

基于联合时序预测网络学习的物理层密钥生成方法

叶宁, 杨林霏, 郑萌, 丁菁芳

(东北大学计算机科学与工程学院, 辽宁 沈阳 110819)

摘要: 物理层密钥生成是一种利用无线信道随机性、互易性和空间去相关性, 从合法通信双方的观测信号中提取共享密钥的技术。现有密钥生成方法大多仅依赖于瞬时的采样值, 无法有效提取时序动态特征, 且难以适配信道慢变化场景; 此外, 由于非理想互易信道产生的双方信道状态观测偏差, 经过量化后会导致密钥不一致率上升。针对上述问题, 本文提出一种基于联合时序预测网络架构的物理层密钥生成方法。该方法首先构建一个基于门控循环单元编码器的预测网络, 以收发双方未来时刻的信道状态作为预测目标对网络进行训练, 从而获得能够刻画双方共有信道演化规律的基础模型。在此基础上, 进一步将收发双方提取的特征差异作为网络训练的损失函数, 对网络进行微调, 以引导双方特征趋于一致。最后, 为降低量化导致的密钥不一致, 将量化误差作为新的网络训练损失函数, 对网络进行再次微调, 使网络在特征提取时兼顾后续量化, 从而降低密钥不一致率。仿真结果表明, 在全信噪比范围内, 与基于幅度/相位量化的物理层密钥生成方法相比, 所提方法可将密钥不一致率降低 58% 以上; 与现有基于深度学习的物理层密钥生成方法相比, 所提方法可将密钥不一致率降低 23% 以上。

关键词: 物理层密钥; 时序预测网络; 信道特征提取; 物理层安全

Physical Layer Key Generation Method Based on Joint Temporal Prediction Network Learning

Ye Ning, Yang Linfei, Zheng Meng, Ding Jingfang

School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China

Abstract: Physical layer key generation technique extracts shared keys from observed signals of legitimate communication parties by exploiting the randomness, reciprocity and spatial decorrelation of wireless channels. Most existing key generation methods rely only on instantaneous sampling values, failing to effectively extract temporal dynamic features and adapt to slow-varying channel scenarios. In addition, the observation discrepancy of channel states at both ends caused by non-ideal reciprocal channels leads to an increased key disagreement rate after quantization. To address these issues, a physical layer key generation method based on a joint temporal prediction network architecture is proposed. First, a prediction network based on a gated recurrent unit encoder was constructed and trained with the channel states of both the transmitter and receiver at future moments as the prediction target, yielding a base model capable of characterizing the common channel evolution law of both parties. On this basis, the feature discrepancy between the two parties was further introduced as the loss function to fine-tune the network, guiding the features of both sides toward consistency. Finally, to reduce the key disagreement caused by quantization, the quantization error was incorporated as a new loss function for a second round of fine-tuning, so that the network takes subsequent quantization into account during feature extraction, thereby lowering the key disagreement rate. Simulation results show that over the entire SNR range, the proposed method reduces the key disagreement rate by more than 58% compared with amplitude/phase quantization-based physical layer key generation methods, and by more than 23% compared with existing deep learning-based physical

收稿日期: XXXX-XX-XX; 修回日期: XXXX-XX-XX

通信作者: 郑萌, zhengmeng@cse.neu.edu.cn

基金项目: 国家自然科学基金资助项目(No.62603127)

Foundation Items: The National Natural Science Foundation of China (No.62603127)

layer key generation methods.

Key words: Physical layer secret key, Time-series prediction network, Channel feature extraction, Physical layer security

0 引言

随着工业物联网、智能制造、车联网及大规模传感网络的快速发展,终端设备数量急剧增加且普遍资源受限,迫切需要一种低功耗、轻量化的安全通信方式。传统密码体系通常依赖密钥预分发、公钥基础设施或复杂密钥管理机制,在动态部署、节点规模大的场景中会带来较高的计算与运维开销。物理层密钥生成利用无线信道的随机性、短时互易性和空间去相关性,从合法通信双方观测到的信道状态信息(Channel State Information, CSI)中提取共享密钥,为物联网轻量化安全通信提供了关键技术支撑^[1-3]。近年来,物理层密钥生成在理论模型、性能分析以及实际无线系统应用方面已取得大量研究成果^[4-6]。

物理层密钥早期研究主要从接收信号强度、CSI幅度、相位或OFDM子载波响应中提取密钥。Mathur等提出Radio-Telepathy协议,利用信道幅度交叉事件生成共享比特^[7];Patwari等通过插值、去相关和多比特量化提高密钥生成速率^[8];Zhao等提出基于接收信号强度的自适应量化密钥生成方案^[9];Wang等进一步利用无线信道相位随机性实现快速密钥生成^[10]。此外,李小倩等对相位信息进行物理层加密^[11];Wan等利用同时透射和反射可重构智能超表面生成物理层密钥^[12]。然而,上述传统方法均建立在理想互易性假设之上,在实际无线通信环境中,该假设无法成立,使得此类方法在现实部署中性能显著下降。

近年来,深度学习被引入物理层密钥生成,用于复杂信道特征提取、非理想互易补偿和共享表示学习。例如,Jiang等通过联合优化和对比学习网络增强合法双方共享表示的一致性^[13];Zhang等针对FDD系统上下行信道不互易问题,利用深度学习建立频段间共享特征映射^[14-15]。Chen等提出基于特征融合自编码器的MIMO系统物理层密钥生成方案^[16];Li等结合自编码器和K-Means量化方法,实现智能反射面辅助的密钥生成^[17]。针对非理想互易问题,Chen等提出信道互易补偿网络CRCNet,通过学习收发双方信道测量之间的映射关系校正互易性偏差来降低密钥不一致率^[19];Guo

等提出互信息驱动自编码器MIAE来提取双方互易特征,并引入互信息神经估计构造训练目标以提升密钥生成速率^[20]。在时序建模方面,Wang等结合LSTM与Kalman滤波对动态环境下的RSS测量进行平滑^[21];Mahalal等利用LSTM-RNN预测量化后的密钥序列以降低LiFi网络中的密钥不一致率^[22]。这些研究表明,深度学习网络能够从复杂的信道观测中挖掘出比幅度、相位等传统特征更深层次的特征。然而,现有基于深度学习的物理层密钥生成方法,大多仅聚焦于收发双方从信道中提取的瞬时特征。文献[21]和文献[22]虽引入时序建模,但未从学习收发双方共享信道演化规律的角度挖掘CSI序列中蕴含的时序信息。另一方面,前述方法的模型训练通常仅考虑特征层面的相似性,当双方特征向量位于码本边界两侧时,微小的特征差异也可能被映射为不同码字,从而导致密钥不一致。

上述局限在信道慢变化场景中尤为突出,此时相邻CSI观测高度相关,单次采样新增的信息量十分有限,进而制约了密钥生成速率;同时,信道自身变化幅度减小,收发双方的CSI观测差异更多地来自噪声与本地扰动,在量化时更易被映射为不同码字^[23-24],导致密钥不一致率(Key Disagreement Rate, KDR)进一步上升。但强时间相关性并非只有负面影响,CSI序列中蕴含着信道随时间演化的规律,该规律可为密钥生成提供关键指导。

对比预测编码(Contrastive Predictive Coding, CPC)通过构建未来状态预测任务学习序列中的长期依赖关系,为无监督时序表示学习提供了一种有效方法^[18]。受此启发,本文提出基于联合时序预测网络(Joint Temporal Prediction Network, JTPNet)的物理层密钥生成方法。该方法通过收发双方互相预测来学习信道中共有的演化规律,并在此基础上设计特征一致性与量化误差两项训练机制,以提升最终密钥的一致性。本文的主要贡献如下:

(1) 构建了一个基于门控循环单元(Gated Recurrent Unit, GRU)编码器的预测网络。网络以收发双方连续探测窗口内的CSI序列作为输入,通过逐帧编码器提取每个时刻的瞬时特征,并利用双层

GRU 沿时间轴聚合历史信息。在此基础上, 设计收发双方双向未来状态预测任务, 即利用 Alice 的历史特征预测 Bob 的未来特征, 同时利用 Bob 的历史特征预测 Alice 的未来特征, 使网络在训练过程中自发学习并提取双方共有的信道演化规律。

(2) 设计了基于两阶段微调的训练机制。在基础模型训练完成后, 首先将收发双方提取的特征差异作为训练目标, 对网络进行微调, 以引导双方特征趋于一致; 随后, 进一步将量化误差引入网络训练目标, 对网络进行再次微调, 使网络在特征提取阶段兼顾后续的量化, 从而降低 KDR。

(3) 验证了 JTPNet 生成密钥的一致性与随机性。仿真结果表明, 在全信噪比范围内, 所提方法的密钥不一致率较基于幅度/相位量化的方法降低 58% 以上, 较现有基于深度学习的方法降低 23% 以上。与此同时, 生成的密钥通过 NIST SP800-22 全部 15 项随机性测试, P-value 均大于 0.01。

1 系统模型

1.1 系统场景与信号模型

本文考虑 TDD 模式下的 OFDM 通信系统, 系统包含 N_{sc} 个子载波, 导频功率为 P_p 。合法通信双方 Alice 与 Bob 在相干时间内交替发送导频以获取 CSI。在探测阶段, 设第 t 个探测时隙、第 n 个子载波上, Alice 到 Bob 方向的信道频域响应记为 $H_{AB}(t, n)$, Bob 到 Alice 方向的信道频域响应记为 $H_{BA}(t, n)$ 。

以 Alice 向 Bob 发送导频为例, Bob 的接收信号可表示为:

$$Y_B(t, n) = \sqrt{P_p} H_{AB}(t, n) S_A(t, n) + V_B(t, n), \#(1)$$

其中, $S_A(t, n)$ 为 Alice 发送的导频符号, $V_B(t, n)$ 为接收端的加性高斯白噪声及残余干扰。

在导频符号已知的条件下, 接收端采用最小二乘法 (Least Squares, LS) 进行信道估计, 获得 CSI 观测。由于系统工作在 TDD 模式下, 当双向探测间隔远小于信道相干时间时, Alice 与 Bob 观测到的物理信道具有短时互易性, 即 $H_{AB}(t, n) = H_{BA}(t, n) = H(t, n)$ 。

然而, 在实际通信系统中, 射频链路响应不一致、收发器本振相位噪声及 LS 信道估计误差等因素会共同破坏理想互易性。为描述这一现象, 将 Alice 与 Bob 实际获得的信道估计值表示为:

$$\hat{H}_A(t, n) = H(t, n) + \Delta_A(t, n),$$

$$\hat{H}_B(t, n) = H(t, n) + \Delta_B(t, n), \#(2)$$

其中, $\Delta_A(t, n)$ 和 $\Delta_B(t, n)$ 分别表示 Alice 端和 Bob 端的本地扰动。因此, 实际物理层密钥生成需要在保留共同信道随机性的同时, 抑制本地扰动造成的双方观测差异, 从含噪且随机的 CSI 观测中提取具有高一致性的共享信道特征。

1.2 窃听模型与信道空间相关性度量

如图 1 所示, 在密钥生成过程中, 假设存在窃听者 Eve, 其可以监听 Alice 与 Bob 之间传输的导频信号。由于无线信道具有空间去相关性, 当 Eve 与合法通信双方的距离大于信号半波长时, Eve 观测到的信道与合法信道在统计上相互独立, Eve 难以从自身观测中获得与合法双方一致的物理层密钥, 这为密钥安全性提供了物理层保障。

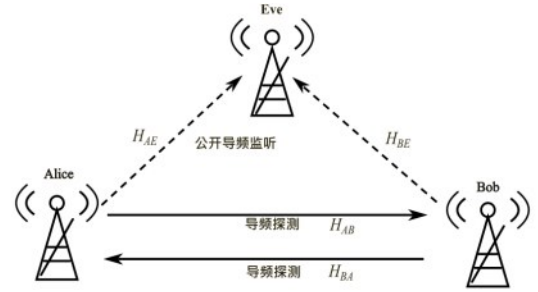


图1 Alice-Bob-Eve 导频探测与威胁模型

为了定量评估窃听者对密钥安全性的潜在威胁, 本文引入空间相关系数来刻画窃听信道与合法信道之间的统计相关程度。由于 OFDM 系统具有频率选择性衰落, 不同子载波上的空间相关程度存在差异。考虑第 t 个探测时隙、第 n 个子载波上, 令 $H_{AE}(t, n)$ 与 $H_{BE}(t, n)$ 分别表示 Alice 到 Eve 和 Bob 到 Eve 之间的信道频域响应。于是, 合法信道频域响应 $H_{AB}(t, n)$ 与窃听信道频域响应 $H_{AE}(t, n)$ 之间的空间相关系数 ρ_{AE} 定义为:

$$\rho_{AE} = \frac{\mathbb{E}[H_{AB}(t, n) H_{AE}^*(t, n)]}{\sqrt{\mathbb{E}[|H_{AB}(t, n)|^2] \cdot \mathbb{E}[|H_{AE}(t, n)|^2]}}, \#(3)$$

其中, $\mathbb{E}[\cdot]$ 表示数学期望, $(\cdot)^*$ 表示复共轭。理想情况下, 空间去相关性使合法信道与窃听信道相互独立, 即 $\rho_{AE} = 0$ 。在实际环境中, 受散射体分布和天线间距的限制, ρ_{AE} 通常大于零。因此, ρ_{AE} 可用于刻画窃听信道与合法信道的相关程度。在仿真

验证中, 本文以 ρ_{AE} 作为控制参数, 分析不同空间相关性条件下 Eve 的 KDR, 以验证所提方法在对抗被动窃听方面的鲁棒性。

1.3 CSI时序观测模型

在物理层密钥生成的探测阶段, Alice 与 Bob 在连续时间窗内获取 CSI 观测。在本文中, CSI 指本地信道估计获得的复数信道频域响应采样序列。在信道慢变化场景中, CSI 观测具有显著的时间相关性。取滑动窗口长度为 W , Alice 和 Bob 在时刻 t 获取的 CSI 序列分别表示为:

$$\mathbf{H}_A(t) = [\hat{H}_A(t-W+1, 1), \dots, \hat{H}_A(t-W+1, N_{sc}); \dots; \hat{H}_A(t, 1), \dots, \hat{H}_A(t, N_{sc})] \# \quad (4)$$

$$\mathbf{H}_B(t) = [\hat{H}_B(t-W+1, 1), \dots, \hat{H}_B(t-W+1, N_{sc}); \dots; \hat{H}_B(t, 1), \dots, \hat{H}_B(t, N_{sc})] \# \quad (5)$$

由式(4)和(5)知, 连续 W 个时隙的观测构成观测矩阵 $\mathbf{H}_A(t), \mathbf{H}_B(t) \in \mathbb{C}^{W \times N_{sc}}$, 其中行数对应时间窗口长度 W , 列数对应子载波数 N_{sc} 。

由于 Alice 和 Bob 在短时间内观测同一传播环境, 其 CSI 序列兼具信道互易性与时间相关性, 连续观测窗口中蕴含双方共有的信道演化规律。然而, 由于双方存在不同的本地扰动

$$\Delta_A(t, n) \neq \Delta_B(t, n), \#(6)$$

收发双方的 CSI 序列在每一时刻均难以完全一致。若仅利用单次瞬时 CSI 观测进行量化, 由于缺乏历史信息来校正上述扰动, 观测值易被映射至不同码字, 从而导致密钥不一致。因此, 如何在利用时序相关性的同时抑制非理想互易引入的观测偏差, 是后续特征提取与量化过程需要解决的关键问题。

2 基于 JTPNet 的物理层密钥生成方法

2.1 总体目标与框架

针对 1.3 节所述的时序 CSI 观测与非理想互易问题, 本文提出基于 JTPNet 的物理层密钥生成方法。所提方法由离线网络训练和在线密钥生成两个阶段组成。离线阶段首先利用收发双方连续 CSI 序列构建未来状态预测任务, 使网络学习共享信道演化规律; 随后依次引入特征一致性损失和量化误差损失, 对网络进行阶段性训练, 并利用训练阶段获得的特征构建固定码本。

图 2 给出了训练完成后的在线密钥生成流程。Alice 与 Bob 分别对连续探测得到的观测序列进行窗口划分, 并将其输入共享参数的 JTPNet, 通过前向计算获得对应的特征向量 $\mathbf{r}_u$ 。随后, 双方利用离线阶段构建的固定码本, 通过量化函数 $Q(\cdot)$ 将连续特征映射为码字索引, 进而生成密钥序列 $\mathbf{b}_u$ 。最后, 通过信息协商纠正少量不一致位, 并进行隐私放大, 得到最终共享会话密钥 K 。

JTPNet 的具体网络结构及双向未来状态预测机制将在 2.2 节介绍, 特征一致性损失与量化误差损失将在 2.3 节给出, 多阶段训练过程及在线生成步骤将在 2.4 节进一步说明。

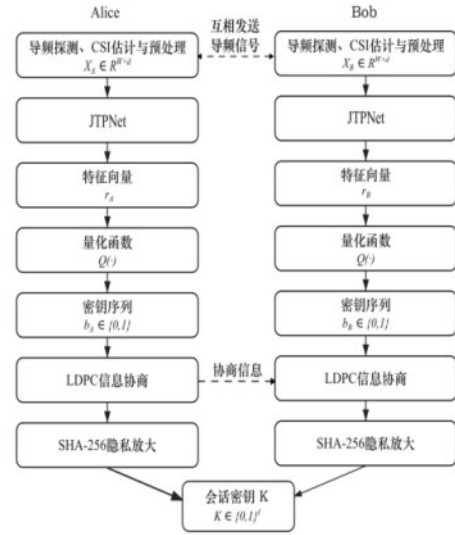


图2 基于 JTPNet 的密钥生成框图

2.2 收发双方双向预测的时序特征提取

如 2.1 节所述, JTPNet 需从 CSI 序列中提取收发双方共有的动态特征。为实现该目标, 本文引入 CPC 的思想, 设计了一个收发双方互相预测的任务, 即利用 Alice 的历史 CSI 窗口预测 Bob 未来时刻的特征状态, 同时利用 Bob 的历史窗口预测 Alice 未来时刻的特征状态。

由于网络输入要求为实数, 本文首先对 1.3 节所述原始 CSI 观测进行预处理, 将每个时刻的 N_{sc} 维复数子载波响应按实部与虚部分解并拼接, 转换为 d 维实数特征向量, 得到网络输入序列。如图 3 所示, 对于 Alice 或 Bob 的一段输入序列, 记 $\mathbf{X}_u$ 为 1.3 节原始复数观测经预处理后的实数形式, 即

$$\mathbf{X}_u = [\mathbf{x}_u(1), \mathbf{x}_u(2), \dots, \mathbf{x}_u(W)] \in \mathbb{R}^{W \times d},$$

$$u \in \{A, B\}, \#(7)$$

其中, $\mathbf{x}_u(t)$ 为第 t 个探测时刻的实数特征向量, W 为序列长度, d 为输入特征维度。

共享逐帧编码器 $g_\phi(\cdot)$ 将每个时刻的特征映射为中间表示:

$$\mathbf{z}_u(t) = g_\phi(\mathbf{x}_u(t)). \#(8)$$

$g_\phi(\cdot)$ 由两个全连接层组成, 用于提取瞬时特征。第一个全连接层 (Fully Connected layer 1, FC1) 将输入特征维度 d 映射为隐藏层维度 h_1 ; 第二个全连接层 (Fully Connected layer 2, FC2) 将其映射为特征维度 d_z 。FC1 与 FC2 之间依次经过批量归一化 (Batch Normalization, BN)、ReLU 激活函数以及 Dropout 层, 随后对 FC2 输出特征进行归一化, 得到 $\mathbf{z}_u(t)$ 。

$g_\phi(\cdot)$ 输出的瞬时特征仅反映了当前时刻的信道状态, 难以直接体现完整观测窗口内的时序变化。为此, 本文进一步利用双层 GRU 沿时间维度聚合历史信息, 得到历史特征: $\mathbf{c}_u(t) = GRU_\theta(\mathbf{z}_u(1), \mathbf{z}_u(2), \dots, \mathbf{z}_u(t)). \#(9)$ GRU 仅依赖当前及过去时刻输入, 适用于在线密钥生成。在线生成阶段, 以窗口末端 GRU 输出 $\mathbf{c}_u(W) \in \mathbb{R}^{d_h}$ 为历史特征, 经线性投影层映射为 d_r 维最终特征向量: $\mathbf{r}_u = \mathbf{W}_p \mathbf{c}_u(W) + \mathbf{b}_p, u \in \{A, B\}, \#(10)$ 其中, 投影层由可学习的权重矩阵 $\mathbf{W}_p \in \mathbb{R}^{d_r \times d_h}$ 与偏置向量 $\mathbf{b}_p \in \mathbb{R}^{d_r}$ 实现。

为利用历史信息预测未来时刻的信道特征, 本文将历史特征 $\mathbf{c}_u(t)$ 输入一个预测头 $p_k(\cdot)$ 。该预测头由多层感知机 (Multi-Layer Perceptron, MLP) 实现, 用于输出未来时刻的预测特征。具体而言, 给定 Alice 的历史特征 $\mathbf{c}_A(t)$, 预测头生成 Bob 在未来 $t+k$ 时刻特征的预测值 $\hat{\mathbf{z}}_B(t+k)$; 反之, 预测头利用 Bob 的历史特征 $\mathbf{c}_B(t)$ 生成 Alice 在未来 $t+k$ 时刻的特征预测值 $\hat{\mathbf{z}}_A(t+k)$ 。于是可得:

$$\hat{\mathbf{z}}_v(t+k) = p_k(\mathbf{c}_u(t)),$$

$$(u, v) \in \{(A, B), (B, A)\}, t = 1, \dots, W - k. \#(11)$$

预测所需的监督信号无需人工标注, 而是通过共享编码器与双层 GRU 从另一方未来时刻的真实 CSI 序列中提取得到, 即双方以各自网络输出的特征作为对方预测的监督信号。该任务采用 InfoNCE 损失函数来训练。以 Alice 预测 Bob 为例, 设

$\text{sim}(a, b)$ 为向量 a 与 b 之间的余弦相似度, 则 InfoNCE 损失定义为:

$$\mathcal{L}_{\text{CPC}}^{A \rightarrow B} = - \sum_{i=1}^{W-k} \log \left[\frac{\exp(\text{sim}(\hat{\mathbf{z}}_B(t+k), \mathbf{z}_B(t+k))/\tau_c)}{\exp(\text{sim}(\hat{\mathbf{z}}_B(t+k), \mathbf{z}_B(t+k))/\tau_c) + \sum_{z_j \in \Omega} \exp(\text{sim}(\hat{\mathbf{z}}_B(t+k), \mathbf{z}_j)/\tau_c)} \right] \#(12)$$

其中, $\mathbf{z}_j$ 为负样本特征, 负样本集合 Ω 由同一观测窗口内除预测目标时刻 $t+k$ 外其余时刻的特征构成, 即 $\Omega = \{\mathbf{z}_j | 1 \leq j \leq W, j \neq t+k\}, |\Omega| = W - 1$, τ_c 为 InfoNCE 温度系数, 刻画损失函数对负样本的敏感度。

上述预测任务的训练目标促使编码器优先保留收发双方共同经历的时变信道信息, 同时抑制单次观测中独立的随机噪声成分。经预测任务训练后的编码器与 GRU 能够输出具有时序一致性的特征向量, 为后续的特征一致性训练与量化训练提供稳定输入。

2.3 特征一致性与量化误差

经过 2.2 节所述的预测任务训练, 编码器与 GRU 提取的特征能够反映收发双方共有的信道演化规律。然而, 由于预测任务分别在 Alice 端和 Bob 端的观测序列上独立执行, 并未直接对双方最终输出的特征施加限制, 因此仅凭预测任务难以保证双方特征高度一致。为此, 本文考虑特征一致性要求, 将双方特征向量之间的欧氏距离作为训练目标, 通过最小化 $\mathcal{L}_{\text{align}}$ 使双方特征趋于一致:

$$\mathcal{L}_{\text{align}} = \frac{1}{d_r} \|\mathbf{r}_A - \mathbf{r}_B\|_2^2. \#(13)$$

然而, 特征向量在数值上的接近并不能保证量化后比特的一致性。当 Alice 与 Bob 的特征向量位于码本边界两侧时, 即使 $\mathcal{L}_{\text{align}}$ 很小, 也可能被映射到不同的码字索引, 从而导致密钥不一致。因此, 本文进一步考虑量化误差, 将该误差作为损失项纳入训练目标。

为实现特征向量到码字的映射, 离线阶段采用 K-Means 聚类对训练特征进行划分, 将特征空间划分为有限数量的离散区域, 得到包含 M 个码字中心的量化码本:

$$\mathbf{C} = \{\mathbf{m}_1, \mathbf{m}_2, \dots, \mathbf{m}_M\}. \#(14)$$

其中, $\mathbf{m}_i$ 表示第 i 个聚类中心。在线密钥生成阶

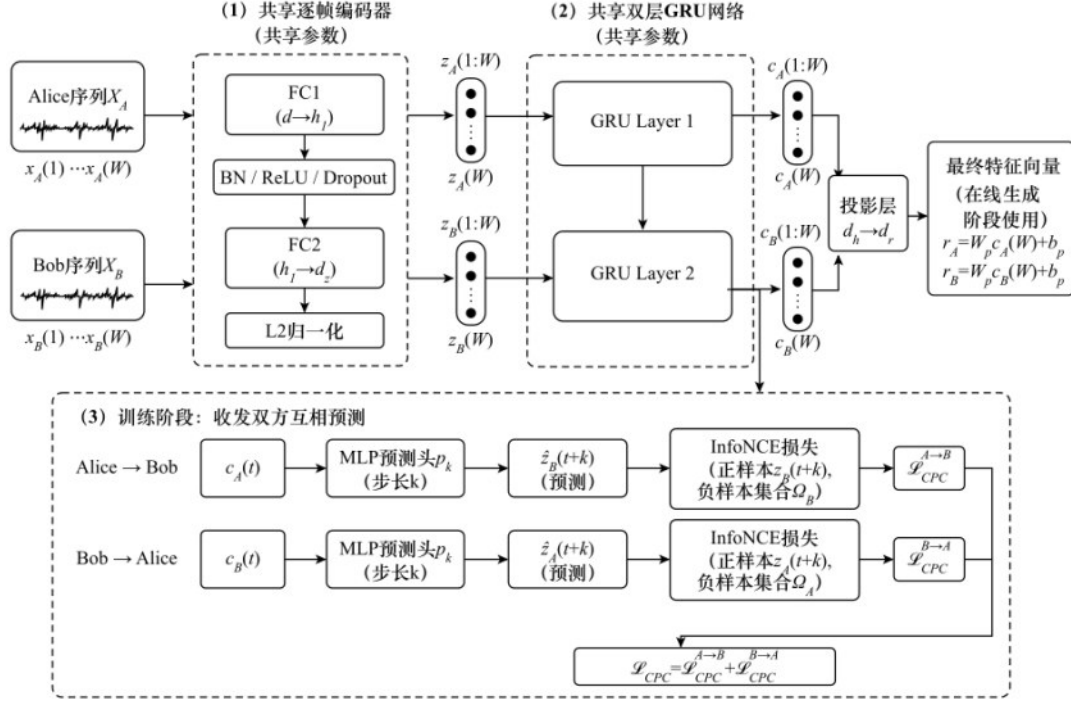


图3 JTPNet的收发互预测结构

段, 特征通过最近邻规则映射至对应码字索引:

$$i_u = \arg \min_i \|r_u - m_i\|_2^2, \quad u \in \{A, B\}, \#(15)$$

索引 i_u 经编码后转换为密钥。由于最近邻量化函数不可导, 梯度无法反向传递至编码器参数。为此, 本文在训练阶段引入基于软量化温度系数 τ_q 的软量化机制^[23-24]。在这一机制下, 特征向量 r_u 被分配至第 i 个码字的软概率 $q_i(r_u)$ 定义为:

$$q_i(r_u) = \frac{\exp(-\|r_u - m_i\|_2^2 / \tau_q)}{\sum_{j=1}^M \exp(-\|r_u - m_j\|_2^2 / \tau_q)}. \#(16)$$

当软量化温度系数 $\tau_q \rightarrow 0$ 时, 式(16)退化为式(15)所示的硬最近邻量化规则。基于软概率分布(16), 可衡量Alice端与Bob端码字分配概率的一致性。本文采用对称交叉熵度量双方码字分配概率分布的差异, 定义量化误差损失为:

$$\mathcal{L}_{QACL} = -\frac{1}{2} \sum_{i=1}^M \left[q_i(r_A) \log q_i(r_B) + q_i(r_B) \log q_i(r_A) \right]. \#(17)$$

通过最小化 $\mathcal{L}_{QACL}$, 网络的训练过程能够充分考虑量化结果。不同于式(13)仅考虑特征向量在数值上的接近程度, 式(17)直接作用于码字的概率分布, 从而减少量化过程中可能出现的错误。上述特征一致性损失(13)与量化误差损失(17)将在2.4节的

多阶段训练中分阶段引入并最小化。

2.4 多阶段训练与在线生成

考虑收发双方未来状态预测损失 $\mathcal{L}_{CPC}$ 、特征一致性损失 $\mathcal{L}_{align}$ 与量化误差损失 $\mathcal{L}_{QACL}$ 三个训练目标, 采用多阶段训练, 并在在线阶段执行低复杂度的前向推理。量化损失需基于码本计算, 而网络参数更新会改变特征分布, 可能导致码本与特征分布不匹配。为此, 首先通过预测训练和一致性训练学习特征, 再根据训练特征构建码本, 最后固定码本进行量化微调, 具体过程如算法1所示。

第一阶段独立执行收发双方未来状态预测预训练, 促使编码器初步捕捉收发双方共享的动态特征; 第二阶段冻结预测头 p_k , 仅微调编码器与GRU以增强双方特征的一致性; 第三阶段基于已学得特征构建固定码本, 并引入量化误差损失进行再次微调。

需指出的是, 在第三阶段的微调中, 码本始终保持不变。由于引入量化误差损失旨在减少量化过程中的错误映射, 因此该阶段仅对编码器和GRU参数进行小幅调整。若参数变化过大, 特征分布可能超出已有码本的覆盖范围, 从而导致码本失效。为防止这一问题, 微调时采用较小的学习率, 将参数更新限制在较小范围内, 从而保证码本依然适用

算法 1 JTPNet 物理层密钥学习算法

输入: Alice 与 Bob 的输入序列 X_A, X_B , 训练轮数 E_1, E_2, E_3 , 学习率 η_1, η_2, η_3

输出: 训练完成的编码器参数 g_ϕ^* 、GRU 参数 GRU_θ^* 以及固定码本 $\mathcal{C}$

离线训练阶段

- 1 初始化逐帧编码器 g_ϕ 、双层 GRU GRU_θ 预测头 p_k
- // 阶段一: 未来状态预测预训练
- 2 **for** epoch=1 **to** E_1 **do**
- 3 执行收发双方未来状态预测任务, 计算 InfoNCE 损失 $\mathcal{L}_{\text{CPC}}(12)$
- 4 反向传播更新 g_ϕ 、 GRU_θ 预测头 p_k 参数
- 5 **end for**
- // 阶段二: 特征一致性微调
- 6 **for** epoch=1 **to** E_2 **do**
- 7 获取特征 r_A, r_B , 计算特征一致性损失 $\mathcal{L}_{\text{align}}(13)$
- 8 固定预测头 p_k 参数, 仅反向传播微调 g_ϕ 、 GRU_θ 参数
- 9 **end for**
- // 构建码本
- 10 提取阶段二模型输出的训练集全部连续特征, 经归一化后执行 K-Means 聚类, 构建固定码本 $\mathcal{C}$
- // 阶段三: 量化误差微调
- 11 **for** epoch=1 **to** E_3 **do**
- 12 基于固定码本 $\mathcal{C}$ 与软量化机制计算软量化误差损失 $\mathcal{L}_{\text{QACL}}(17)$
- 13 码本 $\mathcal{C}$ 固定且不参与梯度更新, 仅反向传播更新 g_ϕ 、 GRU_θ 参数
- 14 **end for**

于调整后的特征分布。

离线三阶段训练完成后, 预测头不再参与实际密钥生成, 相关损失函数仅用于训练阶段。Alice 与 Bob 分别保存相同的网络参数和码本。在线生成密钥时, Alice 与 Bob 仅需将观测序列输入共享网络, 经逐帧编码器、双层 GRU 和线性投影层前向推理得到特征向量, 再通过最近邻码字查询完成码本量化, 即可生成密钥。整个过程中, 双方无需传输 CSI 数据或中间特征, 对外仅交换信息协商与隐私放大所需的公开消息。该过程计算开销较低, 能够满足资源受限终端的实时部署需求, 复杂度分析见 3.5 节。

3 仿真结果**3.1 仿真设置**

为验证本文方案的有效性, 本文基于 3GPP TR 38.901 CDL-B 信道模型构建 TDD-OFDM 仿真场景, 将子载波间隔、终端移动速度和载波频率分别设置为 30 kHz、30 km/h 和 900 MHz。在该参数设置下, 信道相干时间约为 16.9 ms。本文采用 8 ms 观测窗口, 利用信道中相邻 CSI 观测的时间相关性进行特征学习, 不假设整个窗口内信道恒定。Alice 与 Bob 在相干时间内进行双向导频探测, 分别获得受噪声和信道估计误差影响的 CSI 观测。

设 Alice 与 Bob 分别通过码本量化生成密钥序列 b_A 和 b_B , 序列长度均为 L , 窗口持续时间为 T_{win} 。仿真中, 将 KDR 定义为双方生成的密钥序列对应位置不一致元素所占的比例, 即

$$\text{KDR} = \frac{1}{L} \sum_{i=1}^L \mathbb{I}(b_A(i) \neq b_B(i)), \#(18)$$

其中 $\mathbb{I}(\cdot)$ 为指示函数。有效密钥生成速率定义为每探测窗口内双方一致位数与窗口持续时间之比, 即

$$R_{\text{eff}} = \frac{\log_2 M \cdot (1 - \text{KDR})}{T_{\text{win}}}, \#(19)$$

仿真参数设置如表 1 所示。

本文为验证各核心模块对提升密钥质量的作用, 将以下四种方案进行对比。

● 本文方案: 考虑收发双方未来状态预测损失、特征一致性损失以及量化误差损失的完整时序预测网络结构。

● 方案(1)-不考虑未来状态预测损失的本文变体: 移除双层 GRU 及预测支路, 仅保留双层全连接逐帧编码器, 并对窗口内各时刻的瞬时特征取均值作为特征向量, 其余训练流程与本文方案一致, 用于分析时序预测对共享动态特征学习的贡献。

● 方案(2)-不考虑特征一致性损失的本文变体: 保留收发双方未来状态预测损失及量化误差损失, 验证特征一致性损失项对降低双方特征偏差的作用。

● 方案(3)-不考虑量化误差损失的本文变体: 完成预测预训练与特征一致性微调后, 直接基于固定码本进行硬量化, 不执行第三阶段微调, 用于验证量化误差损失项对提升密钥一致性的必要性。

3.2 损失项与训练策略分析

图 4 和图 5 分别给出四种方案在不同信噪比下

表1 仿真参数设置

名称	设置
信道模型	3GPP CDL-B
CSI序列长度 W	16
子载波数 N_{sc}	64
载波频率	900 MHz
子载波间隔	30 kHz
时隙长度	0.5 ms
窗口持续时间 T_{win}	8 ms
CPC 预测步长 k	3
码本大小 M	16
逐帧编码器隐藏层维度 h_1	128
逐帧编码器输出维度 d_z	32
特征向量维度 d_r	32
GRU 隐藏层维度 d_h	64
随机失活	0.2
批量大小 B	64
优化器	AdamW
第一阶段学习率 η_1	1×10^{-3}
第二阶段学习率 η_2	5×10^{-4}
第三阶段学习率 η_3	1×10^{-4}
第一阶段训练轮数 E_1	150
第二阶段训练轮数 E_2	30
第三阶段训练轮数 E_3	15
InfoNCE 温度系数 τ_c	0.07
软量化温度系数 τ_q	0.3
权重衰减 λ	1×10^{-4}

的KDR与 R_{eff} 。

如图4所示,随信噪比提升,各方案的KDR均单调下降,本文方案在所有信噪比条件下KDR均最低。方案(3)的KDR相对于本文方案的KDR增幅至少89%,且信噪比越高,增幅越大。这表明即使双方特征在数值上趋于接近,若训练过程未考虑量化误差损失,码本边界附近的微小特征偏差仍会导致密钥不一致,量化误差损失对密钥一致性的作用最为直接。方案(2)的KDR相对于本文方案的KDR增幅至少58%,说明仅依靠时序预测过程提取共享动态特征时,本地扰动引入的特征偏差仍会显著影响密钥一致性。方案(1)的KDR相对于本文方案的KDR增幅至少28%,增幅相对较小。上述

结果验证了三个损失项对密钥生成可靠性的各自贡献。

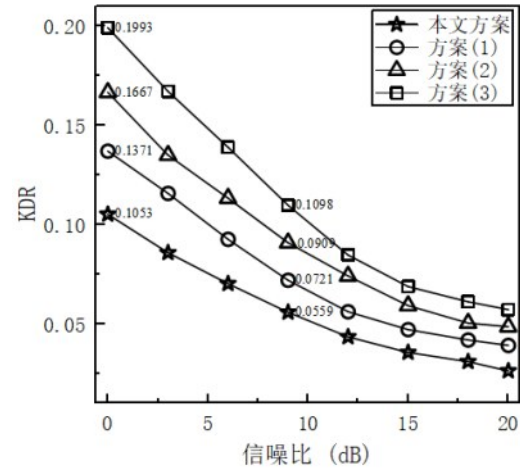


图4 不同信噪比下的KDR

图5给出各方案 R_{eff} 的对比结果。由于各方案每窗口量化位数相同, R_{eff} 由KDR决定,其相对高低与图4完全对应。本文方案在全信噪比范围内均取得最高的 R_{eff} 。

上述仿真分析了各损失项对密钥一致性的影响。为进一步验证分阶段训练方式的合理性,本文设置端到端联合训练对照实验:将预测损失、一致性损失与量化损失加权求和,指导网络参数训练。两种训练方式采用相同的网络结构、训练数据与训练轮数。分阶段训练的码本按算法1在第二阶段后构建,并在第三阶段保持固定。在训练开始前,联合训练对照实验基于训练集特征构建码本。在训练过程中,码本保持固定,不参与反向传播和更新。在训练完成后,联合训练对照实验基于联合模型的训练集特征重建码本。信噪比设置为20 dB,结果如表2所示。

由表2可知,两种训练方式的码字分布均较为均匀,但分阶段训练的KDR更低、码字熵略高。因此,本文采用分阶段训练方式。

3.3 与现有方案的性能对比分析

图6给出了本文方案与基于幅度/相位量化的物理层密钥生成方法^[7,10]及现有基于深度学习的物理层密钥生成方法^[13,19-20]的性能对比结果。本文选取文献[7]和文献[10]分别作为幅度量化和相位量化两类传统技术路线的代表性工作。为保证公平,Radio-telepathy^[7]和 Phase-Randomness^[10]均采用与本

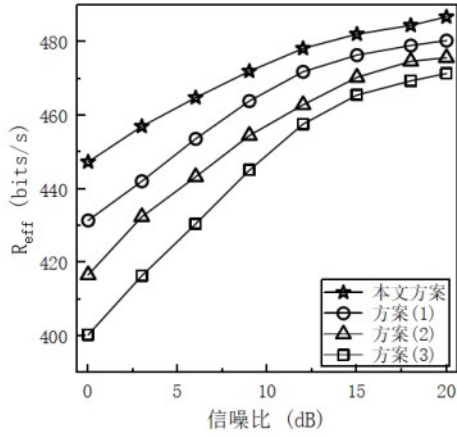
图5 不同信噪比下的 R_{eff}

表2 联合训练与分阶段训练策略的对比结果

训练方式	KDR	码字熵	最大码字占比
分阶段训练 (本文方案)	0.0264	3.94	8.51%
联合训练	0.0415	3.91	9.47%

文相同的密钥长度。如图6(a)所示,本文方案与Radio-telepathy^[7]和Phase-Randomness^[10]相比,KDR分别至少降低58%和68%。这表明传统方法难以抑制非理想互易引入的观测偏差,而本文方案通过时序预测学习共有信道演化规律并在特征提取阶段兼顾量化过程,显著降低了KDR。

为进一步比较基于深度学习的密钥生成方法的性能,本文选取CRCNet^[19]、MIAE^[20]和JOCLNet^[13]三种已有工作的网络结构作为对比模型。各对比模型均采用与本文方案相同的训练数据、码本构建方式、量化方式及后续密钥处理流程,使对比结果主要反映不同网络特征提取能力的差异。

如图6(b)所示,本文方案在所有信噪比条件下均取得最低的KDR:与本文方案差距最小的MIAE相比降低23%以上;与JOCLNet和CRCNet相比,分别降低40%以上和59%以上。CRCNet主要学习收发信道间的映射关系来补偿非理想互易,对时间序列利用有限;MIAE通过自编码器与互信息驱动机制提取双方相关特征,但未直接针对量化结果进行优化;JOCLNet的重点在于缩小双方特征分布差异。而本文方案在提取共享时序动态特征的基础上,依次引入特征一致性损失与量化误差损失,使网络同时兼顾连续特征的一致性与量化的准确性,因而取得最低的KDR。

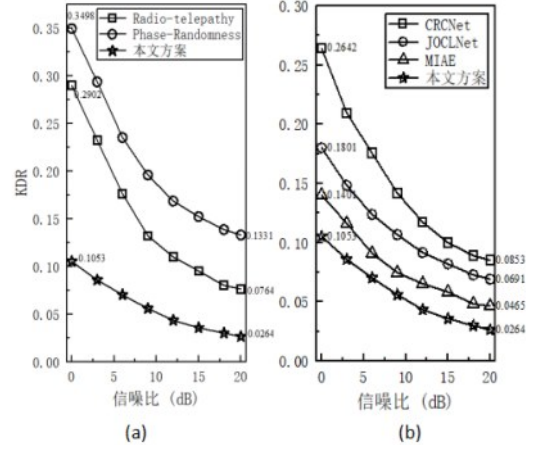


图6 本文方案与现有方案KDR对比

3.4 完整密钥生成流程与安全性评估

为验证所提方法能否有效兼容完整的物理层密钥生成流程,Alice与Bob首先通过本文方案生成密钥,然后采用LDPC码进行信息协商,纠正不一致位,最后经SHA-256处理与SHAKE256派生输出最终会话密钥。最终会话密钥的产生过程如下:以1000个不重叠的连续探测窗口构成一个密钥生成会话,其原始密钥长度为4000 bit、探测窗口总时长为8 s。信息协商采用码率为0.4的LDPC码^[25]。协商成功后,双方将密钥比特串经SHA-256处理,再由SHAKE256派生得到256 bit会话密钥。最终输出长度与原始密钥长度之比为6.4%,密钥输出速率为32 bit/s。

图7给出了完整流程下协商后的误码率随信噪比的变化。针对图7中的每个信噪比点,统计100个独立会话,每个会话原始密钥长度为4000 bit,最终会话密钥长度256 bit。误码率按协商后、哈希处理前的密钥比特计算。随着信噪比提高,误码率由0 dB时的 10^{-2} 量级迅速下降,6 dB时降至 10^{-4} 量级,9 dB时进一步降至 10^{-5} 量级,当信噪比大于9 dB时,误码率降至0。上述结果表明,本文方案生成的密钥不一致位数在LDPC码的纠错能力覆盖范围内,信息协商能够纠正不一致位,完整流程可生成高度一致的最终会话密钥。

除KDR外,密钥的随机性是衡量安全性的重要指标。图8给出了完整流程下密钥的NIST SP800-22随机性测试结果。本文根据NIST测试标准,以显著性水平 $\alpha = 0.01$ 为通过准则。若测试值P-value大于0.01,则在99%的置信度下无法拒绝

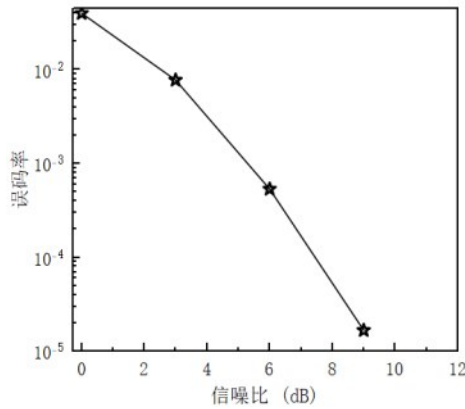


图7 完整流程下协商后的误码率

序列随机性的原假设，即判定序列通过该项测试。结果显示，全部 15 项测试的 P-value 均大于 0.01，所生成密钥通过全部测试，具备较高的随机性。

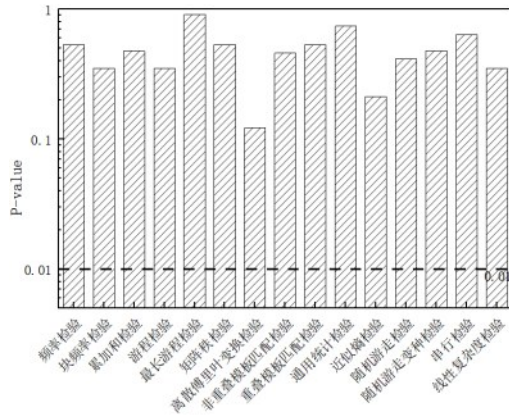
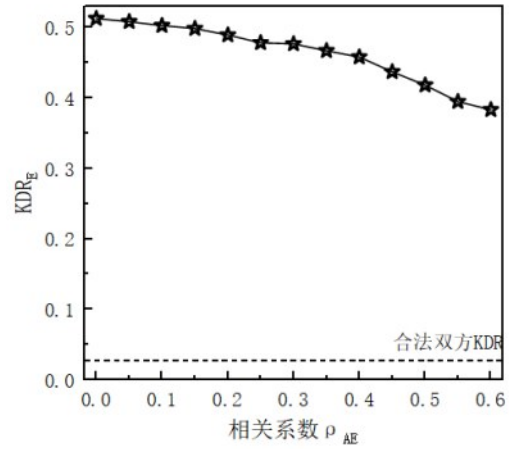


图8 密钥的NIST随机性测试结果

除密钥一致性与随机性外，本文还考虑从密钥熵的角度定量评估密钥材料的统计特性。本文采用 NIST SP800-90B 熵源评估工具，在非 IID 模式下对信息协商前的密钥序列进行最小熵估计。测试条件为信噪比 20 dB，共统计 50 组独立密钥生成会话，每组原始密钥长度为 4000 bit。结果处于 [0.82, 0.92] 区间，平均值为 0.86，表明所生成密钥具有较高的最小熵。

物理层密钥生成的安全性还要求窃听者难以恢复出有效密钥。本文考虑与合法方采用相同特征提取与量化流程、基于自身 CSI 观测生成密钥的窃听者，评估窃听场景下的安全性。图 9 给出了信噪比 20dB 和不同信道相关系数下 Eve 的不一致率 KDR_E 与合法双方的 KDR 。由图 9 可知，在理想空间去相关条件下，即 $\rho_{AE} = 0$ 时， KDR_E 始终稳定在 0.5 附

近，等同于纯随机猜测。随 ρ_{AE} 增大， KDR_E 缓慢下降，但始终远高于同一信噪比条件下合法双方 KDR 。即使窃听信道与合法信道存在中等程度 ($0.4 \leq \rho_{AE} \leq 0.6$) 的相关性， KDR_E 仍维持在 0.4 左右，表明本文方案在被动窃听场景下仍具有一定的抗窃听能力。

图9 不同信道相关系数下 KDR_E

3.5 复杂度分析

为评估所提方法在资源受限终端上的部署可行性，本文统计 JTPNet 在线阶段的推理复杂度。如 2.4 节所述，预测头仅用于离线训练。在线阶段的计算包括逐帧编码器、双层 GRU、线性投影层和码本查询，其中前三者构成在线推理子网络，统计结果如表 3 所示。

由表 3 可知，在线推理子网络包含约 66.8 K 个参数，所需存储空间 (float32 格式) 约 267 KB。码本包含 16 个码字，其存储开销相对于网络权重较小。本文在 Intel Core i7-12700 处理器单线程、批量大小为 1 的条件下，对在线推理的时延进行了 1000 次独立测量，平均时延约为 0.82 ms，仅占探测窗口时长 8 ms 的 10.3%。上述结果为资源受限终端的实时部署提供了依据。

4 结束语

本文提出了一种基于 JTPNet 的物理层密钥生成方法。所提方法的核心在于构建以收发双方未来信道状态预测为训练目标的特征提取网络，并在此基础上，将最小化特征一致性损失与最小量化误差损失作为阶段性训练目标，实现网络模型从提取时序特征到提高特征一致性再到降低量化误差的分

表3 JTPNet在线推理复杂度

模块	参数量 (个)	计算量 (FLOPs)
逐帧编码器	20896	659456
双层GRU	43776	1376256
线性投影层	2080	4096
码本查询	—	约 1.5×10^3
合计	约 66.8 K	约 2.04×10^6

阶段优化。仿真结果表明,本文方案能够显著降低KDR、提高 R_{eff} ,并能与LDPC信息协商、SHA-256处理与SHAKE256派生有效结合,形成完整的物理层密钥生成流程。

未来工作主要包括三个方面。首先,本文面向被动窃听场景开展研究,未涉及导频污染、重放和主动干扰等主动攻击。由于主动攻击会改变导频交互和信道观测过程,后续需要针对不同攻击行为重新建立威胁模型,设计相应的密钥生成与防护机制,并进一步开展被动窃听和主动攻击场景下的信息论安全分析。其次,本文采用的损失函数及其权重设置仍有优化空间,后续将研究替代损失形式和自适应加权策略,以进一步提高密钥一致性。最后,本文的密钥生成方法适用于信道慢变化场景,信道快变化场景下的物理层密钥生成方法仍需进一步研究。

杨林霏(2003-),女,东北大学研究生,主要研究方



向为无线物理层安全。

郑萌(1983-),男,博士,东北大学教授,主要研究



方向为工业物联网和网络化控制系统。

丁菁芳(1994-),女,博士,东北大学讲师,主要研究方向为无线网络资源分配和感传一体化。



参考文献:

- [1] MAURER U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993, 39(3): 733-742.
- [2] AHLSEWEDE R, CSISZAR I. Common randomness in information theory and cryptography. I. Secret sharing[J]. IEEE Transactions on Information Theory, 1993, 39(4): 1121-1132.
- [3] ZENG K. Physical layer key generation in wireless networks: challenges and opportunities[J]. IEEE Communications Magazine, 2015, 53(6): 33-39.
- [4] MITEV M, PHAM T M, CHORTI A, et al. Physical layer security—From theory to practice[J]. IEEE BITS the Information Theory Magazine, 2023, 3(2): 67-79.
- [5] LI J, YANG Y, YAN Z. AI-based physical layer key generation in wireless communications: current advances, open challenges, and future directions[J]. IEEE Wireless Communications, 2024, 31(5): 182-191.
- [6] ALSHAMDAYN A D, MIN M. A survey of quantization techniques for physical layer-based secret key generation in IoT systems[C]//Proceedings of the 2024 IEEE International Conference on Computing (ICOCO). Piscataway: IEEE Press, 2024: 36-41.
- [7] MATHUR S, TRAPPE W, MANDAYAM N, et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel[C]//Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. New York: ACM, 2008: 128-139.
- [8] PATWARI N, CROFT J, JANA S, et al. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements[J]. IEEE Transactions on Mobile Computing, 2010, 9(1): 17-30.
- [9] ZHAO H, ZHANG Y, HUANG X, et al. A physical-layer key generation approach based on received signal strength in smart homes[J]. IEEE Internet of Things Journal, 2022, 9(7): 4917-4927.
- [10] WANG Q, SU H, REN K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks[C]//Proceedings of IEEE INFOCOM 2011. Piscataway, NJ: IEEE, 2011: 1422-1430.
- [11] 李小倩, 李为, 雷菁, 等. OFDM系统中基于三维星座旋转的物理层安全加密算法[J]. 电子学报, 2017, 45(12): 2873-2880.
- [12] LI X Q, LI W, LEI J, et al. Physical Layer Security Encryption Algorithm Based on Three-Dimensional Constellation Rotation in OFDM Systems[J]. Acta Electronica Sinica, 2017, 45(12): 2873-2880.
- [13] WAN Z, CHU Z, MI D, et al. STAR-RIS-assisted physical-layer key generation[J]. IEEE Transactions on Vehicular Technology, 2024, 73(6): 9165-9170.
- [14] JIANG Y, GUO Y, HU A. JOCLNet: a physical layer key generation scheme based on joint optimization and contrastive learning network[J]. IEEE Internet of Things Journal, 2026, 13(13): 29681-29693.
- [15] ZHANG X, LI G, ZHANG J, et al. Deep-learning-based physical-layer secret key generation for FDD systems[J]. IEEE Internet of Things

- Journal, 2022, 9(8): 6081-6094.
- [15] ZHANG X, LI G, ZHANG J, et al. Enabling deep learning-based physical-layer secret key generation for FDD-OFDM systems in multi-environments[J]. IEEE Transactions on Vehicular Technology, 2024, 73(7): 10135-10149.
- [16] CHEN Y, et al. Physical layer key generation scheme for MIMO system based on feature fusion autoencoder[J]. IEEE Internet of Things Journal, 2023, 10(16): 14886-14895.
- [17] LI Z, XU P, GAO Q, et al. Reconfigurable intelligent surface-aided secret key generation using an autoencoder and K-means quantization[J]. Frontiers of Information Technology & Electronic Engineering, 2025, 26(8): 1486-1500.
- [18] VAN DEN OORD A, LI Y, VINYALS O. Representation learning with contrastive predictive coding[C]//Advances in Neural Information Processing Systems. 2018: 1-13.
- [19] CHEN L, CHEN Z, LU T, et al. A physical layer key generation scheme based on deep learning compensation and balanced vector quantization[J]. Security and Communication Networks, 2023: 4911338.
- [20] GUO D, XIONG J, MA D, et al. Physical layer secret key generation based on mutual information-driven autoencoder[J]. IEEE Transactions on Wireless Communications, 2025, 24(10): 8042-8056.
- [21] WANG Z, LIU Y, WANG J, et al. A reliable physical layer key generation scheme based on RSS and LSTM network in VANET[J]. IEEE Internet of Things Journal, 2024, 11(1): 692-707.
- [22] MAHALAL E, ISMAIL M, WU Z Y, et al. Robust deep learning-based secret key generation in dynamic LiFi networks against concept drift [C]//2024 IEEE 21st Consumer Communications & Networking Conference. Las Vegas, NV, USA: IEEE, 2024: 899-904.
- [23] AGUSTSSON E, MENTZER F, TSCHANNEN M, et al. Soft-to-hard vector quantization for end-to-end learning compressible representations[C]//Advances in Neural Information Processing Systems. Red Hook, NY: Curran Associates Inc., 2017: 1141-1151.
- [24] JANG E, GU S, POOLE B. Categorical reparameterization with Gumbel-Softmax[C]//International Conference on Learning Representations Toulon, France: ICLR, 2017.
- [25] MACKAY D J C. Good error-correcting codes based on very sparse matrices[J]. IEEE Transactions on Information Theory, 1999, 45(2): 399-431.

[作者简介]



叶宁 (1982-), 女, 博士, 东北大学讲师, 主要研究方向为无线隐蔽通信和无线物理层安全。