部分：性能预测”，*IEE Proc., Radar Sonar Navig.*，第 152 卷，第 3 期，第 153–159 页，2005 年。[6] P. E. Howland、D. Maksimiuk 和 G. Reitsma，“基于调频广播的双基地雷达”，*IEE Proc., Radar Sonar Navig.*，第 152 卷，115，2005 3，107 no. pp. – 。[7] J. Liu、H. Li 和 B. Himed，“无源雷达应用中互相关检测器的性能研究”，*Signal Process.*，第 113 卷，第 32–37 页，2015 年。[8] G. P. Blasone 、 F. Colone 、 P. Lombardo 、 P. Wojaczek 和 D. Cristallini，“具有自适应信道校准的无源雷达DPCA方案”，*IEEE Trans. Aerosp. Electron. Syst.*，第 56 卷，第 5 期，第 4014–4034 页，2020 年。[9] S. Searle 和 K. Do˘ganc¸ay，“存在采样时钟偏移时的无源雷达信号处理”，*IEEE Trans. Aerosp. Electron. Syst.*，第 57 卷，第 5 期，第 3029–3041 页，2021 年。[10] S. Goel 和 R. Negi，“利用人工噪声保证保密性”，*IEEE Trans. Wireless Commun.*，第 7 卷，第 6 期，第 2180–2189 页，2008 年。

[11] T. Matsumine、H. Ochiai 和 J. Shikata，“一体化感知与通信的物理层安全：综述”，*IEEE Open J. Commun. Soc.*，第 6 卷，第 6690–6743 页，2025 年。[12] Z. Ren、J. Xu、L. Qiu 和 D. W. K. Ng，“存在信息窃听者与感知窃听者时的安全无蜂窝一体化感知与通信”，*IEEE J. Sel. Areas Commun.*，第 42 卷，第 11 期，第 3217– 3231 页，2024 年。[13] Y. Huang、Z. Zhu、Q. Cui、N. Wei、X. Tao 和 P. Zhang，“ISAC隐私保护：通过联合波束成形与扰动实现信号不可辨识性”，*IEEE Trans. Cogn. Commun. Netw.*，第 12 卷，第 9790– 9805 页，2026 年。[14] P. P. Papanikolaou、D. Bozanis、S. A. Tegos、C. Masouros 和 G. K. Karagiannidis，“窃听者不确定性下具有感知隐私的安全ISAC”，*arXiv preprint arXiv:2609.25798*，2026 年。[15] K. Han、K. Meng 和 C. Masouros，“感知安全ISAC：用于削弱未授权感知的模糊函数工程”，*IEEE Trans. Wireless Commun.*，第 25 卷，第 5386–5400 页，2026 年。[16] B. Du、K. Han 和 C. Masouros，“保障ISAC中的感知功能：基于KLD的模糊函数整形”，*npj Wirel. Technol.*，第 2 卷，第 79 页，2026 年。[17] U. U. Erdem、L. Giroto、T. Chaloun、T. Schipper、T. Jeong、C. Karle、B. Nuss 和 T. Zwick，“面向ISAC的安全OFDM波形设计：针对被动感知的人工相位-多普勒偏移”，*arXiv preprint arXiv:2602.23861*，2026 年。[18] M. Temiz、C. Horne、M. Ritchie 和 C. Masouros，“基于FMCW的安全ISAC传输”，载于*Proc. Int. Symp. Commun. Syst. Netw. Digit. Signal Process. (CSNDSP)*，2026 年，第 1–6 页。[19] Y. Zhang、Y. Bai、R. Jantti、Z. Han 和 C. Masouros，“AmbSentry：利用环境物联网设备缓解ISAC系统中的感知窃听”，*arXiv preprint arXiv:2608.11799*，2026 年。[20] M. F. Keskin、K. Han、H. Wymeersch 和 C. Masouros，“利用相位噪声实现ISAC系统中的感知隐私”，*arXiv preprint arXiv:2608.13270*，2026 年。[21] B. Han、H. Chen、M. Sun、H. V. Poor 和 H. D. Schotten，“带切向噪声的傅里叶曲线星座上的匹配译码与欧氏失配译码”，*IEEE Commun. Lett.*，第 30 卷，第 2510–2514 页，2026 年。[22] 3GPP，“NR；物理信道与调制”，3GPP TS 38.211，2025 年。[23] ——，“NR；数据物理层过程”，3GPP TS 38.214，2025 年。[24] Z. Fang、B. Han、S. Li 和 H. D. Schotten，“面向安全ISAC的波形随机化”，arXiv preprint arXiv:2610.07994，2026 年，已提交至 IEEE ICC 2027。[25] E. Barker 和 J. Kelsey，“使用确定性随机比特生成器的随机数生成建议”，美国国家标准与技术研究院，技术报告 NIST Special Publication 800- 90A Revision 1，2015 年。[26] D. P. Kingma 和 J. Ba，“Adam：一种随机优化方法”，arXiv preprint arXiv:1412.6980，2014 年。[27] K. Zhong、J. Hu、Y. Cong、G. Cui 和 J. Wu，“RMOCG：一种基于黎曼流形优化的用于仅相位波束成形综合的共轭梯度法”，*IEEE Antennas Wireless Propag. Lett.*，第 21 卷，第 8 期，第 1625–1629 页，2022 年。[28] A. P. Dempster、N. M. Laird 和 D. B. Rubin，“通过EM算法从不完整数据中进行最大似然估计”，*J. R. Stat. Soc. Ser. B (Methodol.)*，第 39 卷，第 1 期，第 1–22 页，1977 年。[29] T. K. Moon，“期望最大化算法”，*IEEE Signal Process. Mag.*，第 13 卷，第 6 期，第 47–60 页，1996 年。[30] J. Choi，“利用近似EM算法进行频域均衡的联合信道估计与数据检测”，*Signal Pro- cess.*，第 84 卷，第 5 期，第 865–880 页，2004 年。