DOI: 10.13382/j.jemi.B2003842

基于人工神经网络的联合中继和干扰选择策略研究*

张广大[1] 任清华[1,2] 樊志凯[1]

(1. 空军工程大学 信息与导航学院 西安 710077; 2. 中国电子科技集团公司
航天信息应用技术重点实验室 石家庄 050081)

摘 要:针对多中继通信网络,中继选择算法效率低及潜在窃听节点的安全威胁问题。提出一种基于人工神经网络的联合中继和干扰节点选择策略。首先,采用解码转发(decode-and-forward,DF)中继协议,构建存在窃听节点的多中继协作通信网络,结合协作干扰策略,推导得到系统安全中断概率的闭合表达式;然后,对神经网络进行训练,将相关节点的信道状态信息(channel state information,CSI)作为输入对模型进行训练,获得最优模型参数;最后,利用部分数据集验证模型,仿真结果表明对最优节点选择的正确率能够达到93%以上。与传统选择方案相比,所提方案实现复杂度降低且计算时间明显减少,并且有效改善了系统的安全性能。

关键词: 物理层安全;中继选择;人工神经网络;协作干扰;安全中断概率;信道状态信息

中图分类号: TN918.8 **文献标识码**: A **国家标准学科分类代码**: 510.5030

Research on joint relay and jammer selection strategy based on artificial neural network

Zhang Guangda[1] Ren Qinghua[1,2] Fan Zhikai[1]

(1. Information and Navigation College, Air Force Engineering University, Xi'an, 710077, China;
2. Key Laboratory of Aerospace Information Applications, China Electronics Technology Group, Shijiazhuang 050081, China)

Abstract: Aiming at the problems of low efficiency of relay selection algorithm and security threat of potential eavesdropping nodes in multi-relay communication network. A joint relay and jammer selection strategy based on artificial neural network is proposed. Firstly, the decode-and-forward (DF) relay protocol is adopted to construct the multi-relay cooperative communication network with eavesdropper, and the closed form expression of the security outage probability is derived by combination with the cooperative jamming strategy. Then, the neural network is trained, and the channel state information (CSI) of the relevant nodes is taken as the input data to train the model to obtain the optimal model parameters. Finally, some data sets are used to verify the model, and the simulation results show that the accuracy of optimal nodes selection can reach more than 93%. Compared with the traditional selection scheme based on exhaustive search and support vector machine, the proposed scheme reduces the implementation complexity and computation time significantly, and effectively improve the security performance of the system.

Keywords: physical layer security; relay selection; artificial neural network; cooperative interference; secrecy outage probability; channel state information

0 引 言

在第五代移动通信网络技术的蓬勃发展的背景下,越来越多的人们通过移动终端进行信息的传输,而无线传输的广播特性则决定了其数据交换过程极易遭受非法用户的窃听和攻击。因此,提高无线通信网络的安全性至关重要。在传统通信网络中,通信安全主要依赖于以密码学为基础的上层加密算法,其仅仅是通过提高算法的计算复杂度实现[1-2]。但在计算能力的不断提升的背

收稿日期:2020-12-31 Received Date: 2020-12-31
*基金项目:国家重点实验室合作基金(kx162600022)项目资助

景下,加密算法被破解的可能性越来越大。为了寻求新的解决方案,物理层安全[3-4]技术作为一种能够弥补传统加密技术的新兴安全技术,旨在利用合法信道与窃听信道不同的信道特性实现信息的安全传输[5]。1975 年,Wyner 首次提出了搭线窃听模型[6],并证明当合法信道的信道质量优于窃听信道时,完美的保密性是可以实现的,这为物理层安全技术的的研究提供了理论基础和方法指导。

无线通信网络中除了对安全性有着较高要求之外,在信息传输速率、信号覆盖范围以及通信质量等方面的要求也日益增长。文献[7]提出了多天线技术,在通信双方配置多根天线来提高网络的分集增益,从而提高系统的性能。然而,多天线技术会受到设备体积和成本等因素的限制,实际普及较为困难。为了克服这一问题,协作中继技术由此产生。协作中继技术被证明能够显著提高通信系统的有效性、可靠性和稳健性[8]。Laneman 等[9]从协作分集的角度研究无线网络的协作中继技术,提出了协作中继的两种策略,分别是放大转发(amplify-and-forward, AF)和译码转发(decode-and-forward, DF),结论表明两种协作策略可以进一步增加通信系统的效率。

目前,对于存在多个中继节点的协作网络的研究较多,主要集中在窃听信道下,研究利用不同的中继选择策略实现信息的安全传输。文献[10]给出了基于 AF 策略的中继选择方案,通过对系统各链路的信噪比值进行优化选择,实现合法信道的信道质量最优化。文献[11]针对基于 DF 策略下的协作通信网络,研究了一种机会中继选择方法,提升了系统的安全性能。文献[12]讨论了放大转发和解码转发协作机制下的最优中继选择方案,即根据主信道的 CSI 来选择使得通信系统拥有最大安全容量的中继节点。文献[13]分析了基于 AF 和 DF 策略的最优中继选择,提出了一种多中继组合方案,确保了信息传输的可靠性。以上文献主要着眼于如何提升合法信道的质量,对于窃听信道信道质量考虑较少。实际应用中,考虑到若窃听信道质量优于合法信道质量,则系统的安全容量为 0。由于系统功率的限制,表明不同中继选择策略对于合法信道质量的增强是有限的。此时,系统的安全性将无法保证。因此,单一的中继选择方法对通信系统安全的局限性较大。

另外,为了分析和提升系统的性能,往往需要对全部信道状态信息进行计算和分析,根据目标函数选择出性能最佳的中继节点[14-16]。由此带来的系统开销较大,并且随着中继节点数目的增加,信道状态信息将呈指数增长,计算复杂度将逐步加大。所以,如何在保证中继节点选择的最优解的前提下,降低其计算代价也是亟需解决的问题。

随着机器学习研究的不断深入,在诸多领域的应用已取得相当的成果,如计算机视觉,自然语言处理,语音识别等方向。而神经网络作为实现机器学习任务的一种方法,因其具有存储和利用经验知识的特征而应用广泛。近年来,有不少文献研究神经网络在无线通信中的应用[15-17]。其中,文献[17]围绕 LTE 通信中基站的资源管理问题,提出了一种基于深度学习的方法,不仅促进了小基站可以积极的动态的进行信道选择、载波聚合以及部分的频谱接入,并确保了网络中资源分配的公平性。文献[18]基于卷积神经网络,通过构建结构化模型的信道估计器,与传统信道估计算法相比,降低了复杂度,减少了计算量;文献[19]首次提出双层卷积神经网络模型,将天线选择和混合波束成形设计问题抽象为分类问题,仿真表明,该文献提出的框架具有更好的性能和效率。

针对以上问题,在多中继单窃听信道下,本文提出了一种基于人工神经网络的联合中继选择和协同干扰策略。推导出存在协作干扰节点时,系统中断概率的闭合表达式。所提方案将中继节点和干扰节点的选择抽象为一个分类问题,利用人工神经网络学习模型,最优地选择选择两个节点。与之前所提出的不同的中继选择方案进行对比。仿真表明,所提方法在性能与其近乎相同的情况下,拥有更低的复杂度。

1　系统模型和问题描述

1.1　系统模型

无线中继协作通信系统如图 1 所示,该通信系统由一个源节点 S,一个目的节点 D,一个窃听节点 E 和 m 个中继节点组成,中继节点采用 DF 协议,中继节点的集合记为 $S_{\text{relay}}=\{R_1,\cdots,R_m\}$,且通信系统中任一节点只有一根天线接收和发送信号,故节点只能以半双工的方式工作,而该模型不仅需要中继节点作为传输外,还选择一个中继节点用作向窃听节点发送干扰,从而实现安全传输。其中,源节点 S 到各中继节点 R_i 和窃听节点 E 的信道,中继节点到目的节点 D 和窃听者的信道均相互独立,由于障碍物等因素的影响,源节点与目的节点以及窃听用户之间均不存在直接通信链路,即信息传输必须依靠中继节点转发。

假设所有信道均属于静态平坦瑞利衰落信道,信道系数服从零均值复高斯分布。将任意两个节点间的信道系数记 $h_{ij}\sim CN(0,\sigma_{ij}^2)$,其中 i j 分别表示不同的节点。其中 $\sigma_{ij}^2=d_{ij}^{-\beta}$,$d$ 表示任意两个节点间的距离,β 为与环境有关的衰落指数。假设全局信道状态信息对于目的节点来说是已知的。

图 1 模型信息传输过程被分为两个阶段。

1)源节点以发射功率 P_S 向所有中继节点广播源信

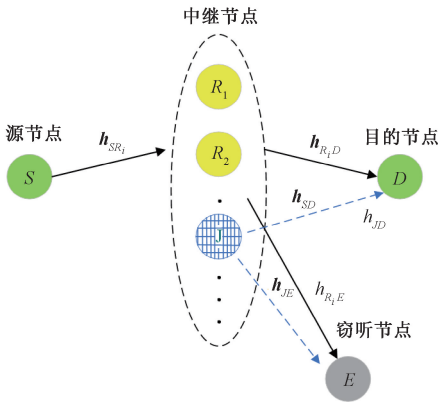


图 1 多中继协作通信系统模型

Fig. 1 System model of multi-relay cooperative communication

号,而且认为中继能够成功地对源信号进行正确解码。此时,将成功解码的所有中继节点构成一个集合 $\Omega \subseteq S_{\text{relay}}$,则 Ω 表示所有可能成功解码的中继组合,称为解码集,$|\Omega|$ 表示在集合中的中继数目。则在各个中继节点 $R_i(i=1,2,\cdots,m)$ 的接收信号的数学表达式为:

$$y_{R_i} = \sqrt{P_S} h_{SR} x_S + n_{R_i} \tag{1}$$

式中:x_s 表示源节点发送的信号;$n_{R_i} \sim CN(0,\sigma_{R_i}^2)$ 表示在中继端处的加性高斯白噪声(additive white Gaussian noise,AWGN)。

对应的 S-R_i 信道的瞬时信道容量为:

$$C_{SR_i} = \frac{1}{2}\log_2(1+\gamma_S |h_{SR_i}|^2) \tag{2}$$

2)中继节点采用机会中继选择策略,基于信道状态信息选择最佳中继,以功率 P_R 向目的节点 D 转发源信号的再编码信号 x'_S。同时,用作干扰的节点 J 发送干扰信号,此时目的节点和窃听节点的信号接受均会受到影响,为了尽量减少干扰信号对目的节点的影响,设定该一般干扰节点 J 的发射功率远远小于源节点和中继节点 R 的发送功率,即满足 $P_J \ll P_S = P_R$。那么目的节点接收信号的表达式为:

$$y_D = \sqrt{P_R} h_{RD} x'_S + \sqrt{P_J} h_{JD} x_J + n_D \tag{3}$$

窃听节点 E 从窃听信道接收到的信号表达式为:

$$y_E = \sqrt{P_R} h_{RE} x'_S + \sqrt{P_J} h_{JE} x_J + n_E \tag{4}$$

式中:$n_D \sim CN(0,\sigma_D^2)$;$n_E \sim CN(0,\sigma_E^2)$ 分别为目的节点处和窃听节点处的高斯白噪声;且 n_{R_i}、n_D、n_E 均是方差 N_0 的复高斯变量;x_J 为发送的干扰信号;P_J 为发送干扰信号功率。

根据信道容量的计算公式,对于任意被选取的中继节点,相应的 R_i-D 和 R_i-E 信道的瞬时信道容量为:

$$C_{R_iD} = \frac{1}{2}\log_2\left(1+\frac{\gamma_R |h_{R_iD}|^2}{1+\gamma_J |h_{JD}|^2}\right) \tag{5}$$

$$C_{R_iE} = \frac{1}{2}\log_2\left(1+\frac{\gamma_R |h_{R_iE}|^2}{1+\gamma_J |h_{JE}|^2}\right) \tag{6}$$

式中:$\gamma_R = P_R/N_0$,$\gamma_J = P_J/N_0$,分别表示中继节点转发信息的平均信噪比和干扰节点发送干扰信号的平均信噪比。

由式(5)和(6)可知,系统瞬时安全容量 C_{sec} 表达式为:

$$\text{if } \Omega = \varnothing \quad C_{sec}^{(\Omega,S_{relay})}(R_i,J) = 0$$

$$\text{if } \Omega \neq \varnothing \quad C_{sec}^{(\Omega,S_{relay})}(R_i,J) =$$

$$[C_{R_iD} - C_{R_iE}]^+ = \left[\frac{1}{2}\log_2\left(1+\frac{\gamma_R |h_{R_iD}|^2}{1+\gamma_J |h_{JD}|^2}\right) - \frac{1}{2}\log_2\left(1+\frac{\gamma_R |h_{R_iE}|^2}{1+\gamma_J |h_{JE}|^2}\right)\right]^+ \tag{7}$$

故联合中继和干扰节点最优选择方案可表达为:

$$(R^*,J^*) = \arg\max_{\substack{R\in\Omega,\\ J\in S_{relay},\\ R\neq J}} \{C_{sec}^{(\Omega,S_{relay})}(R_i,J)\} =$$

$$\arg\max_{\substack{R\in\Omega,\\ J\in S_{relay},\\ R\neq J}} \left\{\frac{1}{2}\log_2\left(\left(1+\frac{\gamma_R |h_{R_iD}|^2}{1+\gamma_J |h_{JD}|^2}\right)/\left(1+\frac{\gamma_R |h_{R_iE}|^2}{1+\gamma_J |h_{JE}|^2}\right)\right)\right\} \tag{8}$$

1.2 问题描述

中断概率是衡量系统安全性能的一个重要指标,主要测度系统安全传输的持续性能。定义为瞬时安全容量低于某一目标安全速率值 R_s 的概率。当安全容量 C_s 满足 $C_s < R_s$ 时,发生中断事件,则通信系统的安全性将无法保证。具体表达为:

$$P_{out} = \Pr(C_s < R_s) \tag{9}$$

通信第 2 阶段中,根据式(8)选择出最佳中继解码转发信息和最佳干扰节点发送干扰,由式(8)可以看出,该式求解复杂,为降低计算复杂度,做渐近分析有,设 $\gamma_J |h_{JD}|^2 \gg 1$,$\gamma_J |h_{JE}|^2 \gg 1$,$P_R/P_J \gg 1$ 该方案表达式可渐进等价为:

$$(R^*,J^*) \simeq \arg\max\left\{\frac{|h_{R_iD}|^2}{|h_{JD}|^2}\Big/\frac{|h_{R_iE}|^2}{|h_{JE}|^2}\right\} =$$

$$\begin{cases} R^* = \arg\max\limits_{R_i\in\Omega}\left\{\dfrac{|h_{R_iD}|^2}{|h_{R_iE}|^2}\right\} \\ J^* = \arg\min\limits_{J\in|S_{relay}-R^*|}\left\{\dfrac{|h_{JD}|^2}{|h_{JE}|^2}\right\} \end{cases} \tag{10}$$

则目的节点 D 仅接收到最佳中继发来的信号。根据全概率公式,可得:

$$P_{out} = \Pr\{C_{sec}^{(\Omega,S_{relay})}(R_i,J) < R_s\} =$$

$$\sum_{n=0}^{m}\Pr\{|\Omega|=n\}*\Pr\{C_{sec}^{(\Omega,S_{relay})}(R_i,J)<R_s\,|\,|\Omega|=n\} \tag{11}$$

$$\Pr\{C_{sec}^{(\Omega,S_{relay})}(R_i,J)<R_s\,|\,|\Omega|=n\}\simeq \Pr\left\{\frac{1}{2}\log_2\left(\frac{|h_{RD}|^2|h_{JE}|^2}{|h_{RE}|^2|h_{JD}|^2}\right)<R_s\right\} \tag{12}$$

其中，$\Pr\{|\Omega|=n\}$ 表示的是在集合 Ω 中，中继数目为 n 的概率。则将式(2)代入有：

$$\Pr\{|\Omega|=n\}=\binom{n}{m}[\Pr(C_{sec}>R_s)]^n[\Pr(C_{sec}\leqslant R_s)]^{m-n}=\binom{n}{m}\left[\exp\left(-\frac{2^{2R_s}-1}{E[|h_{SR_i}|^2]}\right)\right]^n\left[1-\exp\left(-\frac{2^{2R_s}-1}{E[|h_{SR_i}|^2]}\right)\right]^{m-n} \tag{13}$$

当 $n=0$ 对应于解码集为空，此时条件概率为 $\Pr(C_{sec}<R_s\,|\,|\Omega|=n)=0$。

当 $n>0$，则解码集不为空，则存在最佳中继节点 R_0 选择，$\Pr(C_{sec}<R_s\,|\,|\Omega|=n)$ 表示中继选择后系统发生安全中断的概率，将式(7)代入式(11)，即可被计算为：

$$\Pr\{C_{sec}^{(\Omega,S_{relay})}(R_i,J)<R_s\,|\,|\Omega|=n\}=\int_0^{\infty}\left[\prod_{i=1}^{n}\left(\frac{w_2\mu}{w_2\mu+\lambda_i}\right)\right]\times\prod_{j=1}^{m-1}\lambda_j\left\{\frac{d}{dw_2}\left[\prod_{j=1}^{m-1}(w_2+\lambda_j)\right]\right\}/\prod_{j=1}^{m-1}(w_2+\lambda_j)^2\mathrm{d}w_2 \tag{14}$$

设两个随机变量，分别为 $X_i=|h_{R_iD}|^2/|h_{R_iE}|^2$，$Y_j=|h_{JD}|^2/|h_{JE}|^2$，由概率论知识可得，随机变量 Y 的概率分布函数表示如下：

$$F_Y(y)=\frac{y}{y+\lambda_j} \tag{15}$$

设随机变量 $W_1\triangleq\max\{X\}$，$W_2\triangleq\min\{Y\}$ 将定义随机变量 W_1、W_2 代入式(12)得：

$$P_{out}=\Pr\left\{\frac{W_1}{W_2}<2^{2R_s}\right\}=\Pr\{W_1/\mu W_2\}=\int_0^{\infty}F_{W_1}(w_2\mu)f_{W_2}(w_2)\mathrm{d}w_2 \tag{16}$$

根据信道模型可知随机变量 X_i 和 Y_j 相互独立，所以随机变量 W_1 的概率分布函数为：

$$F_{W_1}(w_1)=\prod_{i=1}^{n}\left(\frac{w_1}{w_1+\lambda_i}\right) \tag{17}$$

随机变量 W_2 的概率分布函数为：

$$F_{W_2}(w_2)=1-\prod_{j=1}^{m-1}\left(1-\frac{w_2}{w_2+\lambda_j}\right) \tag{18}$$

对式(17)求导，有随机变量 W_2 的概率密度函数：

$$f_{w_2}(w_2)=\frac{\left\{\frac{d}{dw_2}\left[\prod_{j=1}^{m-1}(w_2+\lambda_j)\right]\right\}\prod_{j=1}^{m-1}\lambda_j}{\prod_{j=1}^{m-1}(w_2+\lambda_j)^2} \tag{19}$$

其中，$\mu=2^{2R_s}$，$\lambda_i=E[|h_{R_iD}|^2]/E[|h_{R_iE}|^2]$ 表示中继节点到目的节点和窃听节点的链路平均信道增益之比，$\lambda_j=E[|h_{JD}|^2]/E[|h_{JE}|^2]$ 表示干扰节点到目的节点和窃听节点的链路平均信道增益之比。

由式(15)、(16)和式(18)可得式(14)。将式(13)和(14)代入式(11)，系统安全中断概率闭合表达式为：

$$P_{out}=\sum_{n=0}^{m}\binom{n}{m}\left[\exp\left(-\frac{2^{2R_s}-1}{E[|h_{SR_i}|^2]}\right)\right]^n\left[1-\exp\left(-\frac{2^{2R_s}-1}{E[|h_{SR_i}|^2]}\right)\right]^{m-n}\times\int_0^{\infty}\left[\prod_{i=1}^{n}\left(\frac{w_2\mu}{w_2\mu+\lambda_i}\right)\right]\frac{\left\{\frac{d}{dw_2}\left[\prod_{j=1}^{m-1}(w_2+\lambda_j)\right]\right\}\prod_{j=1}^{m-1}\lambda_j}{\prod_{j=1}^{m-1}(w_2+\lambda_j)^2}\mathrm{d}w_2 \tag{20}$$

由安全分析可知，最佳中继和干扰选择的问题为非线性的，并且随着中继中继节点数目的增多，选择方案的时间复杂度将呈现平方型增长，消耗资源较大。针对这一问题，本文研究并提出了基于神经网络的联合中继和干扰选择方案，通过把节点的优化选择问题作为分类的问题去解决。利用训练好的模型预测最佳中继节点和干扰节点的标签，所得标签对应节点能够最大化安全容量，增强安全传输性能。

2　基于人工神经网络的联合中继和干扰选择方案

2.1　训练数据集预处理

1)生成训练数据集

根据通信模型，首先构造包含 K 个训练样本的训练数据集合，单个样本由信道状态信息和对应的源节点发送功率组成，样本集合表示为：

$$\boldsymbol{H}_{train}=\{[\boldsymbol{S}_R^1,\boldsymbol{R}_D^1,\boldsymbol{E}_R^1,\boldsymbol{P}_S^1],[\boldsymbol{S}_R^2,\boldsymbol{R}_D^2,\boldsymbol{E}_R^2,\boldsymbol{P}_S^2],\cdots,[\boldsymbol{S}_R^K,\boldsymbol{R}_D^K,\boldsymbol{E}_R^K,\boldsymbol{P}_S^K]\} \tag{21}$$

其中，$\boldsymbol{S}_R^K$ 表示从是源节点和中继节点之间的第 k 个信道状态信息矩阵，$\boldsymbol{R}_D^K$ 表示从中继节点到目的节点的第 k 个信道状态信息矩阵，$\boldsymbol{E}_R^K$ 表示第 k 个中继节点到窃听节点的信道状态信息矩阵，$\boldsymbol{P}_S^K$ 为其对应的源节点发送功率。

(1) 提取各个信道状态信息矩阵中每个元素的实值，构成一个 1×(3m+1)维特征向量，记为：

$$\begin{aligned}\boldsymbol{d}^k = [&|h_{SR_1}^k|,|h_{SR_2}^k|,\cdots,|h_{SR_{m_r}}^k|,\\&|h_{R_1D}^k|,|h_{R_2D}^k|,\cdots,|h_{R_{m_r}D}^k|,\\&|h_{R_1E}^k|,|h_{R_2E}^k|,\cdots,|h_{R_{m_r}E}^k|,p^k]\end{aligned} \tag{22}$$

(2)根据所有的信道状态信息数据集 $\boldsymbol{H}_{train}$，重复步骤(1)，产生 K 个特征向量。记为 $\boldsymbol{d}_1,\boldsymbol{d}_2,\cdots,\boldsymbol{d}_k$。

(3) 堆叠向量 $\boldsymbol{d}_k$ 生成训练数据集 $\boldsymbol{D}\in\boldsymbol{R}^{K\times(3m+1)}$，$\boldsymbol{D}=[\boldsymbol{d}_1^{\mathrm{T}},\boldsymbol{d}_2^{\mathrm{T}},\cdots,\boldsymbol{d}_K^{\mathrm{T}}]^{\mathrm{T}}$。

(4)将矩阵 $\boldsymbol{D}$ 中向量进行归一化处理，获得矩阵 $\boldsymbol{T}$，$\boldsymbol{T}$ 中第(i,j)元素记为 $t_{i,j}$：

$$t_{i,j}=\frac{d_{ij}-\boldsymbol{E}_i\{d_{ij}\}}{\max_i\{d_{ij}\}-\min_i\{d_{ij}\}}$$

式中：d_{ij} 表示 $\boldsymbol{D}$ 第 i 行第 j 列元素，$\max_i\{d_{ij}\}$ 和 $\min_i\{d_{ij}\}$ 分别表示元素所在行最大值和最小值。

2)对训练数据集标记

本文选取安全容量为关键性能指标(key performance indicator, KPI)。计算每个中继集合通信方案的安全容量，选择达到最大的安全容量对应的集合索引，作为该训练样本的类别标记。

在联合中继和干扰最优节点选择方案中，m 个节点中选择两个不同作用的节点，则共有 $m\times(m-1)$ 个类标签。同时方案中需要考虑所有中继节点不能正确解码的情况，即无信息传输(no transmission, NT)。本文所提方案中共有 $M=m\times(m-1)+1$ 个类别标签。表 1 为含有 3 个中继节点(R_1,R_2,R_3)通信系统示例。

表 1 三个中继节点系统的标签示例

Table 1 Example of labeling for the system with three relays

联合中继和干扰节点(R_i,R_j)	标签(t)
Ø	0
(R_1,R_2)	1
(R_1,R_3)	2
(R_2,R_1)	3
(R_2,R_3)	4
(R_3,R_1)	5
(R_3,R_2)	6

综上，完成完成 K 个训练样本标签后，将样本标签向量记为 $\boldsymbol{L}=[l_1,l_2,\cdots,l_K]^{\mathrm{T}}$。则完整训练数据集表示为 $\boldsymbol{D}_{train}=\{(t_1,l_1),(t_2,l_2),\cdots,(t_K,l_K)\}$，$\boldsymbol{t}_k$ 为矩阵 $\boldsymbol{T}$ 中行向量。

2.2 人工神经网络(ANN)模型建立

ANN 是指由大量的处理单元互相连接而形成的复杂信息处理系统，是一种多层前馈式网络。通过误差逆传播算法通过反向传播误差信号调制网络权值训练数据，使实际输出与期望误差最小[20]。由于 ANN 不需要建立复杂的数学模型，且只要选取合理的参数和通过足够数据的训练，对复杂的非线性问题有较强的拟合能力[21]。

本文用到的人工神经网络拓扑如图 2 所示，该网络包括一层输入层、两层隐藏层以及一层输出层。其中输入层神经元个数由通信模型中节点的数据特征数决定；而隐藏层神经元节点数目对神经网络模型预测进度有比较重要的影响，节点数目过多，结构庞大，训练时间增加，隐藏层节点数目低，结构简单，但不容易收敛。本文利用实验法得到分类效果最佳的隐藏层神经元数目。

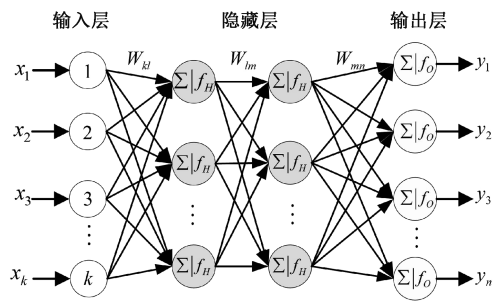


图 2 人工神经网络拓扑结构

Fig. 2 The topological structure of artificial neural networks

图 2 中，$x_1,x_2,\cdots,x_k$ 为输入序列，W_{kh_1}、$W_{h_1h_2}$、W_{h_2n} 神经元之间的对应的权值，$y_1,y_2,\cdots,y_n$ 为输出序列；k 为输入序列维数。h_1 和 h_2 表示两层隐藏层神经元数目，n 为输出层神经元个数。f_H、f_O 分别为隐藏层和输出层激活函数，对于隐藏层，选取 ReLU 函数作为激活函数。Softmax 函数应用于输出层，得到所有类别的概率分布，然后获得具有最大概率值的对应类别标签。损失函数采用分类交叉熵函数。表达式如下：

$$f_{\mathrm{ReLU}}(x)=\max(0,x) \tag{23}$$

$$f_{\mathrm{Softmax}}(y_i)=\frac{\exp(y_i)}{\sum_{j=1}^{n}\exp(y_j)} \tag{24}$$

$$Loss=\sum_{i=1}^{Q}\sum_{j=1}^{C}t_{ij}\mathrm{In}y_{ij} \tag{25}$$

式中：y_i 为第 i 个节点的输出值，对应每一个分类标签；Q 代表样本数目，I_{ij} 表示指示变量(0 或 1)，当输出标签 j 和样本 i 标签相同就是 1，否则是 0；y_{ij} 表示对于测试样本 i 属于类别 j 的预测概率。

2.3　基于神经网络的联合中继和干扰节点选择步骤

本算法使用分类准确率和损失值评估神经网络分类模型,并且比较不同模型结构的性能。基于神经网络的选择算法步骤如下。

1)确定选择模型输入与输出。

2)生成描述输入与输出关系的数据集。

3)将数据集分为训练集与验证集,70%数据集作为训练集,30%数据集作为验证集。

4)使用训练集对 ANN 模型进行训练。为了找到合适的隐藏层节点数量,使用不同的神经网络结构与超参数重复步骤 1)~4)。同时采用不同的隐藏节点数量进行模型训练,利用验证集进行验证。如果在上述步骤完成后并未获得最高的准确率或者良好的收敛情况,则应执行如下步骤:(1)确定模型的结构参数和超参数;(2)使用训练集训练 ANN 模型;(3)使用验证集验证模型表现;(4)对验证数据集在模型的表现进行分析,评估 ANN 选择结果的性能。

2.4　基于支持向量机(SVM)最优中继和干扰节点选择方案

SVM 作为一种基于统计学习理论的机器学习算法,其具有泛化错误低且学习结果具有很好地推广性等优点,已经成为机器学习领域的研究热点。

当其用于多分类问题时,常见的有“一类对余类(one-versus-rest, OVR)”“一类对一类(one-versus-one, OVO)”,分类模型有 OVO 和 OVR。OVO 模型通过将任意两个类别中训练一个分类器;OVR 模型通过将其中的一个类别视为一类,剩余的其他所有类别视为另一类。

考虑到开销和复杂度,本文采用“一类对余类”模型。通过 OVR 模型需要构造 M 个二分类器,实现步骤如下。

1) 设分类目标标签 x,定义子训练数据集$\{T_x\}$,包含上文训练数据集$\{T\}$中对应标签为 x 所有训练样本。同时将$\{T\}$中剩余的样本数据构造另一个子训练数据集$\{\overline{T}_x\}$。

2) 生成 $K\times1$ 维二分类标签向量记为 $b_x, x\in M$, $b_x=[b_x[1],b_x[2],\cdots,b_x[K]]^{\mathrm{T}}$, 向量 $\boldsymbol{L}$ 中若 $l_k=x$, 则令 $\boldsymbol{b}_x[k]=1$,否则置为 0。

3) 根据二分类训练子集为$\{T_x,\overline{T_x}\}$,结合相应的二分类标签向量。构建如下目标函数:

$$\theta_x=\min_{\theta_x}C\sum_{k=1}^{K}[b_x[k]g_1(\theta_x^{\mathrm{T}}f(t_k))+(1-b_x[k])\times g_0(\theta_x^{\mathrm{T}}f(t_k))]+\|\theta_x\|^2/2$$

其中, C 为惩罚因子;$g_a(z)$ 为损失函数,且 $g_a(z)=\max((-1)^a z+1,0)$;$f(t_k)$ 为高斯径向基核函数向量,第 i 个元素为 $f_i(t_k)=\exp(-\|t_i-t_k\|^2/2\sigma^2)$,$\sigma$ 为核函数参数。

4)对参数进行寻优。在训练集上,使用网格搜索法,通过 10 折交叉验证,以平均准确率作为分类性能指标,找到惩罚因子 C 和核参数 σ 最优值。

5)将得到优化的参数代入多分类模型中,通过验证集的准确率评估模型性能。

3　仿真分析

3.1　仿真场景以及参数

为验证本文所提方案的准确性以及有效性。仿真将本文所提基于人工神经网络的联合中继和干扰选择算法,与基于 SVM 选择方案和基于穷举搜索方案进行比较。

本文主要研究中继和干扰节点的选择,在仿真场景中,假设所有节点均布置在一个 1×1 的单位区域内,其中源节点与目的节点、窃听节点均设置为固定位置,对应的坐标分别为(0,0),(0,1),(1,0),源节点发射功率 P_S 和中继功率 P_R, 有 $P_S=P_R$。在分别考虑中继节点数目为 8、16、24 不同情况下,采用系统安全容量和安全中断概率衡量系统的安全性能。仿真生成 10^6 个信道状态信息作为数据集用于训练和验证本文所提出方案的有效性。仿真实验参数如表 2 所示。

表 2　仿真参数设置

Table 2　Simulation parameter setting

主要参数	量值
中继节点个数	8、16、24
路径损耗指数 β	3.5
高斯白噪声	1 dBm
干扰节点发送功率	−20~20 dBm
目标保密速率 R_s	2 bit/s/Hz

3.2　方案性能仿真

1)人工神经网络方案参数确定和性能分析

对于不同的训练数据集合,隐藏层神经元个数的最优值往往不同,结果如表 3 所示。

表 3　基于不同结构神经网络训练结果

Table 3　Based on the training results of neural networks with different structures

隐藏单元总数	准确率	运行时间
50	61.18	4.5
100	73.70	7.5
150	76.80	10.1
200	83.04	12.9
250	87.43	16.9
300	90.44	22.9
350	95.25	26.8
400	94.57	33.9

通过实验对比可以看到,测试后神经网络在神经元

350~400 达到了最高的分类准确率。在进一步实验后，确定隐藏层数目为 370~390，准确率最高。由于本文中神经网络被设计为两层隐藏层的结构，故隐藏层神经单元个数可以有不同的组合。仿真结果表明，当隐藏层节点数目较小时，分类精度随着节点数目的增加而增加，当 2 个隐藏层中节点的数目分别达到 128 和 256 时，分类的准确率可以达到 95.36%。且随着数目的增加保持稳定。而当节点数目选择得过大会导致训练时间加长，因此，可以将隐藏层节点数目设置为 128 和 256。

2) 中继和干扰节点选择方案性能仿真

针对所提出的联合中继和干扰节点选择方案进行性能分析。

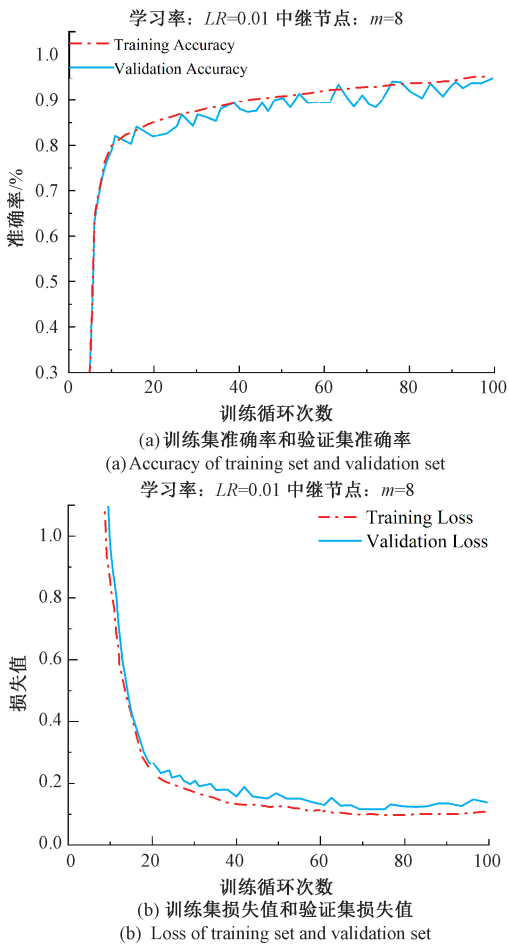


图 3 8 个中继模型训练结果

Fig. 3 Model training results with eight relays

图 3 和 4 所示为本文提出的神经网络模型在训练集和验证集后的收敛情况，通过训练和验证设置中继节点数目 $m=8$ 和 $m=16$ 的不同模型。干扰节点发射功率 $P_R/P_J=100$。可以看出，在每个训练循环后，验证集在训练模型虽然产生轻微震荡，但模型总体上表现较好，两种模型在准确率和损失函数均能够很快收敛到稳定状态，

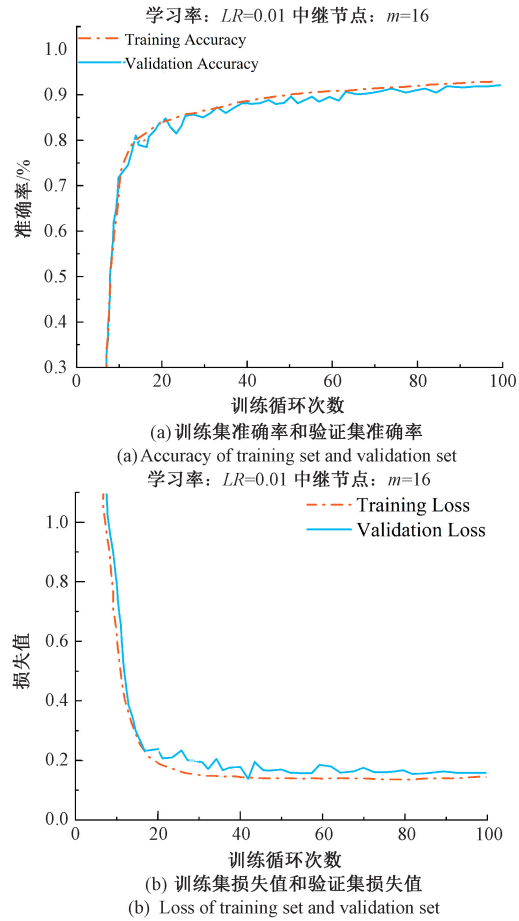


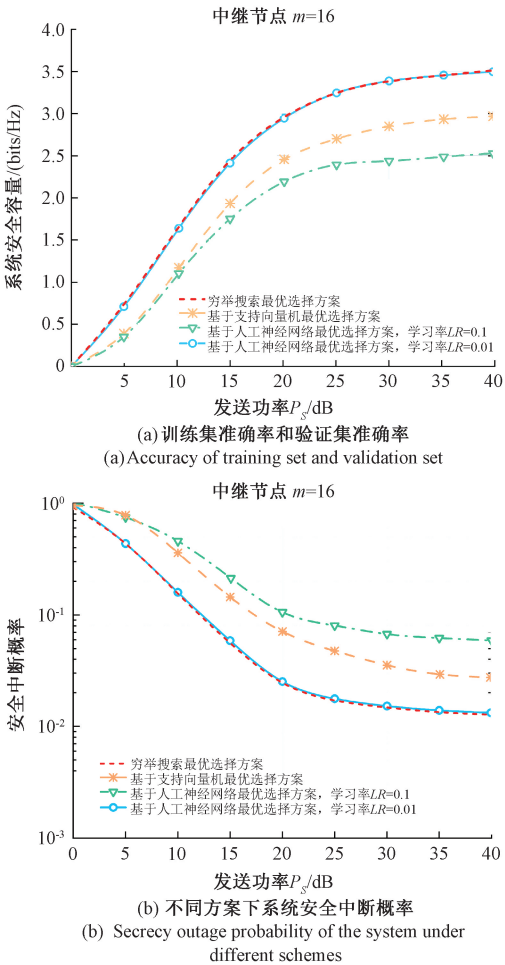
图 4 16 个中继模型训练结果

Fig. 4 Model training results with sixteen relays

训练和验证的准确率。此外，验证集上的曲线拟合情况较好，意味着不存在过拟合问题。经过对比，发现所提出的神经网络模型性能在中继节点数目增加后略有下降。

图 5 所示为本文在当中继节点数目 $m=16$ 时，中继和干扰节点在不同选择方案的系统安全容量和安全中断概率的对比曲线。考虑系统安全容量性能时，可以看到在任意发射功率下，基于神经网络的方案（$LR=0.01$）的系统的安全容量要明显高于基于支持向量机的方案和基于神经网络的方案（$LR=0.1$），并且该方案与穷举搜索最优选择方案几乎完全重合。

而考虑系统安全中断概率，可以发现，随着发射功率的增大，基于神经网络的方案（$LR=0.01$）的安全中断概率与其他方案的差距越来越大，逐渐逼近于穷举搜索的最优方案。而基于神经网络的方案（$LR=0.1$）时，系统的中断概率最大，中断性能最差。显然，对于在学习率 $LR=0.1$ 时，模型训练效果较差，对于中继节点和干扰节点的选择产生较大误差。由于，本文所提方案综合考虑所有信道，通过提取信道特征，对中继和干扰节点进行选择。因此，在学习模型构建较好的前提下，基于神经网络



(a) 训练集准确率和验证集准确率
(a) Accuracy of training set and validation set

(b) 不同方案下系统安全中断概率
(b) Secrecy outage probability of the system under different schemes

图 5　不同选择方案对系统安全性能的影响

Fig. 5　The security performance of the system under different selection schemes

的方案相较于基于支持向量机的方案具有更好的安全性能。

图 6 所示为在不同中继节点数目 m 下，基于神经网络的中继节点和干扰节点选择方案的安全中断概率变化的情况。仿真参数与图 5 中参数设置相同。分别取中继节点数目 $m=8,16,24$。从图 6 直观地分析出，本方案中当中继个数逐渐增多时，本文方案的安全中断概率随之降低。当发送功率为 20 dB 时，3 种不同情况对应的安全中断概率分别为 0.036 5、0.016 4、0.003 6。说明该方案下通信系统的安全性能会随着中继节点数目的增加而得到改善。这是因为在系统中，存在的潜在中继个数越多，从中选取的最佳中继和协作干扰节点的性能更好的概率越大，因此中断概率也下降。需要强调的是，虽然中继节点数目的增加会提升安全性能，但同时也提升实现的复杂度。故中继节点数目的增加要结合实际应用进行整体考虑。

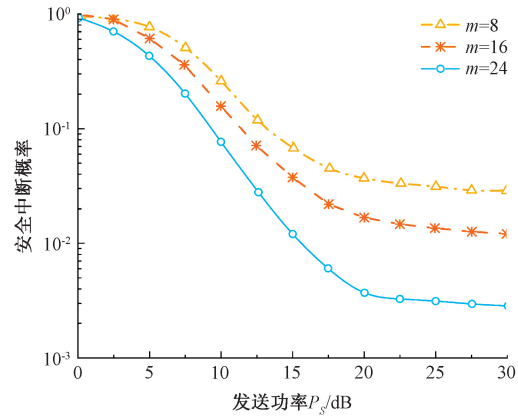


图 6　不同中继个数对于系统安全性能的影响

Fig. 6　The influence of different relay number on system security performance

3) 不同方案时间复杂度性能比较

比较了所提到的 3 种不同方案的预测复杂度和反馈开销，如表 4 所示。

表 4　复杂度和开销比较

Table 4　Complexities and overheads comparison

方案	穷举搜索	SVM	ANN
反馈开销	$F-1$ 维复向量	$F-1$ 维实向量	$F-1$ 维实向量
复杂度	$O(F+\lvert M\rvert\log\lvert M\rvert)$	$O(F^2)$	$O(Fh_1+h_1h_2+h_2M)$

表 4 中，F 代表特征向量的维度，M 代表类别标签。从表 4 可以看到，随着中继节点的增长，基于穷举搜索方案的复杂度相较于另外两种方案将越来越大。尽管基于 ANN 的方案在复杂度上要高于基于 SVM 的方案，但当处理数据规模逐渐加大时，基于 SVM 方案分类的准确率要差于神经网络模型。因此，基于神经网络的方案总体表现要优于另外两种方案。此外，神经网络模型和支持向量机反馈开销也是穷举搜索方案的 1/2。表 5 通过对比计算测试样本的平均预测时间来衡量模型的时间复杂度。从两种方案的计算时间比较可以看到，在不同中继节点个数的情况下，本文所提方案的运行时间均优于穷举搜索算法的运行时间。当中继节点个数增加时，穷举搜索方案计算时间明显增加。因此，基于人工神经网络方案在确保准确率的前提下，计算效率更高。

表 5　计算时间比较

Table 5　Comparison of computation time

中继节点个数	穷举搜索方案时间/s	ANN 方案(测试)时间/s
$m=8$	0.008 58	0.000 26
$m=16$	0.019 44	0.000 52
$m=24$	0.047 82	0.000 70

4 结 论

本文提出了基于神经网络的联合中继节点和干扰节点方案。将协作网络中的中继选择和协作干扰节点的选择问题抽象为多分类问题,以最小化系统安全中断概率为目标函数,利用神经网络构建分类模型进行中继和干扰节点的选择。通过基于不同参数的仿真,从多种角度对该方案的安全性能进行分析。结果表明,所提出的方法对于中继和干扰节点的选择能够达到较高的准确率,并且在计算时间显著降低的情况下,能够达到与穷举搜索方法几乎相同的安全性能。但是,模型随着中继节点个数的增加准确率有所降低,且模型自适应能力较弱。下一步将就模型自适应能力和准确率的提升展开研究。

参考文献

[1] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[2] 张启星, 付敬奇. 基于信道特征提取的物理层安全密钥生成方法[J]. 电子测量与仪器学报, 2019, 33(1): 16-22.
ZHANG Q X, FU J Q. Physical layer security key generation method based on channel feature extraction[J]. Journal of Electronic Measurement and Instrumentation, 2019, 33(1): 16-22.

[3] ZENG W, ZHANG J, CHEN S, et al. Physical layer security over fluctuating two-ray fading channels[J]. IEEE Transactions on Vehicular Technology, 2018, 67(9): 8949-8953.

[4] 潘蕾, 李赞, 李向阳, 等. 基于双向协作中继网络的物理层安全技术研究[J]. 兵工学报, 2020, 41(1): 102-107.
PANL, LI Z, LI X Y, et al. Research on the physical layer security technologies of two-way cooperative relay networks [J]. Acta Armamentarii, 2020, 41(1): 102-107.

[5] POOR H V. Information and inference in the wireless physical layer[J]. IEEE Wireless Communications, 2012, 19(1): 40-47.

[6] LEUNG-YAN-CHEONG S, HELLMAN M. The Gaussian wire-tap channel[J]. IEEE Transactions on Information Theory, 1978, 24(4): 451-456.

[7] 冯友宏, 岳雪峰, 杨志, 等. 窃听多天线的多用户调度安全性能分析[J]. 无线电通信技术, 2018, 44(3): 224-229.
FENG Y H, YUE X F, YANG ZH, et al. Multiuser scheduling security performance analysis of wiretapping multiple antennas [J]. Radio Communications Technology, 2018, 44(3): 224-229.

[8] DING Z, LEUNG K K, GOECKEL D L, et al. Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting[J]. IEEE Transactions on Wireless Communications, 2011, 10(6): 1725-1729.

[9] LANEMAN J N, TSE D N C, WORNELL G W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior[J]. IEEE Transactions on Information Theory, 2004, 50(12): 3062-3080.

[10] WANG D, BAI B, CHEN W, et al. Achieving high energy efficiency and physical-layer security in AF relaying [J]. IEEE Transactions on Wireless Communications, 2016, 15(1): 740-752.

[11] KRIKIDIS I. Opportunistic relay selection for cooperative networks with secrecy constraints [J]. IET Communications, 2010, 4(15): 1787.

[12] BLETSAS A, SHIN H, WIN M. Cooperative communications with outage-optimal opportunistic relaying [J]. IEEE Transactions on Wireless Communications, 2007, 6(9): 3450-3460.

[13] ZOU Y, WANG X, SHEN W. Optimal relay selection for physical-layer security in cooperative wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(10): 2099-2111.

[14] LIU F, LI J, LI S, et al. Physical layer security of full-duplex two-way AF relaying networks with optimal relay selection[C]. 2018 IEEE Globecom Workshops (GC Wkshps), 2018: 1-6.

[15] ZHOU H, HE D, WANG H, et al. Optimal relay selection with a full-duplex active eavesdropper in cooperative wireless networks[C]. IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Malaysia: IEEE, 2019: 1-5.

[16] 阳俐君, 曹张华, 张士兵, 等. 单窃听双跳协作网络的中继选择方案及其性能分析[J]. 重庆邮电大学学报(自然科学版), 2016, 28(5): 648-657.
YANG L J, CAO ZH H, ZHANG SH B, et al. Relay selection schemes for dual-hop cooperative networks with an eavesdropper and their performance analysis [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2016, 28(5):648-657.

[17] CHALLITA U, DONG L, SAAD W. Proactive resource management for LTE in unlicensed spectrum: A deep learning perspective[J]. IEEE Transactions on Wireless Communications, 2018, 17(7): 4674-4689.

[18] NEUMANN D, WIESE T, UTSCHICK W. Learning the

MMSE channel estimator[J]. IEEE Transactions on Signal Processing, 2017, arXiv:1707.05674.

[19] ELBIR A M, MISHRA K V. Deep learning design for joint antenna selection and hybrid beamforming in massive MIMO[C]. IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting, 2019: 1585-1586.

[20] 刘国光, 武志玮, 牛富俊, 等. 基于 BP 神经网络的场道脱空检测方法及实验[J]. 深圳大学学报(理工版), 2016, 33(3): 309-316.
LIU G G, WU ZH W, NIU F J, et al. Airport pavement void testing based on back propagation neural network[J]. Journal of Shenzhen University Science and Engineering, 2016, 33(3): 309-316.

[21] 蓝金辉, 王迪, 申小盼. 卷积神经网络在视觉图像检测的研究进展[J]. 仪器仪表学报, 2020, 41(4): 167-182.
LAN J H, WANG D, SHEN X P. Research progress on visual image detection based on convolutional neural network[J]. Chinese Journal of Scientific Instrument, 2020, 41(4): 167-182.

作者简介

张广大, 2019 年于成都信息工程大学获得学士学位, 现为空军工程大学硕士研究生, 主要研究方向为网络空间安全、物理层安全。
E-mail: 2694539041@qq.com

Zhang Guangda received B. Sc. degree from Chengdu University of Information Technology in 2019. Now he is a M. Sc. candidate at Air Force Engineering University. His main research interests include Cyberspace Security and physical layer security.

任清华, 1984 年于空军工程大学获得学士学位, 1991 年于空军工程大学获得硕士学位, 现为空军工程大学教授, 主要研究方向为军事航空通信、变换域通信、物理层安全。
E-mail: rentsinghua@163.com

Ren Qinghua received B. Sc. degree from Air Force Engineering University in 1984, M. Sc. from Air Force Engineering University in 1991. Now he is a professor at Air Force Engineering University. His main research interests include military aviation communication, transform domain communication and physical layer security.

樊志凯, 2019 年于空军工程大学获得学士学位, 现为空军工程大学硕士研究生, 主要研究方向为网络空间安全、物理层安全。
E-mail: 331225372@qq.com

Fan Zhikai received B. Sc. degree from Air Force Engineering University in 2019. Now he is a M. Sc. candidate of Air Force Engineering University. His main research interests include cyberspace security and physical layer security.