文章编号：2095-4980(2024)01-0039-07

信道估计误差下的深度人工噪声预编码生成方法

宋晓岩，刘友江*，徐慧远，霍飞向

(中国工程物理研究院 电子工程研究所，四川 绵阳 621999)

摘　要：基于人工噪声的物理层安全通信系统，传统人工噪声通常采用推导得到的闭式表达式或最优化方法数值求解生成，要求输入准确的传输信道矩阵信息，才能保证通信系统的保密性。但实际环境中存在的信道估计误差会导致人工噪声预编码误差，从而降低通信系统保密容量。为此提出一种基于深度学习的人工噪声预编码生成方法，通过将有误差的信道估计信息作为输入，与无估计误差情况下传统数值求解得到的预编码矩阵进行拟合，训练得到可适应信道估计误差的深度神经网络。仿真表明，该方法在信道估计有误差时的保密性能与鲁棒性优于传统人工噪声生成系统；相比于其他深度学习方法在物理层安全的应用，所提方法具有更快的收敛速度。

关键词：人工噪声；深度学习；物理层安全；预编码

中图分类号：TN929.5　　**文献标志码：**A　　**doi：**10.11805/TKYDA2021410

Deep artificial noise precoding generation method considering channel estimation error

SONG Xiaoyan，LIU Youjiang*，XU Huiyuan，HUO Feixiang

(Institute of Electronic Engineering，China Academy of Engineering Physics，Mianyang Sichuan 621999，China)

Abstract：For the physical layer security communication system based on artificial noise, traditional artificial noise is usually generated by using closed-form expressions derived from derivation or numerical optimization methods which both require accurate channel state information matrix to guarantee the secrecy of the communication system. However, the channel estimation error in the real scenarios causes the artificial noise precoding error to reduce the security capacity of the communication system. For this reason, this paper proposes an artificial noise precoding generation method based on deep learning. By taking the channel estimation information with estimation error as input and fitting it with the precoding matrix obtained by traditional numerical solution generated by perfect channel estimation, a well-trained deep neural network that can adapt to the channel estimation error is obtained. Simulation shows that the security performance and robustness of this method when there are errors in channel estimation are better than traditional artificial noise generation systems. Compared with other deep learning methods for physical layer security, the method proposed in this paper has faster convergence speed.

Keywords：artificial noise；deep learning；physical layer security；precoding

在无线通信技术研究中，物理层安全通过利用无线信道的特性(如衰落、噪声和干扰)实现安全通信，同时避免传统密钥通信[1]的泄露与被破解问题以及额外频谱资源的浪费。在物理层安全方法(如保密波束赋形、中继选择[2]等)中，通常假设窃听者的信道状态信息(Channel State Information，CSI)在合法发射机上是已知的，但在实际通信场景中，很难证明这种假设成立，尤其是在被动窃听场景中。GOEL S 和 NEGI R 通过引入人工噪声[3](Artificial Noise，AN)的概念解决了这个问题。AN 是一种处于合法信道零空间内的随机噪声，通过预编码矩阵预处理并发送后，通过合法信道时，会与信道抵消，故不会对合法端用户产生影响，但与合法端用户处于不同信道的窃听端则会被噪声干扰，从而降低非法信道容量，实现保密通信[4-5]。当前 AN 的研究方向主要包括将 AN 应

收稿日期：2021-12-07；**修回日期：**2022-02-01

*通信作者：刘友江　email:liuyj04@163.com

用到不同衰落信道环境下[6]及AN最优功率分配等[7]问题。

传统的AN预编码生成方法通常采用推导得到的闭式解析表达或通过最优化方法数值求解，均要求合法信道信息准确已知，但在实际的无线通信环境中，信道估计存在误差，使用传统AN预编码生成方法必然引入预编码误差，导致生成的AN预编码不准确，使人工噪声泄露进合法信道空间，恶化合法接收机的信噪比，导致系统保密容量恶化。针对上述问题，文献[8]提出一种深度人工噪声方法，但其采用2步训练方法，导致训练过程复杂，且模型结构简单，难以适应信道估计误差较大的场景。

本文针对信道估计误差下的人工噪声预编码生成方法进行研究，提出一种人工噪声生成方法——人工噪声卷积神经网络(Artificial Noise Convolutional Neural Network，AN-CNN)。将有估计误差的信道与理想情况下传统方法数值计算得出的预编码矩阵分别作为数据集的输入和输出，进行训练，得到的AN-CNN比传统闭式表达式与最优化数值求解方法性能更优；通过构建层数更深的CNN并引入残差块的方法，保证了CNN网络的拟合与预测能力及模型的稳定收敛；进一步探讨不同优化算法对AN-CNN性能影响，所提出的AN-CNN与传统闭式解析式方法[3]、最优化数值解析以及深度人工噪声方法[8]相比，具备更优的保密性能与鲁棒性。

1 系统模型

如图1所示的物理层安全通信模型，由 $n_{\mathrm{T}}\geqslant 2$ 根天线的合法发送端(transmitter A)、单天线合法接收端(receiver B)与单天线无源窃听端(eavesdropper E)组成。$\boldsymbol{s}$ 为信息承载信号，$\boldsymbol{r}$ 为AN信号。为保证信息安全，发射端A每一时刻都会随机产生新的 $\boldsymbol{r}$，以确保AN的随机性。$\boldsymbol{b}_s\in\mathbb{C}^{n_{\mathrm{T}}\times 1}$ 为信息承载信号的预编码向量，$\boldsymbol{B}_r\in\mathbb{C}^{n_{\mathrm{T}}\times(n_{\mathrm{T}}-1)}$ 为AN信号的预编码矩阵。在传统方法中，$\boldsymbol{b}_s$ 用来使发射信号与接收信号的互信息最大，$\boldsymbol{B}_r$ 设计为通过信道 $\boldsymbol{h}$ 后能够被消除，即 $\boldsymbol{h}\cdot\boldsymbol{B}_r=\boldsymbol{0}$。发送端A至接收端B和窃听端E之间的信道为瑞利信道，其信道状态信息分别表示为 $\boldsymbol{h}\in\mathbb{C}^{1\times n_{\mathrm{T}}}$，$\boldsymbol{g}\in\mathbb{C}^{1\times n_{\mathrm{T}}}$，均服从复高斯分布，接收端B与窃听端E处的接收信号分别为 $\boldsymbol{r}_{\mathrm{b}}$ 与 $\boldsymbol{r}_{\mathrm{e}}$。

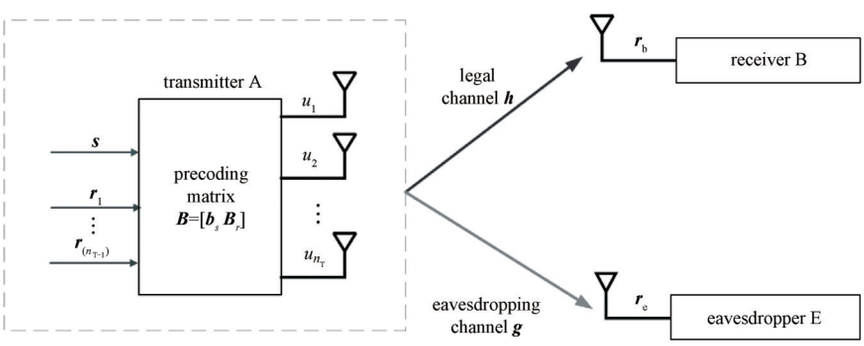


Fig.1 System model

图1 系统模型

在人工噪声的相关研究中，通常假设发送端A可以通过向接收端B发射训练序列的方式准确估计 $\boldsymbol{h}$，且B可以通过特殊的无噪反馈信道，将估计出的 $\boldsymbol{h}$ 实时反馈给A。而E为一个被动窃听者，只窃听而不发射任何信号，因此A将无法获知 $\boldsymbol{g}$ 的情况。

实际通信场景中，需考虑信道估计误差给传统方法生成的预编码矩阵带来的影响。合法接收端B的估计信道建模[9]如下：

$$\hat{\boldsymbol{h}}=\boldsymbol{h}+\boldsymbol{h}_{\mathrm{err}} \tag{1}$$

式中 $\boldsymbol{h}_{\mathrm{err}}\in\mathbb{C}^{1\times n_{\mathrm{T}}}$ 为合法接收机处的估计误差。发射端输出信号 $\boldsymbol{u}\in\mathbb{C}^{1\times n_{\mathrm{T}}}$ 为信息承载信号 $\boldsymbol{s}\in\mathbb{C}$ 与AN信号 $\boldsymbol{r}\in\mathbb{C}^{(n_{\mathrm{T}}-1)\times 1}$ 通过预编码矩阵处理后的线性和：

$$\boldsymbol{u}=\boldsymbol{b}_s\boldsymbol{s}+\boldsymbol{B}_r\boldsymbol{r}=\boldsymbol{x}+\boldsymbol{y} \tag{2}$$

合法接收端与窃听端信号分别表示为：

$$\boldsymbol{r}_{\mathrm{b}}=\boldsymbol{h}\boldsymbol{u}+n_{\mathrm{b}}=\hat{\boldsymbol{h}}\boldsymbol{u}-\boldsymbol{h}_{\mathrm{err}}\boldsymbol{u}+\boldsymbol{n}_{\mathrm{b}} \tag{3}$$

$$\boldsymbol{r}_{\mathrm{e}}=\boldsymbol{g}\boldsymbol{u}+\boldsymbol{n}_{\mathrm{e}} \tag{4}$$

假设此系统中发送端A与接收端B处的噪声是均值为0、方差为 σ^2 的复高斯白噪声，即 $\boldsymbol{n}_{\mathrm{b}}\sim\mathcal{CN}(0,\sigma_{\mathrm{b}}^2)$ 与

$\boldsymbol{n}_{\mathrm{e}} \sim \mathcal{CN}(0,\sigma_{\mathrm{e}}^2)$。通常采用保密率和接收端信噪比来衡量人工噪声通信系统的传输安全性能，其中平均保密率评估系统传输信息安全性，接收端信噪比评估接收信号中的AN与其他噪声对合法信号的影响。对于给定的一组$\boldsymbol{b}_s$和$\boldsymbol{B}_r$，平均保密率$\bar{R}_s(\boldsymbol{b}_s,\boldsymbol{B}_r)$表示为：

$$\bar{R}_s(\boldsymbol{b}_s,\boldsymbol{B}_r)=E\left[I\left(\boldsymbol{s};\boldsymbol{r}_{\mathrm{b}}\middle|\hat{\boldsymbol{h}}\right)-I\left(\boldsymbol{s};\boldsymbol{r}_{\mathrm{e}}\middle|\boldsymbol{h},\boldsymbol{g}\right)\right] \tag{5}$$

式中：$I(\cdot)$为互信息，$I\left(\boldsymbol{s};\boldsymbol{r}_{\mathrm{b}}\middle|\hat{\boldsymbol{h}}\right)$为合法信道容量，$I\left(\boldsymbol{s};\boldsymbol{r}_{\mathrm{e}}\middle|\boldsymbol{h},\boldsymbol{g}\right)$为窃听信道容量，两者相减表示系统传输的保密容量；$E[\cdot]$为求保密容量的期望，即平均保密率。人工噪声预编码是为了使式(5)最优，因此可以将AN求解过程表示为式(6)优化过程：

$$\left(\hat{\boldsymbol{b}}_s,\hat{\boldsymbol{B}}_r\right)=\underset{\substack{\boldsymbol{b}_s\boldsymbol{b}_s^{\mathrm{H}}\succ 0,\ \boldsymbol{B}_r\boldsymbol{B}_r^{\mathrm{H}}\succ 0\\ \mathrm{tr}(\boldsymbol{b}_s\boldsymbol{b}_s^{\mathrm{H}}+\boldsymbol{B}_r\boldsymbol{B}_r^{\mathrm{H}})\leqslant P}}{\arg\max}\ \bar{R}_s(\boldsymbol{b}_s,\boldsymbol{B}_r) \tag{6}$$

式中P为通信系统的发射总功率。由于式(2)中$\boldsymbol{x}$和$\boldsymbol{y}$为半正定矩阵，且$E\left[\boldsymbol{s}\boldsymbol{s}^{\mathrm{H}}\right]=1$，$E\left[\boldsymbol{r}\boldsymbol{r}^{\mathrm{H}}\right]=1$，因此优化函数应满足$\boldsymbol{b}_s\boldsymbol{b}_s^{\mathrm{H}}\succ 0$、$\boldsymbol{B}_r\boldsymbol{B}_r^{\mathrm{H}}\succ 0$与$\mathrm{tr}(\boldsymbol{b}_s\boldsymbol{b}_s^{\mathrm{H}}+\boldsymbol{B}_r\boldsymbol{B}_r^{\mathrm{H}})\leqslant P$，其中$\boldsymbol{a}\succ 0$表示$\boldsymbol{a}$为正定矩阵。相应地，接收端信噪比表示为：

$$R_{\mathrm{SN}}=E\left\{\frac{\left\|\hat{\boldsymbol{h}}\cdot\boldsymbol{b}_s\cdot\boldsymbol{s}\right\|^2}{\left\|\hat{\boldsymbol{h}}\cdot\boldsymbol{B}_r\cdot\boldsymbol{r}\right\|^2+n_{\mathrm{b}}}\right\} \tag{7}$$

从式(5)~式(7)可以看出，闭式表达式或最优化数值求解得到的预编码会受到信道估计误差$\boldsymbol{h}_{\mathrm{err}}$影响，导致保密率下降。为此，引入深度神经网络方法提升AN预编码生成的鲁棒性，式(5)进一步由文献[5]展开为：

$$\bar{R}_s(\boldsymbol{b}_s,\boldsymbol{B}_r)=E\left[\log\left(1+\frac{\left\|\hat{\boldsymbol{h}}\boldsymbol{b}_s\right\|^2}{\sigma_{\mathrm{b}}^2+\left\|\boldsymbol{h}_{\mathrm{err}}\boldsymbol{b}_s\right\|^2}\right)-\log\left(1+\frac{\left\|\boldsymbol{g}\boldsymbol{b}_s\right\|^2}{\sigma_{\mathrm{e}}^2+\left\|\boldsymbol{g}\boldsymbol{B}_r\right\|^2}\right)\right] \tag{8}$$

进一步考虑信息承载信号的功率分配比为$P_s\in[0,1]$时，式(8)由文献[10]展开为：

$$\bar{R}_s(\boldsymbol{b}_s,\boldsymbol{B}_r)=E\left[\log\left(1+\frac{\hat{\boldsymbol{h}}\boldsymbol{b}_s\boldsymbol{b}_s^{\mathrm{H}}\hat{\boldsymbol{h}}^{\mathrm{H}}P_s}{\sigma_{\mathrm{b}}^2+\hat{\boldsymbol{h}}\boldsymbol{B}_r\boldsymbol{B}_r^{\mathrm{H}}\hat{\boldsymbol{h}}^{\mathrm{H}}P_s+\boldsymbol{h}_{\mathrm{err}}\left(\boldsymbol{b}_s\boldsymbol{b}_s^{\mathrm{H}}+\boldsymbol{B}_r\boldsymbol{B}_r^{\mathrm{H}}\right)\boldsymbol{h}_{\mathrm{err}}^{\mathrm{H}}P_s}\right)-\log\left(1+\frac{\boldsymbol{g}\boldsymbol{b}_s\boldsymbol{b}_s^{\mathrm{H}}\boldsymbol{g}^{\mathrm{H}}(1-P_s)}{\sigma_{\mathrm{e}}^2+\boldsymbol{g}\boldsymbol{B}_r\boldsymbol{B}_r^{\mathrm{H}}\boldsymbol{g}^{\mathrm{H}}(1-P_s)}\right)\right] \tag{9}$$

式(9)将作为本文后续仿真评估系统保密性能主要指标。

2　基于深度学习的预编码生成

本文提出一种基于深度神经网络的物理层安全通信方法，流程如图2所示：获取信道估计信息$\hat{\boldsymbol{h}}$，输入到已完成训练的AN–CNN模型中，得到预测的预编码矩阵$\boldsymbol{b}_s$和$\boldsymbol{B}_r$；通过信号发生器分别生成需要传输的信息承载信号$\boldsymbol{s}$与随机AN信号$\boldsymbol{r}$，将2种信号在发射端通过预编码矩阵处理后在发送端A处进行发送。本研究假设合法端信道互相统计独立，但受噪声与估计误差的干扰。下面详细阐述AN–CNN的具体网络结构与训练过程。

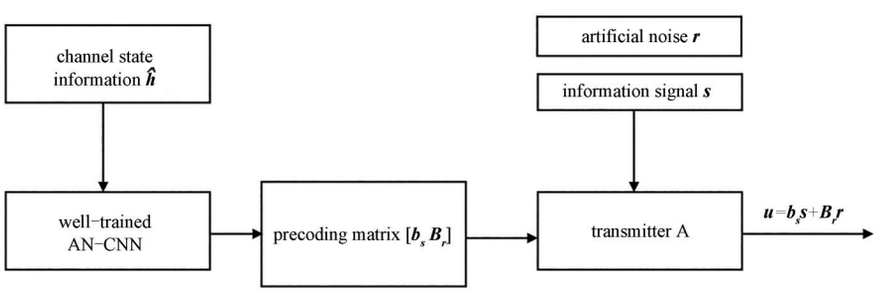


Fig.2 Flow chart of physical layer secure communication based on deep neural network
图2 基于深度神经网络的物理层安全通信流程图

2.1 AN–CNN 网络结构

本文提出的AN–CNN网络结构如图3所示，为了获得更优的保密性能以及更稳定的模型，网络采用多层卷积层提取信道的有效信息，通过加入残差块加强深度神经网络训练的稳定性，使用多层全连接层整合所提取的信息以及微调所提取的信道特征，通过高效的有监督训练减少训练时间与计算复杂度。

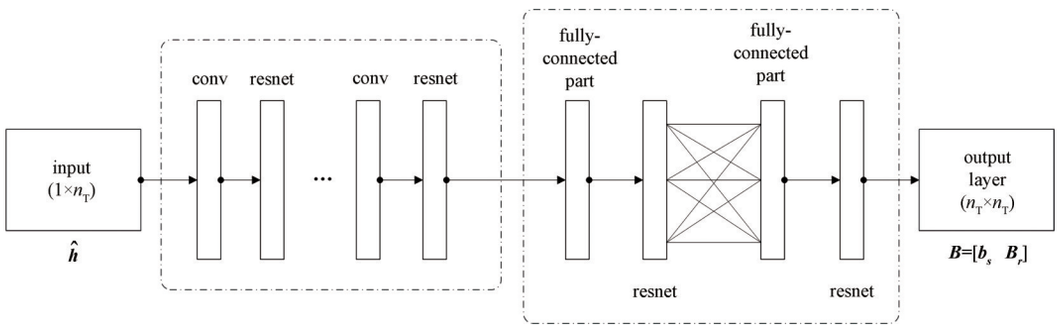


Fig.3 Structure of the proposed AN–CNN
图3 AN–CNN网络结构

网络由M层卷积层、残差块和L层全连接层、残差块连接组成，其中，参数选择与优化函数的设置将在实验部分进行阐述。网络输入端为合法端信道估计信息$\hat{\boldsymbol{h}}$，输出端为无估计误差的理想情况下传统数值求解得到的预编码矩阵$\boldsymbol{b}_s$和$\boldsymbol{B}_r$。其中残差块[11]用于解决多层神经网络导致的网络模型性能退化问题，如图4所示。残差网络将一层的输入添加到更深2层的输出中，网络学习残差函数作为特征提取的一部分，梯度消失可以通过归一化技术解决。由于CNN会因为网络层数的加深导致计算复杂、网络性能退化，通过残差函数可以确保模型性能的稳定性。

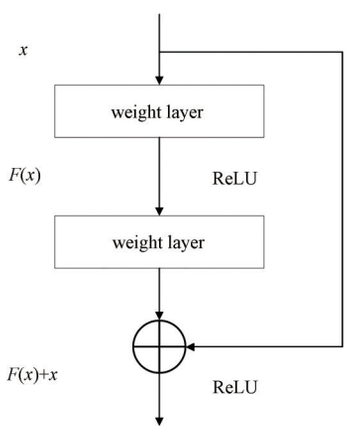


Fig.4 Resnet block
图4 残差块

每层卷积层与全连接层通过补零保证输入输出维度大小相匹配。卷积层计算过程以第k层为例：令$\boldsymbol{Z}_k$表示第k层卷积层的输入，则输出$\boldsymbol{X}_k$为：

$$\boldsymbol{X}_k=\varphi_k\left(\boldsymbol{W}_{\mathrm{C},k}*\boldsymbol{Z}_k+\boldsymbol{b}_{\mathrm{C},k}\right),\ \ k\in\{1,2,\cdots,K\} \tag{10}$$

式中：$\boldsymbol{W}_{\mathrm{C},k}$为卷积层权重矩阵；$\boldsymbol{b}_{\mathrm{C},k}$为偏置向量；$\varphi_k$为激活函数。卷积层的输出作为残差块的输入，其中卷积核大小为m'。残差块的输出表示为：

$$v_{r+1}=F\left(x_r,W_r\right)+x_r \tag{11}$$

式中：x_r为输入；$F\left(x_r,W_r\right)$为需要学习的残差部分。

全连接部分由L个连续的全连接层组成，令v_ℓ表示第ℓ层全连接层的输入，输出y_ℓ可以表示为：

$$\boldsymbol{y}_\ell=\sigma_\ell\left(\phi_\ell\left(\boldsymbol{W}_{\mathrm{F},\ell}\boldsymbol{v}_\ell+\boldsymbol{b}_{\mathrm{F},\ell}\right)\right),\ \ \ell\in\{1,2,\cdots,L\} \tag{12}$$

式中：$\boldsymbol{W}_{\mathrm{F},\ell}$为全连接层的权重矩阵；$\boldsymbol{b}_{\mathrm{F},\ell}$为偏置向量；$\phi_\ell$为激活函数；$\sigma_\ell$为第$\ell$层全连接层归一化函数。

2.2 AN–CNN 训练方法

为保证CNN网络的收敛速度和稳定性，在加深网络层数的同时加入残差块，改善网络层数加深带来的性能下降问题。其中，预训练中的损失函数由式(13)给出：

$$\mathrm{loss}(\boldsymbol{b}_s,\boldsymbol{B}_r,\boldsymbol{\Theta})=\left\|\hat{\boldsymbol{b}}_s-\boldsymbol{b}_s\right\|_2+\left\|\boldsymbol{h}\times\hat{\boldsymbol{B}}_r\right\|_{\mathrm{F}} \tag{13}$$

式中$\boldsymbol{\Theta}$为CNN网络中的所有权重和偏置矩阵。式(13)右边第1项表示使信息承载信号预编码逼近最优值，第2项表示AN预编码对合法信道影响最小。本文CNN网络中通过不同的优化算法进行训练，具体细节将在实验部分进行说明。

3　仿真结果与分析

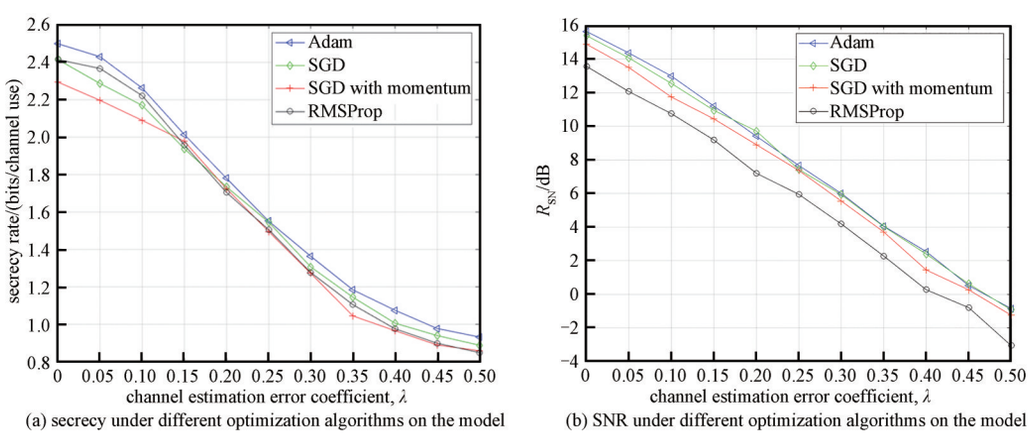
3.1　数据集

依据系统模型生成信道状态信息 $\hat{\boldsymbol{h}}$ 与预编码矩阵 $[\boldsymbol{b}_s\ \boldsymbol{B}_r]$。信道为瑞利分布，令 $\boldsymbol{h}\sim\left(0,\boldsymbol{I}_{1\times n_{\mathrm{T}}}\right)$，$\boldsymbol{g}\sim\left(0,\boldsymbol{I}_{1\times n_{\mathrm{T}}}\right)$，$\boldsymbol{h}_{\mathrm{err}}\sim\mathcal{N}\left(0,\lambda\boldsymbol{I}_{1\times n_{\mathrm{T}}}\right)$[12]，其中 $\boldsymbol{h}\sim\mathcal{N}\left(\mu,\partial^2\right)$ 表示 $\boldsymbol{h}$ 服从均值为 μ、方差为 ∂^2 的高斯分布，$\lambda\in[0,1]$ 表示信道估计误差系数范围，数值越高，则估计误差越大。根据每个合法信道 $\boldsymbol{h}$，生成无估计误差的理想情况下传统 AN 方案数值求解得到的信息承载信号预编码和 AN 预编码 $[\boldsymbol{b}_s\ \boldsymbol{B}_r]$。规定数据集输入部分为含有误差的信道估计向量 $\hat{\boldsymbol{h}}$，输出部分为 $\boldsymbol{b}_s$ 和 $\boldsymbol{B}_r$。为对比不同的误差对模型性能的影响，在生成数据集时，将信道估计误差系数设为 $\lambda\in[0,0.5]$，步进为 0.05，共生成 11 组不同的数据集，每组数据量为 10^4，包括训练集、验证集与测试集，故每次训练与测试所用的数据集估计误差系数相同。最后，使用与训练样本不同的 2 000 个测试样本以及 2 000 个验证信道来评估系统性能。

3.2　不同训练参数情况下模型性能对比

卷积部分和全连接部分的层数分别设置为 10 和 2，所有卷积核大小 $m'=3$，每个卷积层深度设为 n_{T}。使用 leakyReLU 函数作为卷积层的激活函数。全连接层采用线性激活和批归一化处理以允许输出为负值，并满足发射功率约束。最后一层输出层采用线性激活函数，保证输出值有正负数。卷积层与全连接层所有卷积核的大小设置为 n_{T}，学习率 $\alpha=0.001$。设通信系统中的热噪声参数为 $\sigma_{\mathrm{b}}^2=0.5$、$\sigma_{\mathrm{e}}^2=0.5$。

为使模型性能达到最优，本文比较了随机梯度下降算法(Stochastic Gradient Descent，SGD)、加入动量的随机梯度下降算法(SGD with momentum)、均方根反向传播算法(Root Mean Square Propagation，RMSProp)、适应性动量算法(Adaptive Momentum，Adam)4 种优化算法对训练结果的影响。实验结果如图 5 所示，图 5(a)~(b)分别为不同优化算法下模型保密率与接收端信噪比随信道估计误差 λ 变化的曲线图。SGD 算法每次只随机选择一个样本更新模型参数，因此每次的学习非常快速，并且可以进行在线更新。其最大的缺点在于每次更新可能并不会按照正确的方向进行，因此会带来优化扰动，使迭代次数增多，收敛速度变慢。对于加入动量的 SGD，在更新模型参数时，会对于那些当前的梯度方向与上一次梯度方向相同的参数进行加强或削减，因此可以获得更快的收敛速度并减少振荡。鉴于神经网络都是非凸条件下的，RMSProp 算法在非凸条件下结果更好。为进一步优化损失函数在更新中存在摆动幅度过大的问题，并进一步加快优化函数的收敛速度，在 RMSprop 基础上使用动量与偏差修正，提出了 Adam[13]算法。Adam 算法加入了每次迭代率的更新，针对特征密集与稀疏等不同场景进行更新，同时也加入了初始化偏差较正项，有效矫正初始训练时的偏差。



(a) secrecy under different optimization algorithms on the model　(b) SNR under different optimization algorithms on the model

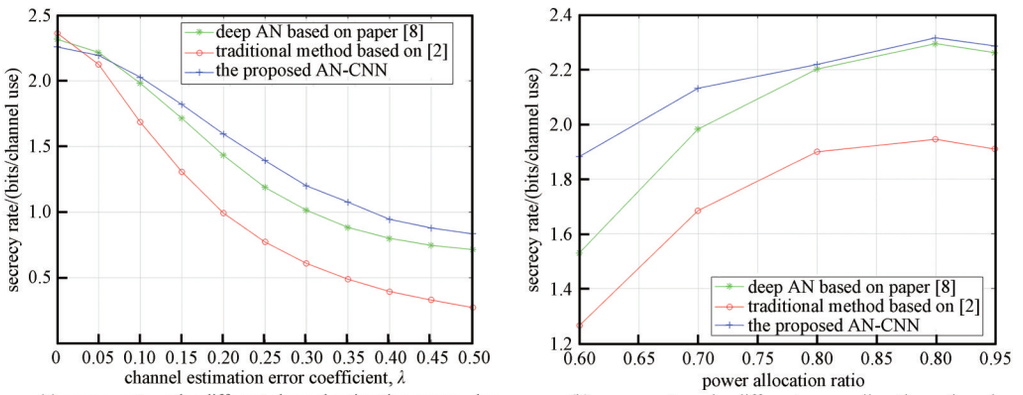
Fig.5　Impact of different optimization algorithms on the model

图 5　不同优化算法对模型的影响

令信息承载信号与 AN 信号的发射功率分配比为 0.9，训练 *epoch*=30，可以看出 Adam 优化算法下的模型在加入信道估计误差后，接收端的保密率与 SNR 最高。这是由于输入信道数据特征稀疏。为更有效地提取信道特征，且适应本文考虑的非凸优化条件下的问题，因此网络选择使用 Adam 算法，在训练过程中无需调整学习率。

为测试 AN-CNN 系统性能，分别计算所提出的 AN-CNN 模型、传统数值解析算法[3]与深度人工噪声模型[8]在不同信道估计误差 λ 与功率分配比下得到的预编码矩阵，得到接收端保密率。其中，令训练 *epoch*=30。图 6(a)为保密率随信道估计误差变化的曲线，可以看出，AN-CNN 模型较其他算法在信道估计误差系数大于 0.1 时，保密

率更高；当信道误差系数为0时，由于神经网络拟合存在微小偏差，此时传统方法数值求解出一一对应的准确结果，因此传统方法在理想情况下效果较好。在实际通信环境中，随着信道估计误差增大，所提出的AN–CNN模型保密性能更好。图6(b)为保密率随功率分配比变化曲线，整体而言，保密率随P_s由小变大，系统保密率由小变大再变小。这是由于当大量功率用于发射AN信号时，信息承载信号的发送功率较小，导致合法信道的保密容量降低；当P_s增大时，AN功率相应减小，窃听信道容量增大，致使系统保密率降低。从图6(b)中进一步看出，所提出的AN–CNN方法在不同功率分配比下整体性能最高。



(a) secrecy rate under different channel estimation errors when power allocation ratio is 0.9

(b) secrecy rate under different power allocation ratios when channel estimation error is 0.10

Fig.6 Variation curve of secrecy rate under different system parameters

图6 不同系统参数下的保密率变化曲线

对图6(a)进行定量分析，图7为不同信道估计误差下保密率增益曲线对比，其中$R_0=R_{\mathrm{AN-CNN}}/R_{\mathrm{deep-AN}}$，$R_1=R_{\mathrm{AN-CNN}}/R_{\mathrm{tra}}$，$R_{\mathrm{AN-CNN}}$、$R_{\mathrm{deep-AN}}$与$R_{\mathrm{tra}}$分别表示AN–CNN模型、深度人工噪声模型与传统算法的保密率，可见随着信道估计误差λ增加，AN–CNN模型保密性能越好。

为测试AN–CNN系统收敛速度，分别计算了AN–CNN模型加入残差块前后的收敛曲线与训练epoch的关系。令信息承载信号与AN信号的发射功率分配比为0.9，训练*epoch*=30，结果如图8所示。在加入残差块的情况下，系统在训练20个epoch后收敛，且保密率较高；未加入残差块时，系统在训练35个epoch后收敛，保密率较低。这是由于残差块可以改善网络层数加深带来的性能下降问题，并且通过归一化技术解决了梯度消失问题，使系统保密率达到较高数值，且收敛速度较快。同时，在加入信道估计误差λ=0.10后，虽然对保密率有一定的影响，但加入残差块的系统保密率提升22.88%。可见，引入残差块对本文提出的AN–CNN性能有更佳的提升。

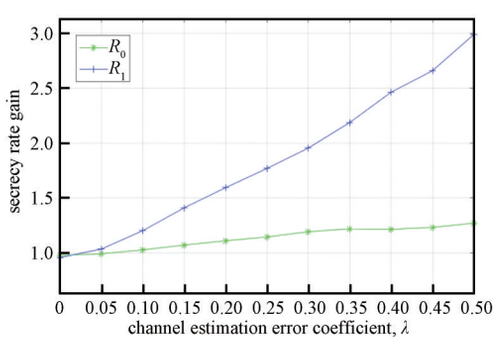


Fig.7 Secrecy rate gain under different channel estimation errors

图7 不同信道估计误差下保密率增益曲线对比

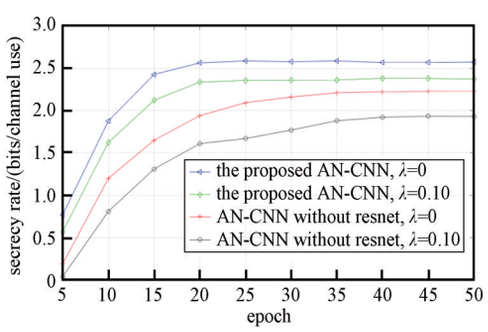


Fig.8 Convergence curve comparison of different networks

图8 不同网络结构下收敛曲线对比

最后，针对所提出的AN–CNN系统的计算复杂度进行分析。由于该方案是离线训练的，因此，推理预测的计算复杂度相比训练过程的计算复杂度要更加重要。卷积层、全连接层和残差块的推理预测在数学上可以表示成卷积和矩阵乘法，因此计算复杂度可表示为$\sum_{m=1}^{M}m'c_{m-1}c_m n_{\mathrm{T}}+\sum_{l=1}^{L}n_{l-1}n_l$。其中$m'$表示卷积核大小，$c_m$表示第$m$个卷积层输入的深度，$n_l$表示第$l$个全连接层输入的节点数。

4　结论

本文针对传统AN预编码方案存在信道估计误差导致保密性能降低的问题，提出了一种基于深度神经网络的最优AN预编码矩阵预测模型。通过采用CNN并引入残差块，以有估计误差的信道信息作为输入，以理想情况下传统数值求解得到的预编码矩阵作为输出，对AN-CNN进行训练。仿真表明，所提出的AN-CNN与传统数值求解方法[3]和深度人工噪声方法[8]相比，具有更优的保密性能，对于实际无线系统中信道信息无法准确估计，具有更好的实用价值。本研究结果是在仿真中得到的，实际场景模型情况更为复杂，因此AN-CNN模型在实际工程应用中会存在很多约束，如何改进AN-CNN模型以更接近实际应用情况，将是下一步的研究重点。

参考文献：

[1] 陈许星,何遵文,张焱,等. 一种基于信道特征参数的无线通信密钥生成方法[J]. 太赫兹科学与电子信息学报, 2017,15(5):834-840. (CHEN Xuxing, HE Zunwen, ZHANG Yan, et al. A key generation scheme for wireless communication based on channel characteristics[J]. Journal of Terahertz Science and Electronic Information Technology, 2017,15(5):834-840.) doi:10.11805/TKYDA201705.0834.

[2] 周叶,束锋,刘婷婷,等. 全双工MIMO中继系统高性能的波束成型算法[J]. 太赫兹科学与电子信息学报, 2017,15(1):42-46,58. (ZHOU Ye,SHU Feng,LIU Tingting,et al. A high-performance beamforming scheme for full duplex MIMO relays[J]. Journal of Terahertz Science and Electronic Information Technology, 2017,15(1):42-46,58.) doi:10.11805/TKYDA201701.0042.

[3] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6):2180-2189. doi:10.1109/TWC.2008.060848.

[4] GOEL S, AGGARWAL V, YENER A, et al. The effect of eavesdroppers on network connectivity: a secrecy graph approach[J]. IEEE Transactions on Information Forensics and Security, 2011,6(3):712-724. doi:10.1109/TIFS.2011.2148714.

[5] ZHOU Xiangyun, MCKAY M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation[J]. IEEE Transactions on Vehicular Technology, 2010,59(8):3831-3842. doi:10.1109/TVT.2010.2059057.

[6] YAO Li,LIU Youjiang. A novel optimization scheme for the beamforming method selection in artificial-noise-aid MU-MISOME broadcast secure communication system[C]// 2020 International Symposium on Computer Engineering and Intelligent Communications(ISCEIC). Guangzhou,China:IEEE, 2020:175-179. doi:10.1109/ISCEIC51027.2020.00044.

[7] 邓浩,王慧明. 人工噪声策略的临界信噪比和功率分配研究[J]. 通信学报, 2019,40(6):66-73. (DENG Hao,WANG Huiming. Research on critical SNR and power allocation of artificial noise assisted secure transmission[J]. Journal on Communications, 2019,40(6):66-73.) doi:10.11959/j.issn.1000-436x.2019114.

[8] YUN S,KANG J M,KIM I M,et al. Deep artificial noise:deep learning-based precoding optimization for artificial noise scheme[J]. IEEE Transactions on Vehicular Technology, 2020,69(3):3465-3469. doi:10.1109/TVT.2020.2965959.

[9] LIN P H, LAI S H, LIN S C, et al. On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels[J]. IEEE Journal on Selected Areas in Communications, 2013,31(9):1728-1740. doi:10.1109/JSAC.2013.130907.

[10] YUN S,IM S,KIM I M,et al. On the secrecy rate and optimal power allocation for artificial noise assisted MIMOME channels[J]. IEEE Transactions on Vehicular Technology, 2018,67(4):3098-3113. doi:10.1109/TVT.2017.2776338.

[11] HE Kaiming,ZHANG Xiangyu,REN Shaoqing,et al. Deep residual learning for image recognition[C]// 2016 IEEE Conference on Computer Vision and Pattern Recognition(CVPR). Las Vegas,NV,USA:IEEE, 2016:770-778. doi:10.1109/CVPR.2016.90.

[12] DING Minhua, BLOSTEIN S D. Maximum mutual information design for MIMO systems with imperfect channel knowledge[J]. IEEE Transactions on Information Theory, 2010,56(10):4793-4801. doi:10.1109/TIT.2010.2059870.

[13] KINGMA D P,BA J. Adam:a method for stochastic optimization[C]// The 3rd International Conference for Learning Representations. San Diego:ICLR, 2015.

作者简介：

宋晓岩(1998-)，女，在读硕士研究生，主要研究方向为物理层安全技术.email:songxiaoyan19@gscaep.ac.cn.

刘友江(1986-)，男，博士，研究员，博士生导师，主要研究方向为智能化无线电系统与理论.

徐慧远(1996-)，女，在读硕士研究生，研究实习员，主要研究方向智能抗扰通信.

霍飞向(1990-)，男，硕士，助理研究员，主要研究方向为调制和无人机集群.