深度学习辅助的随机频率分集阵列下的三维无线安全传输

胡锦松[①②] 蒋宛伶[①] 陈由甲*[①②] 徐艺文[①②] 赵铁松[①②] 束 锋[③]

[①](福州大学物理与信息工程学院 福州 350108)

[②](福建省媒体信息智能处理与无线传输重点实验室 福州 350108)

[③](海南大学信息与通信工程学院 海口 570228)

摘 要：针对相控阵列辅助的无线通信系统中发射波束只依赖角度特性而导致的安全隐患问题，以及传统的迭代算法所带来的高计算复杂度问题，该文提出由深度学习(DL)和随机频率分集阵列(RFDA)辅助带有3维安全区域的安全传输方案。首先，推导在3维空间中带有安全区域的期望用户实现安全通信的传输条件。在此基础上，构建系统安全速率下界最大化问题。随后，提出基于深度学习的神经网络方案来设计最优的波束成形矢量和人工噪声(AN)矢量来降低计算复杂度。仿真结果表明：即便是在窃听者位于安全区域边缘的最差情况下，所提方案仍能够在实现3维安全传输，能够保证安全区域内接收到的信息不被窃听。

关键词：安全传输；随机频率分集阵列；深度学习

中图分类号：TN92 **文献标识码**：A **文章编号**：1009-5896(2023)06-2063-08

DOI: 10.11999/JEIT220457

3D Wireless Secure Transmission under Random Frequency Diversity Array Assisted by Deep Learning

HU Jinsong[①②] JIANG Wanling[①] CHEN Youjia[①②] XU Yiwen[①②]
ZHAO Tiesong[①②] SHU Feng[③]

[①](*College of Physics and Information Engineering*, *Fuzhou University*, *Fuzhou* 350108, *China*)

[②](*Fujian Key Laboratory for Intelligent Processing and Wireless Transmission of Media Information*, *Fuzhou* 350108, *China*)

[③](*School of Information and Communication Engineering*, *Hainan University*, *Haikou* 570228, *China*)

Abstract: To solve the potential security issue caused by the fact that the transmitted beam in the phased array-assisted wireless communication systems only depend on angle characteristics and high computational complexity caused by the traditional iteration algorithms. A secure transmission scheme with 3D secure region assisted by Random Frequency Diverse Array (RFDA) and Deep Learning (DL) is proposed in this paper. Firstly, the requirements for the secure communication with the desired user within 3D secure zone are derived. Based on it, an optimization problem is formulated to maximize the lower bound of the secure rate of the considered system. Then, an optimization scheme based on deep learning is proposed to design the beamforming vector and Artificial Noise (AN) vector, so as to reduce the computational complexity. Simulation results show that even when the eavesdropper is located at the edge of the desired user's secure region, the proposed scheme can achieve the 3D secure transmission, and ensure the received confidential information in secure region.

Key words: Secure transmission; Random Frequency Diverse Array (RFDA); Deep Learning (DL)

收稿日期：2022-04-18；改回日期：2022-06-17；网络出版：2022-06-24

*通信作者： 陈由甲 youjia.chen@fzu.edu.cn

基金项目：国家自然科学基金(62001116, 62071234, 62171134), 福建省自然科学基金(2020J05106)

Foundation Items: The National Natural Science Foundation of China (62001116, 62071234, 62171134), The Natural Science Foundation of Fujian Province (2020J05106)

1 引言

随着第5代移动通信系统的发展与推广，大量智能终端设备被推广应用，移动数据流量将成倍增长。在此背景下，通信网络的拓扑结构将变得更加复杂，其中通信网络的无线链路层又有很高的开放性，这给无线信息的安全传输带来了严峻的挑战[1,2]。物理层安全技术作为传统加密技术的扩展与延伸，被广泛地认为是利用无线信道特性实现信息安全传输的一种关键性方法。

近年来，以多天线为基础的物理层安全技术受到了越来越多的关注，特别是将方向调制(Directional Modulation, DM)与多天线技术结合以增强无线通信系统的安全性能。DM技术是一种在支持多天线的物理层安全技术上推出的方法，DM技术能够保持期望方向信号的星座图，同时扭曲非期望方向信号的星座图，有效地保证了信息的安全传输[3,4]。文献[5]考虑方向角存在误差的场景，提出了具有稳健性的DM设计方案。因DM技术在保证信息安全传输方面上具有独特的优势，文献[6]提出将DM与智能反射面(Intelligent Reflecting Surface, IRS)相结合以实现系统安全速率最大化。在现有的工作中，大多数是利用相控阵列(Phased Array, PA)实现DM传输，并且假设期望用户与窃听者处于不同的方向角。考虑到PA具有的仅与角度有关联而存在的安全隐患问题，频率分集阵列(Frequency Diverse Array, FDA)的概念被提出并且有学者对RFDA的波束图进行了数学上的分析[7]。基于此，文献[8]提出将随机频率分集阵列(Random Frequency Diverse Array, RFDA)与人工噪声(Artificial Noise, AN)辅助的DM相结合，保证信号的能量主峰只出现在期望方向和期望距离处，实现无线通信系统在角度和距离上的2维安全传输。文献[9]提出精准安全传输的概念，通过随机子载波选择技术、DM技术以及相位对齐技术使发射波束具有方向角-距离的特性，使私密信息能够安全、准确地传输给期望用户。文献[10]考虑合法用户比窃听者离发射机更远的无线通信场景，分析收发机的相对位置对RFDA辅助的DM系统的无线安全性能影响。

在多天线通信系统中，通过波束成形技术将信号能量集中到指定的期望方向，用于补偿因传播损耗而导致的性能下降问题。波束成形技术被认为是设计多天线无线通信系统最重要的技术之一，因为它能够实现更高的传输速率和频谱效率[11]。然而，庞大的天线阵元数量会导致较高的计算复杂度，也无法满足通信的实时性要求。基于数据的深度学习(Deep Learning, DL)通过学习输入和输出之间的关系在实时处理最佳波束成形问题上具有巨大的潜力[12]。文献[13]提出使用深度神经网络模型来解决毫米波大规模多输入多输出(Multiple-Input Multiple-Output, MIMO)系统中的混合预编码问题，验证了基于深度神经网络的方法不仅能够降低系统的误码率而且还提高了频谱效率。文献[14]提出一种基于监督深度学习的自动编解码方案来实现大规模MIMO通信系统的物理层安全，使用二进制的信道状态信息(Channel State Information, CSI)作为反馈对神经网络模型进行优化训练。不同于文献[14]，文献[15]还考虑了CSI的恢复问题，提出基于DL的一种新颖的CSI感知和恢复机制网络，证明所提出的CSI网络能够保持有效的波束成形增益，保证信息的安全传输。

受此启发，本文提出借助DL设计私密信息的波束成形矢量与AN矢量来实现基于RDFA的具有安全区域的无线DM传输方案。通过分析推导带有安全区域的期望用户在3维空间中实现安全传输的条件，构建系统安全速率下界最大化问题，提出基于DL的多层感知机网络设计最优波束成形矢量和AN。

2 安全传输条件与优化问题建模

2.1 系统模型

在实际应用场景中，窃听者不可能无限制地接近期望用户，期望用户具有一定的安全传输区域。基于上述实际情况，给出了具有安全区域的通信系统模型。如图1所示，发射端(Alice)向期望用户(Bob)发送私密信息，而潜在的窃听者(Eve)想要拦截私密信息并且随机分布在期望用户Bob周围。假设Alice配备了具有$N \times M$根天线的均匀平面阵列，N表示沿x轴的天线阵元个数，M表示沿y轴的天线阵元个数，期望用户和窃听者都配备了单根天线。除此之外，假设Bob的安全区域中不存在窃听者，并且发射端位于3维坐标系的原点。

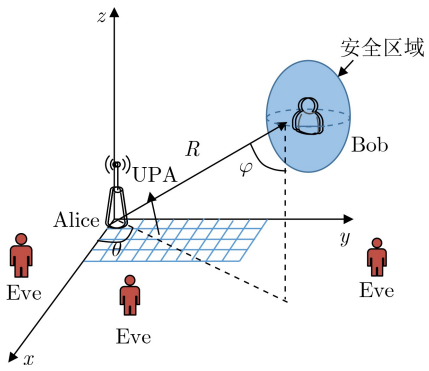

图 1 基于RFDA实现方向调制的通信系统框图

根据RFDA的特性，其第(n,m)个天线阵元上分配的频率为

$$f_{n,m}=f_{\mathrm{c}}+\Delta f_{x,n}+\Delta f_{y,m},\ n=0,1,\cdots,N-1,\ m=0,1,\cdots,M-1 \tag{1}$$

其中，f_{c}为天线阵元的中心载波频率，$\Delta f_{x,n}$和$\Delta f_{y,m}$分别是沿着x轴上第n个、y轴上第m个天线阵元的频率增量，服从均匀分布，即$\Delta f_{x,n}\in[\Delta f_{x,\min},\Delta f_{x,\max}]$和$\Delta f_{y,m}\in[\Delta f_{y,\min},\Delta f_{y,\max}]$。

RFDA的第(n,m)个天线阵元与3维空间中的期望用户的距离可表示为

$$R_{n,m}=R+\left(\frac{N-1}{2}-n\right)d_x\sin\theta\cos\varphi+\left(\frac{M-1}{2}-m\right)d_y\sin\theta\sin\varphi \tag{2}$$

其中，d_x和d_y分别是沿着x轴方向和y轴方向的天线阵元之间的距离，θ,φ和R分别是参考天线阵元与期望用户之间的水平角、俯仰角和距离。

在实际的通信系统中频率增量和中心载波频率之间需要遵从关系式$\sum_{n=0}^{N-1}\Delta f_{x,n}+\sum_{m=0}^{M-1}\Delta f_{y,m}\ll f_{\mathrm{c}}$，且天线阵列相邻阵元之间的距离接近波长长度$(d_x=d_y=\lambda/2)$，数值相对前两项非常小，因此相位差的第3项可以被忽略。RFDA的第(n,m)个天线阵元与参考相位点之间形成的相位差可以简化为

$$\begin{aligned}\psi_{n,m}=&\frac{2\pi}{\mathrm{c}}f_{n,m}R_{n,m}-\frac{2\pi}{\mathrm{c}}f_{\mathrm{c}}R\\ \approx&\frac{2\pi}{\mathrm{c}}\left[f_{\mathrm{c}}\left(\left(\frac{M-1}{2}-m\right)d_y\sin\theta\sin\varphi+\left(\frac{N-1}{2}-n\right)d_x\sin\theta\cos\varphi\right)+((\Delta f_{y,m}+\Delta f_{x,n})R)\right]\end{aligned} \tag{3}$$

通过上述分析，RFDA在3维空间中的某一点(θ,φ,R)的归一化导向向量可以表示为

$$\boldsymbol{h}(\theta,\varphi,R)=\frac{1}{\sqrt{NM}}\left[\mathrm{e}^{-\mathrm{j}\psi_{0,0}},\cdots,\mathrm{e}^{-\mathrm{j}\psi_{0,N}},\mathrm{e}^{-\mathrm{j}\psi_{1,0}},\cdots,\mathrm{e}^{-\mathrm{j}\psi_{M,N}}\right]^{\mathrm{T}} \tag{4}$$

其中，$(\cdot)^{\mathrm{T}}$表示对向量进行转置操作。

在考虑的系统中，假设Bob的位置为$(\theta_{\mathrm{b}},\varphi_{\mathrm{b}},R_{\mathrm{b}})$，Eve的位置为$(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})$。根据DM技术的原理，为了保证Bob的安全通信，在发射端采用带有AN的波束成形技术来保证期望用户接收到原始发射信号，扭曲窃听者接收到的信号，则发射端发送的信号表示为

$$\boldsymbol{x}=\sqrt{\alpha P_t}fs+\sqrt{(1-\alpha)P_t}\boldsymbol{w} \tag{5}$$

其中，P_t为发射端的发射功率，α为私密信号与人工噪声之间的功率分配因子，s表示需传输的信息且平均功率满足$\mathbb{E}[|s|^2]=1$，$\boldsymbol{f}$为发射端的波束成形矢量，$\boldsymbol{w}$为人工噪声矢量。$\boldsymbol{f}$表示为

$$\boldsymbol{f}=\boldsymbol{h}(\theta_{\mathrm{b}},\varphi_{\mathrm{b}},R_{\mathrm{b}}) \tag{6}$$

因而，Bob处接收到的信号可以表示为

$$\begin{aligned}y(\theta_{\mathrm{b}},\varphi_{\mathrm{b}},R_{\mathrm{b}})=&\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{b}},\varphi_{\mathrm{b}},R_{\mathrm{b}})\boldsymbol{x}+n_{\mathrm{b}}\\ =&\sqrt{\alpha P_{\mathrm{t}}}\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{b}},\varphi_{\mathrm{b}},R_{\mathrm{b}})\boldsymbol{f}s+n_{\mathrm{b}}\end{aligned} \tag{7}$$

其中，$(\cdot)^{\mathrm{H}}$为对向量进行共轭转置操作，n_{b}为Bob所在信道的加性高斯白噪声，分布服从$n_{\mathrm{b}}\sim\mathcal{CN}(0,\sigma_{\mathrm{b}}^2)$。类似地，Eve处的接收信号可以表示为

$$\begin{aligned}y(\theta_{\mathrm{e}},\varphi_{\mathrm{b}},R_{\mathrm{e}})=&\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})\boldsymbol{x}+n_{\mathrm{e}}\\ =&\sqrt{\alpha P_{\mathrm{t}}}\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})\boldsymbol{f}s\\ &+\sqrt{(1-\alpha)P_{\mathrm{t}}}\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})\boldsymbol{w}+n_{\mathrm{e}}\end{aligned} \tag{8}$$

其中，n_{e}分别为Eve所在信道的加性高斯白噪声，分布服从$n_{\mathrm{e}}\sim\mathcal{CN}(0,\sigma_{\mathrm{e}}^2)$。

由式(7)可知Bob处的信噪比为$\gamma_{\mathrm{b}}=\alpha P_{\mathrm{t}}/\sigma_{\mathrm{b}}^2$，依据式(8)Eve处的信干噪比为$\gamma_{\mathrm{e}}=\dfrac{\alpha P_{\mathrm{t}}\left|\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})\boldsymbol{f}\right|^2}{(1-\alpha)P_{\mathrm{t}}\left|\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})\boldsymbol{w}\right|^2+\sigma_{\mathrm{e}}^2}$。

2.2 安全传输条件

在系统中，天线个数设置为$N\times M$，RFDA的第(n,m)个阵元的频率表示为$f_{n,m}=f_{\mathrm{c}}+\Delta f_{x,n}+\Delta f_{y,m}$。$f_{n,m}$采取不同的分布会导致天线阵列具有不同的频率分布，则RFDA各阵元采用的频率增益表示为

$$\Delta\boldsymbol{f}_{x,y}=[\Delta f_{x,0},\Delta f_{x,1},\cdots,\Delta f_{x,N},\Delta f_{y,0},\Delta f_{y,1},\cdots,\Delta f_{y,M}]^{\mathrm{T}} \tag{9}$$

进一步定义变量$F_{xy}=\Delta\boldsymbol{f}_{x,y}^{\mathrm{T}}\Delta\boldsymbol{f}_{x,y}$。

这里定义Bob的安全区域在水平角度、俯仰角度和距离上都具有偏移量，分别设置为$\Delta\theta$, $\Delta\varphi$和ΔR，即Bob的安全区域表示为$\mathbb{D}=[\theta_{\mathrm{b}}-\Delta\theta,\theta_{\mathrm{b}}+\Delta\theta]\cap[\varphi_{\mathrm{b}}-\Delta\varphi,\varphi_{\mathrm{b}}+\Delta\varphi]\cap[R_{\mathrm{b}}-\Delta R,R_{\mathrm{b}}+\Delta R]$。考虑Eve位于安全区域边界时的极限情况，则此时与Bob的信道相关系数的最大值可以表示为

$$\eta=\max\left\{\left|\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{b}}\pm\Delta\theta,\varphi_{\mathrm{b}}\pm\Delta\varphi,R_{\mathrm{b}}\pm\Delta R)\boldsymbol{h}(\theta_{\mathrm{b}},R_{\mathrm{b}})\right|^2\right\} \tag{10}$$

类似地，窃听用户Eve与期望用户Bob之间的相关系数为

$$\left|\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})\boldsymbol{h}(\theta_{\mathrm{b}},\varphi_{\mathrm{b}},R_{\mathrm{b}})\right|^2=\left|\frac{1}{NM}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\mathrm{e}^{\mathrm{j}x_{n,m}}\right|^2 \tag{11}$$

其中

$$x_{n,m}=\left(\frac{M-1}{2}-m\right)q+\left(\frac{N-1}{2}-n\right)t+(\Delta f_{y,m}+\Delta f_{x,n})u \tag{12}$$

$$q=\frac{2\pi}{\mathrm{c}}f_{\mathrm{c}}d_y(\sin\theta_{\mathrm{e}}\sin\varphi_{\mathrm{e}}-\sin\theta_{\mathrm{b}}\sin\varphi_{\mathrm{b}}) \tag{13}$$

$$t=\frac{2\pi}{\mathrm{c}}f_{\mathrm{c}}d_x(\sin\theta_{\mathrm{e}}\cos\varphi_{\mathrm{e}}-\sin\theta_{\mathrm{b}}\cos\varphi_{\mathrm{b}}) \tag{14}$$

$$u=\frac{2\pi}{\mathrm{c}}(R_{\mathrm{e}}-R_{\mathrm{b}}) \tag{15}$$

为了确保3维空间中带有安全区域的期望用户实现安全传输，应满足$\left|\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})\boldsymbol{h}(\theta_{\mathrm{b}},\varphi_{\mathrm{b}},R_{\mathrm{b}})\right|^2\le\eta$即有式(16)成立

$$\left|\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\mathrm{e}^{\mathrm{j}x_{n,m}}\right|^2\le\eta(NM)^2 \tag{16}$$

式(16)中不等式左边部分利用欧拉公式展开，具体为

$$\begin{aligned}\left|\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\mathrm{e}^{\mathrm{j}x_{n,m}}\right|^2&=\left(\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\mathrm{e}^{\mathrm{j}x_{n,m}}\right)+\left(\sum_{l=0}^{M-1}\sum_{i=0}^{N-1}\mathrm{e}^{\mathrm{j}x_{l,i}}\right)^{\mathrm{H}}\\&=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\sum_{l=0}^{M-1}\sum_{i=0}^{N-1}\cos(x_{n,m}-x_{l,i})\end{aligned} \tag{17}$$

对于式(17)，利用泰勒展开将余弦函数近似为

$$\cos(x_{n,m}-x_{l,i})\approx1-\frac{1}{2}(x_{n,m}-x_{l,i})^2 \tag{18}$$

根据式(19)和式(20)，将式(18)重写为

$$\begin{aligned}&\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\sum_{l=0}^{M-1}\sum_{s=0}^{N-1}(x_{n,m}-x_{s.l})^2=C_1q^2+C_2t^2\\&\quad+b_1(f)u^2+2C_3qt+2b_2(f)qu+2b_3(f)tu\\&\quad\le2(NM)^2(1-\eta)\end{aligned} \tag{19}$$

其中

$$C_1=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\sum_{l=0}^{M-1}\sum_{i=0}^{N-1}(l-m)^2=\frac{N^2M^2(M^2-1)}{6} \tag{20}$$

$$C_2=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\sum_{l=0}^{M-1}\sum_{i=0}^{N-1}(i-n)^2=\frac{N^2M^2(N^2-1)}{6} \tag{21}$$

$$C_3=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\sum_{l=0}^{M-1}\sum_{i=0}^{N-1}(n-i)(m-l)=0 \tag{22}$$

$$b_1(f)=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\sum_{l=0}^{M-1}\sum_{i=0}^{N-1}(\Delta f_{n,m}-\Delta f_{i,l})^2 \tag{23}$$

$$b_2(f)=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\sum_{l=0}^{M-1}\sum_{i=0}^{N-1}(l-m)(\Delta f_{n,m}-\Delta f_{i,l}) \tag{24}$$

$$b_3(f)=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\sum_{l=0}^{M-1}\sum_{i=0}^{N-1}(i-n)(\Delta f_{n,m}-\Delta f_{i,l}) \tag{25}$$

基于文献[7]中RFDA波束图数学模型分析基础，可知

$$b_1(f)=2N\times M\times F_{xy} \tag{26}$$

$$b_2(f)=b_3(f)=0 \tag{27}$$

将式(21)进行整理可以得到近似于椭球的函数形式，具体表达式为

$$\begin{aligned}&\frac{C_1(2\pi f_{\mathrm{c}}d_y)^2}{2(NM)^2(1-\eta)\mathrm{c}^2}(\sin\theta_{\mathrm{e}}\sin\varphi_{\mathrm{e}}-\sin\theta_{\mathrm{b}}\sin\varphi_{\mathrm{b}})^2\\&+\frac{C_2(2\pi f_{\mathrm{c}}d_x)^2}{2(NM)^2(1-\eta)\mathrm{c}^2}(\sin\theta_{\mathrm{e}}\cos\varphi_{\mathrm{e}}\sin\theta_{\mathrm{b}}\cos\varphi_{\mathrm{b}})^2\\&+\frac{b_1(f)(2\pi)^2}{2(NM)^2(1-\eta)\mathrm{c}^2}(R_{\mathrm{e}}-R_{\mathrm{b}})^2=1\end{aligned} \tag{28}$$

为了便于分析，将式(28)重写为

$$\begin{aligned}&\frac{(\sin\theta_{\mathrm{e}}\sin\varphi_{\mathrm{e}}-\sin\theta_{\mathrm{b}}\sin\varphi_{\mathrm{b}})^2}{\left(\dfrac{\sqrt{2(1-\eta)}NM\mathrm{c}}{\sqrt{C_1}2\pi f_{\mathrm{c}}d_y}\right)^2}\\&+\frac{(\sin\theta_{\mathrm{e}}\cos\varphi_{\mathrm{e}}-\sin\theta_{\mathrm{b}}\cos\varphi_{\mathrm{b}})^2}{\left(\dfrac{\sqrt{2(1-\eta)}NM\mathrm{c}}{\sqrt{C_2}2\pi f_{\mathrm{c}}d_x}\right)^2}\\&+\frac{(R_{\mathrm{e}}-R_{\mathrm{b}})^2}{\left(\dfrac{\sqrt{2(1-\eta)}NM\mathrm{c}}{\sqrt{b_1(f)}2\pi}\right)^2}=1\end{aligned} \tag{29}$$

基于上述分析，若带有安全区域的期望用户实现安全通信，则应当保证处于安全区域外的窃听用户满足

$$|\sin\theta_{\mathrm{e}}\sin\varphi_{\mathrm{e}}-\sin\theta_{\mathrm{b}}\sin\varphi_{\mathrm{b}}|\ge\frac{\sqrt{2(1-\eta)}NM\mathrm{c}}{\sqrt{C_1}2\pi f_{\mathrm{c}}d_y} \tag{30}$$

$$|\sin\theta_{\mathrm{e}}\cos\varphi_{\mathrm{e}}-\sin\theta_{\mathrm{b}}\cos\varphi_{\mathrm{b}}|\ge\frac{\sqrt{2(1-\eta)}NM\mathrm{c}}{\sqrt{C_2}2\pi f_{\mathrm{c}}d_x} \tag{31}$$

$$|R_{\mathrm{e}}-R_{\mathrm{b}}|\ge\frac{\sqrt{2(1-\eta)}NM\mathrm{c}}{\sqrt{b_1(f)}2\pi} \tag{32}$$

将式(32)—式(34)整合，可推导得到3维空间中实现安全传输的条件为

$$M_{\min}=\sqrt{\frac{12(1-\eta)\mathrm{c}^2}{(2\pi f_{\mathrm{c}}d_y\Delta q)^2}+1} \tag{33}$$

$$N_{\min}=\sqrt{\frac{12(1-\eta)\mathrm{c}^2}{(2\pi f_{\mathrm{c}}d_y\Delta t)^2}+1} \tag{34}$$

$$F_{xy_{\min}}=\frac{(1-\eta)\mathrm{c}^2N_{\min}M_{\min}}{4\pi^2\Delta r^2} \tag{35}$$

其中，$\Delta q=|\sin\theta_{\mathrm{e}}\sin\varphi_{\mathrm{e}}-\sin\theta_{\mathrm{b}}\sin\varphi_{\mathrm{b}}|$，$\Delta t=|\sin\theta_{\mathrm{e}}\cos\varphi_{\mathrm{e}}-\sin\theta_{\mathrm{b}}\cos\varphi_{\mathrm{b}}|$，$\Delta r=|R_{\mathrm{e}}-R_{\mathrm{b}}|$。

2.3 安全性能分析与优化问题构建

根据Bob的信噪比，可以得到Bob的安全速率表示为

$$R_{\mathrm{b}}=\log_2(1+\gamma_{\mathrm{b}})=\log_2\left(1+\frac{\alpha P_{\mathrm{t}}}{\sigma_{\mathrm{b}}^2}\right) \tag{36}$$

相似地，窃听用户的安全速率为

$$\begin{aligned}R_{\mathrm{e}}=&\log_2(1+\gamma_{\mathrm{e}})\\=&\log_2\left(1+\frac{\alpha P_{\mathrm{t}}\left|\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})\boldsymbol{f}\right|^2}{(1-\alpha)P_{\mathrm{t}}\left|\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})\boldsymbol{w}\right|^2+\sigma_{\mathrm{e}}^2}\right)\\\le&\log_2\left(1+\frac{\alpha P_{\mathrm{t}}\eta}{(1-\alpha)P_{\mathrm{t}}\mu(1-\eta)+\sigma_{\mathrm{e}}^2}\right)\end{aligned} \tag{37}$$

上述不等式部分根据安全传输条件$\left|\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{e}},\varphi_{\mathrm{e}},R_{\mathrm{e}})\boldsymbol{h}(\theta_{\mathrm{b}},\varphi_{\mathrm{b}},R_{\mathrm{b}})\right|^2\le\eta$转化得到，其中

$$\mu=\frac{1}{\mathrm{Tr}\left\{[\boldsymbol{I}-\boldsymbol{h}(\theta_{\mathrm{b}},\varphi_{\mathrm{b}},R_{\mathrm{b}})\boldsymbol{h}^{\mathrm{H}}(\theta_{\mathrm{b}},\varphi_{\mathrm{b}},R_{\mathrm{b}})]^2\right\}} \tag{38}$$

运算符Tr{ • }表示对矩阵求迹。

根据Bob的安全速率和Eve的安全速率，可以得到通信系统的可实现的安全速率为

$$\begin{aligned}R=&R_{\mathrm{b}}-R_{\mathrm{e}}\\\ge&\log_2\left(\frac{1+\alpha P_{\mathrm{t}}/\sigma_{\mathrm{b}}^2}{1+\alpha P_{\mathrm{t}}\eta/((1-\alpha)P_{\mathrm{t}}\mu(1-\eta)+\sigma_{\mathrm{e}}^2)}\right)=R_{\mathrm{L}}\end{aligned} \tag{39}$$

其中，R_{L}为通信系统实现安全传输时的安全速率的下界。

为了实现通信的安全传输，对于给定的可达安全速率R_{s}应当保证$R_{\mathrm{L}}\ge R_{\mathrm{s}}$，对于安全传输约束$\eta$有

$$\eta\le\frac{(1-\alpha)P_{\mathrm{t}}\mu+\sigma_{\mathrm{e}}^2}{(1-\alpha)P_{\mathrm{t}}\mu+\alpha P_{\mathrm{t}}2^{R_{\mathrm{s}}}\sigma_{\mathrm{b}}^2/(\sigma_{\mathrm{b}}^2+\alpha P_{\mathrm{t}}-\sigma_{\mathrm{b}}^2 2^{R_{\mathrm{s}}})} \tag{40}$$

综上，最大化系统安全速率下界的优化问题建模为

$$\begin{aligned}&\max_{f,w}\ \mathrm{R_L},\\&\text{s.t. }\left|[\boldsymbol{f}]_n\right|^2=1,\ n=1,2,\cdots,N,\ P_{\mathrm{t}}\le P_{\max}\end{aligned} \tag{41}$$

其中，$|[\boldsymbol{f}]_n|^2=1$表示发射端的波束成形矢量的常模约束，$P_{\max}$为发射端的最大发射功率。

3 DL解决安全速率下界最大化优化问题

近年来，深度学习因具有超强的识别和表示能力被认为是处理复杂的非凸问题和高计算问题的绝佳工具。在此基础上，本文提出一种基于神经网络的设计方案实现 DM 传输，并获得波束成形向量$\boldsymbol{f}$与AN矢量来解决优化问题。如图2 所示，所提出方案中的 DL 神经网络结构基于多层感知器架构，由1个输入层、3个隐藏层、1个输出层和1个自定义层组成。

针对图2所提出的神经网络，具有下述特殊设置：

(1)输入层：训练神经网络的完美信道状态信

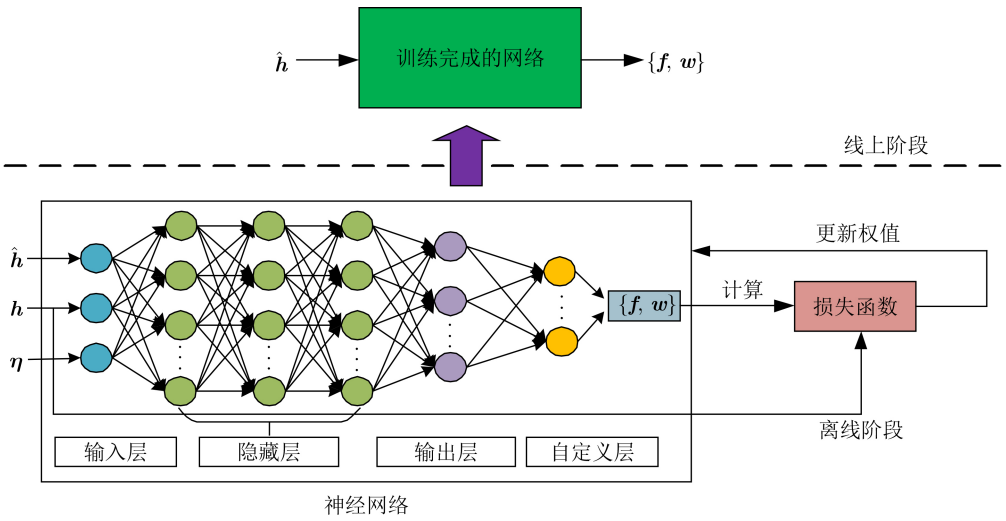

图 2 神经网络结构及训练方式

息$\boldsymbol{h}$依据式(4)生成，对俯仰角、水平角以及距离引入误差生成非完美的信道状态信息$\hat{h}$用于提取信道特征，为了解决神经网络不能处理复数数据的问题，将信道状态信息的实部和虚部拆分成两个独立的数据。此外，将安全传输条件η输入神经网络用于计算损失函数。

(2)自定义层：该层位于输出层的尾端同时输出波束形成矢量$\boldsymbol{f}$和人工噪声矢量$\boldsymbol{w}$，这也说明了$\boldsymbol{f}$和$\boldsymbol{w}$的优化总共需要$2(N\times M)$个复值。因此，自定义层的输出数据维度为$2(N\times M)\times 1$。为了确保波束形成矢量$\boldsymbol{f}$是复数值并满足常模约束，且在输出人工噪声矢量$\boldsymbol{w}$的同时能够保证满足发射功率的约束，在自定义层中将输入数据进行数学操作，从而使得输出的波束形成矢量$\boldsymbol{f}$和人工噪声矢量$\boldsymbol{w}$能够被归一化处理，其输出形式可以写为$f_{\text{base}}=\text{e}^{\text{j}\boldsymbol{\theta}}=\cos(\boldsymbol{\theta})+\text{j}\sin(\boldsymbol{\theta})$，$\boldsymbol{\theta}$表示输出层的实值，表示波束成形向量$\boldsymbol{f}$和人工噪声矢量$\boldsymbol{w}$的相位。基于上述数据处理过程，可知$||\boldsymbol{f}_{\text{base}}||^2=||\boldsymbol{f}||^2+||\boldsymbol{w}||^2=1$。因此，在将$\sqrt{P_{\max}}$乘以$\boldsymbol{f}$和$\boldsymbol{w}$中的所有元素后，将始终满足最大化安全速率下界优化问题中的发射功率约束。

(3)损失函数：与传统监督学习不同，在所提出的神经网络中对损失函数的设计与文献[12]中的无监督学习设计类似，在训练神经网络的过程中不需要标签，所提出的神经网络是采用了与优化问题中的目标函数直接相关的新损失函数，具体可以表示为$\text{Loss}=-\sum_{q=1}^{Q}R_{\text{L}_q}\Big/Q$，其中$Q$表示训练样本的总数，值得注意的是，损失函数中的安全速率下界R_{L}的计算是根据完美的信道状态信息计算得出的。根据神经网络的特点可知损失函数的减少对应于平均安全速率下界负值的降低。

综合上述分析，为了展示神经网络的详细结构，考虑发射天线总数目为64的前提下，所提出的用于求解最大化安全速率下界问题的波束神经网络的具体结构如表1所示。

值得注意的是，当发射端天线数量发生改变时，神经网络的输入层参数以及输出层参数应当相应发生改变。所提出的具有鲁棒特性的波束设计方案的训练过程总结在算法1中。

下面通过浮点数计算数量以进一步分析对比优化算法的复杂度，针对神经网络优化方案，只需计算线上阶段的浮点数操作，即为$(2N_{\text{I}}-1)N_{\text{o}}$，其中$N_{\text{I}}$是输入的维度，$N_{\text{o}}$表示输出的维度。例如，$N\times M=64$，所提出的神经网络的浮点运算数量约为180 000。对于传统方案，由于每个元素的矩阵求逆和频率分配等操作，复数乘法次数的计算复杂度为$O(N^3)$。例如，$N\times M=64$，复数乘法次数约为260 000次。可以看出，与传统方案相比基于神经网络的设计方案具有更低的计算复杂度。

4 仿真结果

本文通过数值仿真来展示所提传输方案的安全性能，系统的主要参数设置如下：中心载波频率$f_{\text{c}}=3$ GHz，频率增益的分布情况为$\Delta f_{y,\min}=\Delta f_{x,\min}=-10$ MHz，$\Delta f_{y,\max}=\Delta f_{x,\max}=10$ MHz，期望用户Bob的位置为$(45^\circ,30^\circ,100\text{ m})$，期望用户的安全区域的偏移量设置为$\Delta\theta=5^\circ$，$\Delta\varphi=5^\circ$，$\Delta R=10$ m。

图3绘制了不同发射天线数目和发射功率下私密信息与人工噪声的功率分配因子对系统安全速率的影响。首先，从图3可以明显地观察到，当发射端天线数量较少时，系统的安全速率随着功率分配因子的增大先提升后降低，这表明发射数目较少时需要借助最优功率分配比下的人工噪声来最大化系统的安全性能。此外，从图3还观察到，在相同发射天线数目的前提下，发射功率的增加也会提高系统的安全性能，这是因为增加发射功率可以提高发射波束的能量。其次，当发射天线数目较大时，从

表 1 所提神经网络模型参数

层名	输出维度	激活函数
输入层	64×2	无
批量标准化层	64×2	无
扁平层	128×1	无
批量标准化层	128×1	无
隐藏层1	256×1	ReLU
批量标准化层	256×1	无
隐藏层2	128×1	ReLU
输出层	128×1	无
自定层	128×1	无

算法1 求解优化问题式(41)的鲁棒算法

输入：完美无线信道系数h、非完美的信道状态信息$\hat{h}$以及安全传输条件η；

输出：输出训练完成的神经网络；

(1) 初始化神经网络；

(2) While $i\le T$ do

(3) While 训练数据全部进入神经网络 do

(4) 从训练数据从采样K个数据；

(5) 计算自定义损失函数并更新神经网络参数；

(6) End While

(7) 更新训练次数$i=i+1$；

(8) End While

图3可以观察到系统的安全速率随着功率分配因子的增大而增加，这表明足够大数量的发射天线已经能够发射更窄的波束，不需要人工噪声的辅助便能实现系统的安全传输。

图4显示了在不同发射功率下系统期望的安全速率与最小的发射天线数量之间的关系。值得注意的是，当功率分配因子$\alpha=1$时，表示系统将发射功率全部分配给了私密信息的波束，这就意味着通信系统没有人工噪声的辅助。从图4可以观察到，无论是否有人工噪声的辅助，系统的期望安全速率的提升必然会导致发射端发射天线数量的增加。除此之外，还可以观察得到，无论是否有人工噪声的辅助，增加发射功率可以通过增强发射波束的能量来帮助减弱增加发射端发射天数的压力，并且增加发射功率对有人工辅助的系统安全性能的影响要大于没有人工噪声辅助的系统的安全性能的影响。

图5绘制了不同F_{xy}值下系统期望安全速率与发射功率之间的关系，F_{xy}的取值通过已知的期望安全速率、天线阵列阵元数以及相对应的安全传输条件，根据式(37)计算得出。根据F_{xy}的定义可知其大小与天线频率分配的带宽有关，F_{xy}值越大意味着带宽越大。从图中可以明显观察到系统的安全性能随着发射功率的增加而被得到提升。而在具有相同发射功率的前提下，增大F_{xy}值也可以提高系统

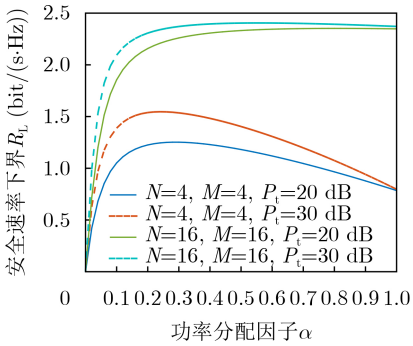

图 3 不同发射天线和发射功率下系统安全速率与功率分配因子的关系

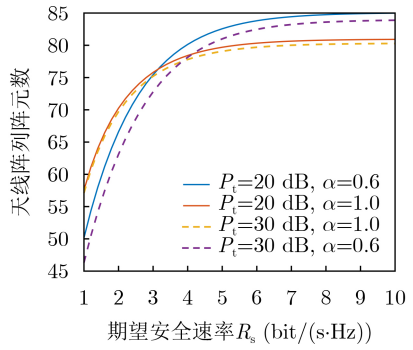

图 4 不同发射功率下系统总天线数量和期望安全速率的关系

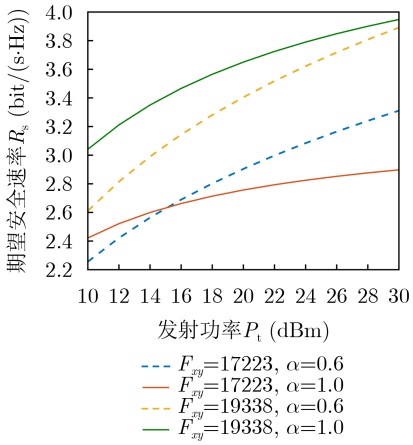

图 5 不同F_{xy}值下系统安全速率和系统发射功率的关系

的安全速率，从F_{xy}值所代表的物理意义理解，增大F_{xy}值即为增加带宽从而提高了系统的安全性能。此外，还可以观察得到，增大F_{xy}值对提升没有人工辅助的系统安全性能的影响要大于有人工噪声辅助的系统的安全性能的影响。

5　结束语

针对相控阵列只具有角度特性而存在的安全隐患，本文研究了基于深度学习实现随机频率分集阵列辅助带有安全区域的无线安全传输系统。首先，推导带有安全区域的期望用户在3维空间中实现安全传输的条件。随后，构建联合优化波束成形矢量和人工噪声矢量的系统安全速率下界最大化问题，同时针对系统实现安全速率下界最大化优化问题提出了复杂度较低的优化设计方案，该优化方案通过基于多层感知机的神经网络来实现。最后实验仿真分析有无人工噪声辅助对系统安全性能的影响，以及与相控阵列相比，所提出的无线传输方案实现了俯仰角-水平角-距离上的3维安全传输。在未来的工作中，将进一步研究在窃听者配备多天线的场景下，并采用深度学习相关技术来完成信道估计，以此实现无线通信系统的安全传输。

参 考 文 献

[1] YERRAPRAGADA A K, EISMAN T, and KELLEY B. Physical layer security for beyond 5G: Ultra secure low latency communications[J]. *IEEE Open Journal of the Communications Society*, 2021, 2: 2232–2242. doi: 10.1109/OJCOMS.2021.3105185.

[2] ARFAOUI M A, SOLTANI D M, TAVAKKOLNIA I, *et al*. Physical layer security for visible light communication systems: A survey[J]. *IEEE Communications Surveys & Tutorials*, 2020, 22(3): 1887–1908. doi: 10.1109/COMST.2020.2988615.

[3] WEI Zhongxiang, MASOUROS C, and LIU Fan. Secure

directional modulation with few-bit phase shifters: Optimal and iterative-closed-form designs[J]. *IEEE Transactions on Communications*, 2021, 69(1): 486–500. doi: 10.1109/TCOMM.2020.3032459.

[4] ZHANG Bo, LIU Wei, LI Qiang, *et al*. Directional modulation design under a given symbol-independent magnitude constraint for secure IoT networks[J]. *IEEE Internet of Things Journal*, 2021, 8(20): 15140–15147. doi: 10.1109/JIOT.2020.3040303.

[5] HU Jinsong, SHU Feng, and LI Jun. Robust synthesis method for secure directional modulation with imperfect direction angle[J]. *IEEE Communications Letters*, 2016, 20(6): 1084–1087. doi: 10.1109/LCOMM.2016.2550022.

[6] SHU Feng, TENG Yin, LI Jiayu, *et al*. Enhanced secrecy rate maximization for directional modulation networks via IRS[J]. *IEEE Transactions on Communications*, 2021, 69(12): 8388–8401. doi: 10.1109/TCOMM.2021.3110598.

[7] MA Yezi, WEI Ping, and ZHANG Huaguo. General focusing beamformer for FDA: Mathematical model and resolution analysis[J]. *IEEE Transactions on Antennas and Propagation*, 2019, 67(5): 3089–3100. doi: 10.1109/TAP.2019.2900400.

[8] HU Jinsong, YAN Shihao, SHU Feng, *et al*. Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays[J]. *IEEE Access*, 2017, 5: 1658–1667. doi: 10.1109/ACCESS.2017.2653182.

[9] SHU Feng, WU Xiaomin, HU Jinsong, *et al*. Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array[J]. *IEEE Journal on Selected Areas in Communications*, 2018, 36(4): 890–904. doi: 10.1109/JSAC.2018.2824231.

[10] WANG Shuaiyu, YAN Shihao, ZHANG Jia, *et al*. Secrecy zone achieved by directional modulation with random frequency diverse array[J]. *IEEE Transactions on Vehicular Technology*, 2021, 70(2): 2001–2006. doi: 10.1109/TVT.2021.3054803.

[11] XIE Ning, LI Zhuoyuan, and TAN Haijun. A survey of physical-layer authentication in wireless communications[J]. *IEEE Communications Surveys & Tutorials*, 2021, 23(1): 282–310. doi: 10.1109/COMST.2020.3042188.

[12] LIN Tian and ZHU Yu. Beamforming design for large-scale antenna arrays using deep learning[J]. *IEEE Wireless Communications Letters*, 2020, 9(1): 103–107. doi: 10.1109/LWC.2019.2943466.

[13] HUANG Hongji, SONG Yiwei, YANG Jie, *et al*. Deep-learning-based millimeter-wave massive MIMO for hybrid precoding[J]. *IEEE Transactions on Vehicular Technology*, 2019, 68(3): 3027–3032. doi: 10.1109/TVT.2019.2893928.

[14] ZENG Jun, HE Zhengran, SUN Jinlong, *et al*. Deep transfer learning for 5G massive MIMO downlink CSI feedback[C]. 2021 IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China, 2021. doi: 10.1109/WCNC49053.2021.9417349.

[15] HU Zhengyang, GUO Jianhua, LIU Guanzhang, *et al*. MRFNet: A deep learning-based CSI feedback approach of massive MIMO systems[J]. *IEEE Communications Letters*, 2021, 25(10): 3310–3314. doi: 10.1109/LCOMM.2021.3099841.

胡锦松：男，博士，讲师，研究方向为无线通信与深度学习、隐蔽通信、物理层安全、天线阵列信号处理等.

蒋宛伶：女，硕士生，研究方向为无线通信与深度学习、物理层安全、天线阵列信号处理等.

陈由甲：女，博士，博士生导师，教授，研究方向为移动通信、边缘计算、工业物联网、深度学习等.

徐艺文：男，博士，博士生导师，教授，研究方向为视频编码与传输、触感信息编码、人工智能与大数据分析等.

赵铁松：男，博士，博士生导师，教授，研究方向为无线通信与深度学习、智能视频编码、计算机视觉等.

束 锋：男，博士，博士生导师，教授，研究方向为无线信息安全传输、大规模MIMO、无人机通信、无线定位技术等.

责任编辑：余 蓉